LANrev
User Guide

macOS Admin Version

HEAT software

www.heatsoftware.com

March 24, 2017

LANrev User Guide 7.3.2 - Documentation Release 1

HEAT Software USA Inc. reserves the right to revise this document, and to periodically make changes in the content hereof without notice of such changes, unless required to do so by prior agreement.

Information contained herein is provided solely for guidance in product usage and not as a warranty of any kind. HEAT Software USA Inc. assumes no responsibility for use of this information, nor for any infringements of patents or other rights of third parties resulting from the use of this information.

HEAT Software USA Inc., 490 N. McCarthy Blvd., Milpitas, California USA 95035.

This product is protected by US patents 7 818 557, 8234 359, 9 009 857, and 9 081 639. Additional patents are pending.

Contents

Part 1: Getting Started

The Getting Started part of the manual contains the information you need to get LANrev running:

“Introduction” on page 2 describes the structure and basic concepts of LANrev.

“Installation” on page 11 guides you through the installation of all LANrev components.

Chapter 1 Introduction

Welcome to HEAT LANrev, the comprehensive management solution for network administrators.

The following text explains the scope and concepts of LANrev and the different parts of the LANrev system. If you want to get your feet wet right away, you can turn to “Installation” on page 11; however, starting with this section will make it easier for you to set up LANrev in the way best suited to your requirements and to quickly employ it for maximum benefit.

For an overview of LANrev, see:

- “What does LANrev do?” on page 2
- “The LANrev system” on page 2
  - “Elements of the LANrev system” on page 3
  - “How commands work” on page 3
  - “LANrev users” on page 9

What does LANrev do?

LANrev helps you manage the computers and mobile devices in your company:

- Collect a wide range of technical information on the devices for overview reports or in-depths analyses of individual devices.
- Control computers, terminating troublesome processes, executing utility scripts, restarting computers, and much more.
- Manage the configuration and security of mobile devices.
- Automate software installations by just specifying the software that is to be installed on each computer or in a workgroup and letting LANrev do the rest. You can even reinstall the operating system or control the distribution of vendors’ operating system patches and third-party patches.
- Distribute software to mobile devices.
- Configure mobile device settings.
- Locate mobile devices.
- Monitor software installations and usage, to always make sure that you stay within license limits (both installation-based and concurrent use licenses) and to know just what your licensing needs are.

And LANrev does all this without you having to leave your desk at all.

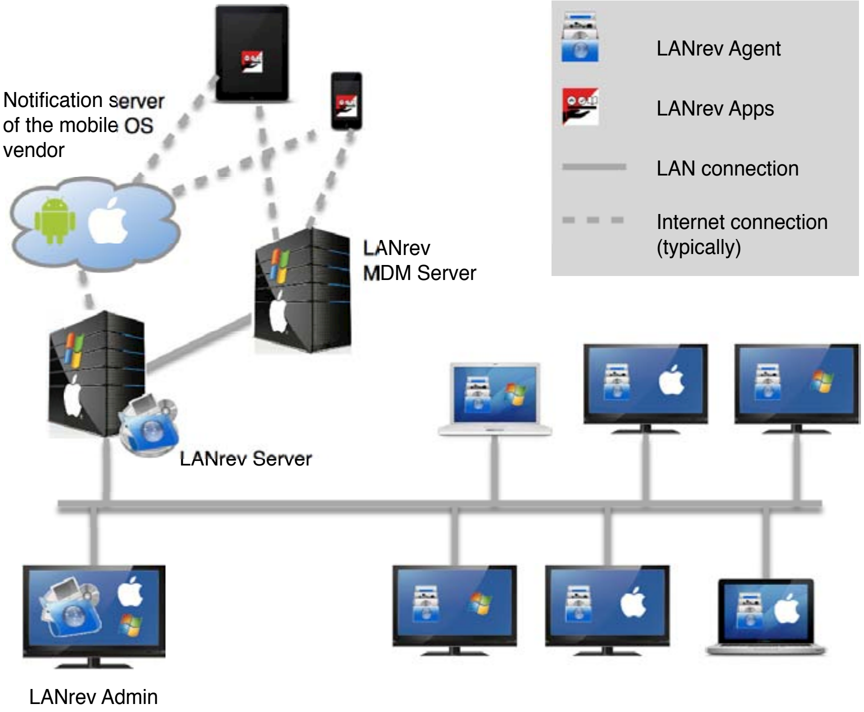
The LANrev system

The LANrev system consists of several different elements that are installed on the computers in the network. There are also different groups of users, as described below.

Elements of the LANrev system

There are several components in the LANrev system:

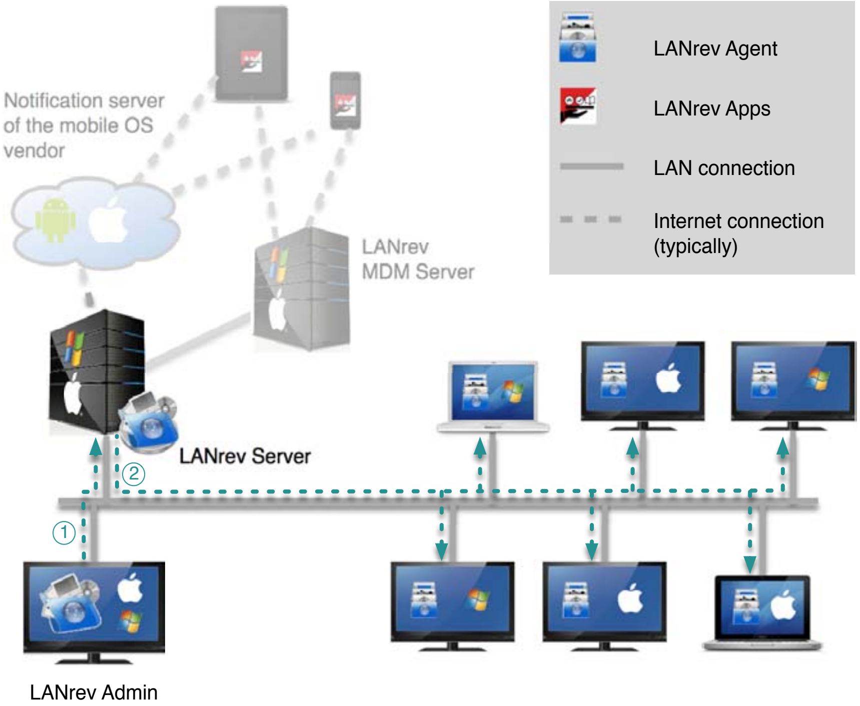
- An agent is installed on each managed device. Agents receive commands from LANrev and carry them out on the local computer, sending back information when required. There is a minimal local interface to specify some information.
- A central server acts as the hub of the system: On instructions from you, it sends out commands to the agents, collects the information they send back, and stores it in its database.
  There is usually one server per managed network; multiple servers are possible. Servers have no user interface of their own; they are managed by the admin application.
  LANrev effortlessly handles hierarchies of servers and specialized servers for, for example, software distribution.
- An optional MDM server handles the management of mobile devices. It is tightly coupled to the main LANrev Server and controlled from the same admin application.
- The admin application is your command center for the system. You use it both to control the server and – via the server – the agents, and to display the required information. The admin application can be installed on as many computers as desired.



Multiple components can be installed on the same computer.

How commands work

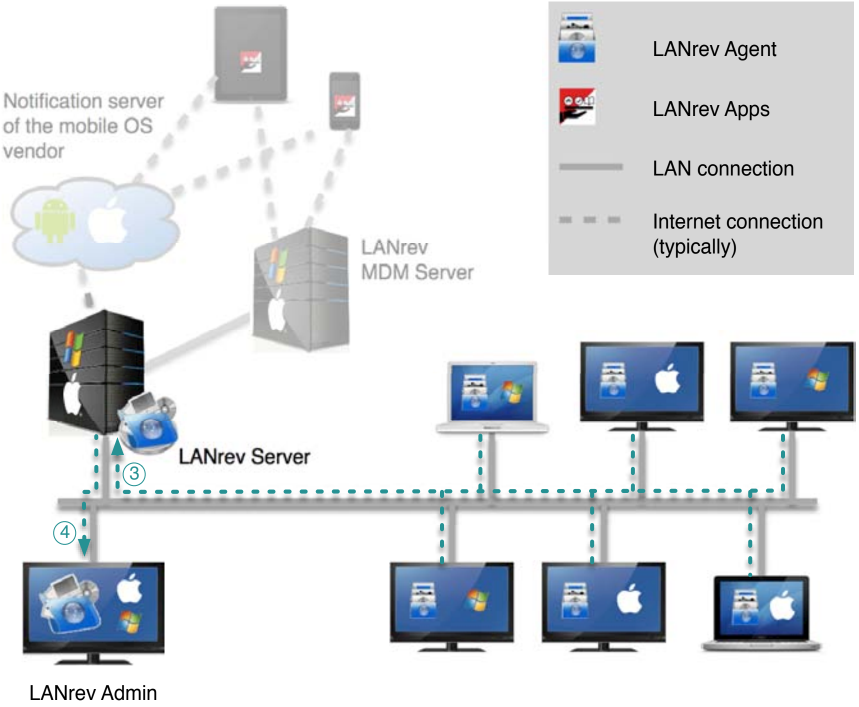
The basic principle of working with LANrev is the same for all commands (except for a software distribution and license monitoring, which are described separately in “Installing software” on page 293 and “Monitoring licenses” on page 348, respectively.)



When you issue a command to the LANrev system, the command is transmitted from your admin application to the server (1).

The server checks whether it needs additional information from the agents to complete the command or whether the command involves any agent actions. If neither is the case, the server does not contact the agents.

If, however, the agents need to be involved, the server sends them the appropriate commands (2). Commands may be sent to one, some, or all agents, depending on the command specification from the admin.



The contacted agents perform the appropriate tasks on their computers or collect requested information. They send back the results to the server (3) – either information on the client computer or at least feedback that the set task has been completed.

Any information on the client computers returned by the agents is stored by the server in its database for future reference.

If the original command (1) from the administrator requires the return of information, the server sends the requested information back to the admin (4), processing it first if required.

How software distribution and license monitoring work

Software distribution and license monitoring work in the same basic way described above, in that the admin communicates with the server and the server with the agents.

However, instead of sending commands to the server that are then forwarded to the agents, the admin merely sets up the server as required. Later on, the agents communicate on their own with the server, sending information and, in the case of software distribution, requesting software that is available for them.

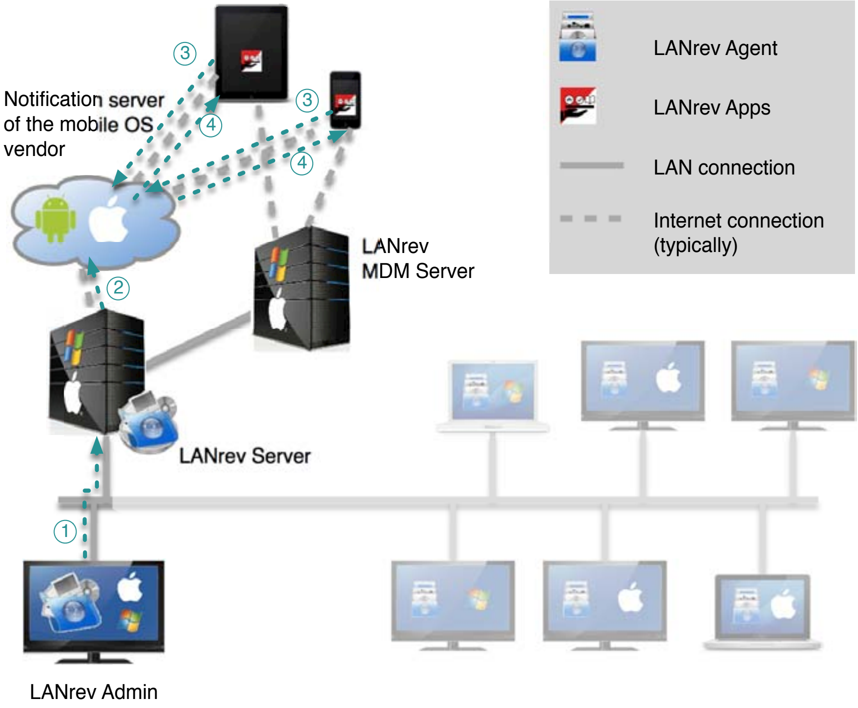
The admin is not involved in these exchanges beyond the initial setup and – if desired – the review of reports and logs.

An explanation of the principles and details of software distribution and license monitoring is available in "Installing software" on page 293 and "Monitoring licenses" on page 348, respectively.

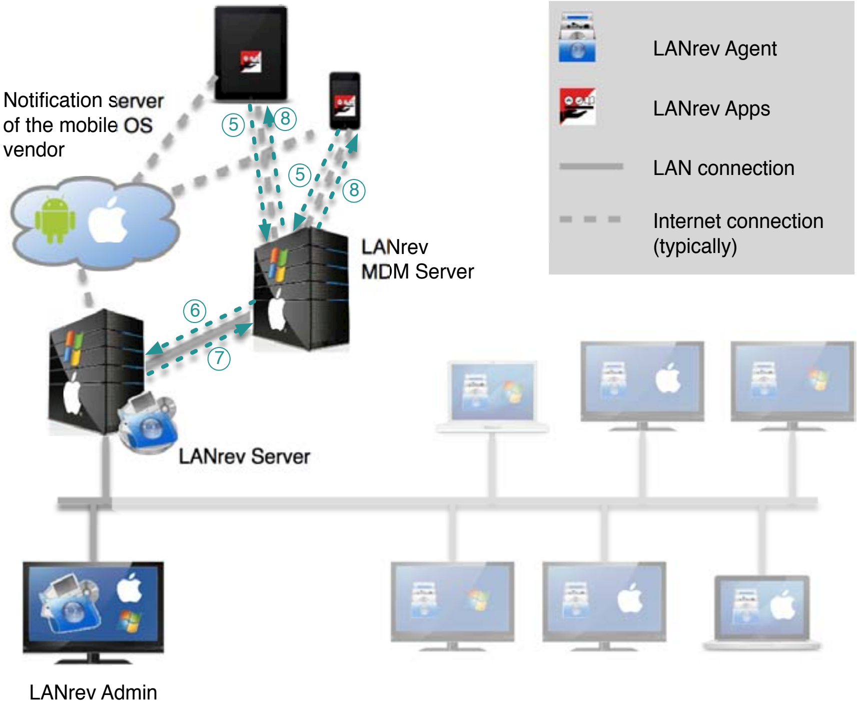
How managing mobile devices works

Mobile devices are managed in a similar way as desktop computers. However, there are some differences:

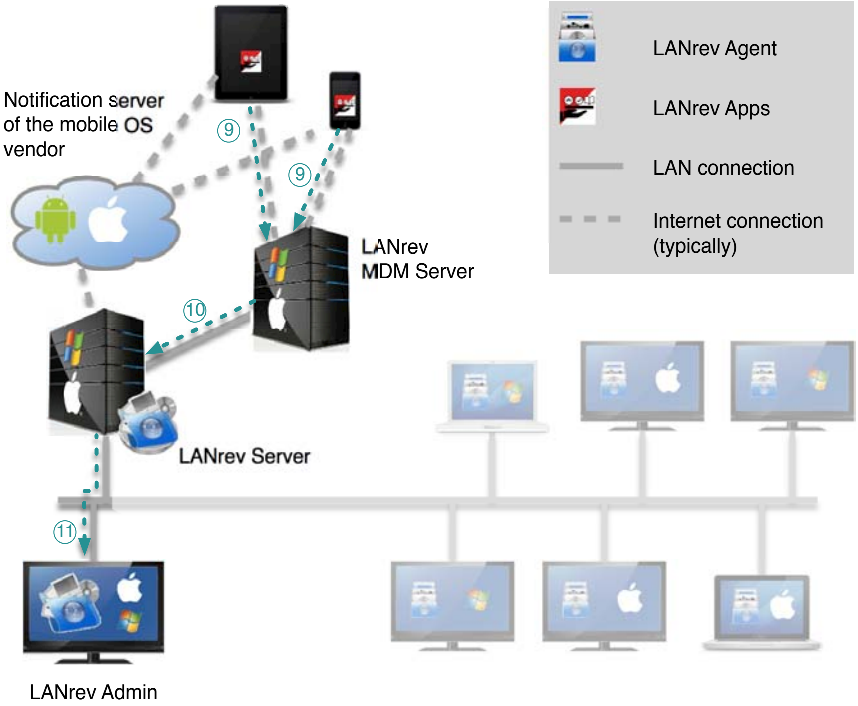
- The LANrev Server cannot contact the mobile devices directly. Instead, contact must be made through a notification server operated by the mobile OS vendor (Apple, Google or Microsoft) and an MDM server. The process for iOS and Android is described below; the one for Windows Phone differs slightly, as described in "Windows Phone" on page 8.



When an admin issues a command that involves mobile devices, it is first sent to LANrev Server (1). If that server determines that the commands require contacting mobile devices, it sends a contact request to OS vendor's notification server (2), which is regularly contacted by the mobile devices. When a device for which a request is pending next contacts the notification server (3), the contact request is forwarded to the LANrev client (LANrev Apps) running on the device (4).



The mobile device contacts the MDM server (5), which forwards the contact notice to the LANrev Server (6). The LANrev Server sends the command required to execute the original admin request (1) to the MDM server (7), which forwards it to the mobile device (8).



If the request requires a response by the device (for example, returning device status information), the response is sent to the MDM server (9), which forwards it to LANrev Server (10). When the data has arrived on that server, the admin can retrieve it (11).

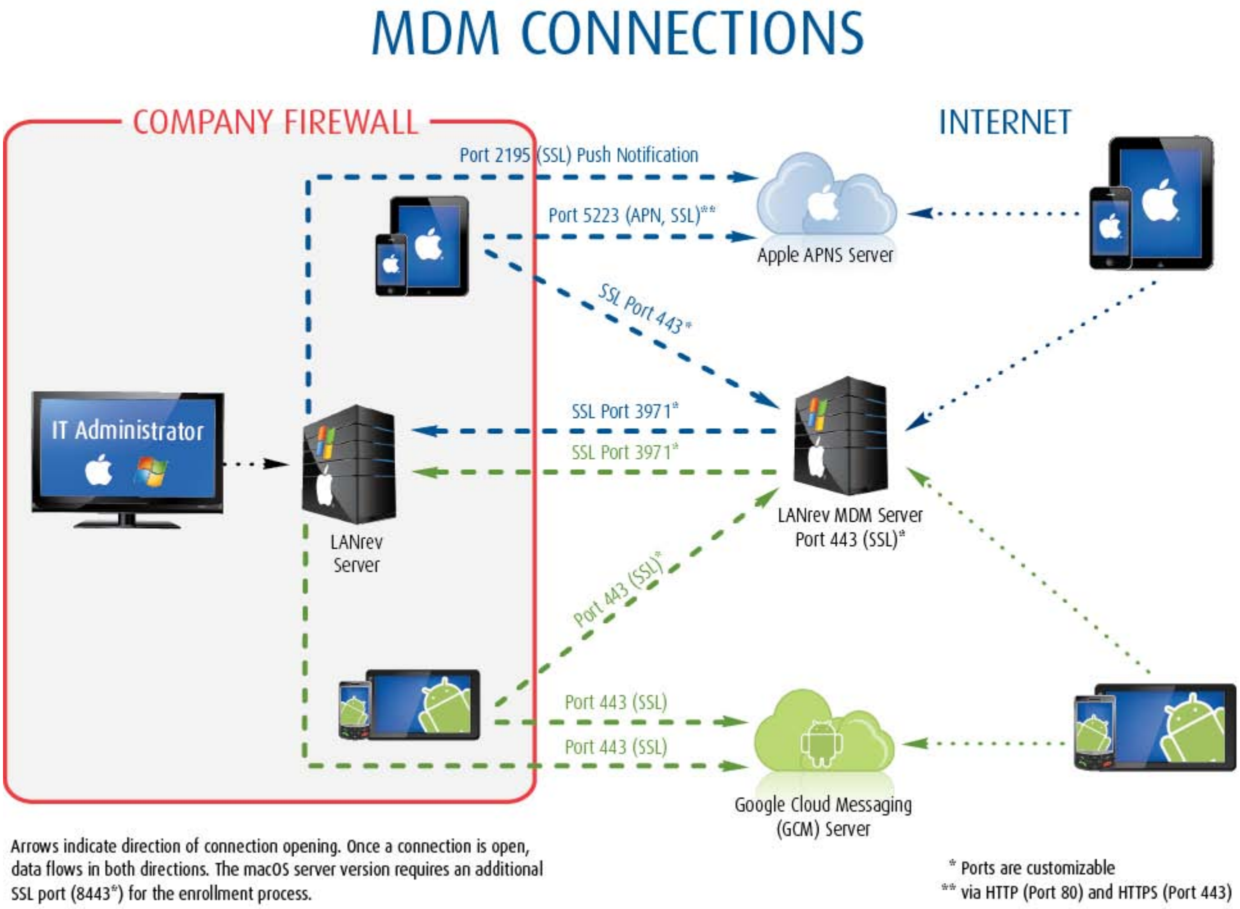
Windows Phone

The process for contacting managed Windows Phone devices is largely similar to the process described above, with these differences:

- Instead of a central notification server run by Microsoft, LANrev Server contacts the Exchange server to which the phone is synchronized.
- Except during the initial enrollment process, the LANrev MDM server is bypassed. Instead, the mobile device communicates with the Exchange server, which in turn communicates with LANrev Server.

Ports used

A number of different ports are used in this process:



Arrows indicate direction of connection opening. Once a connection is open, data flows in both directions. The macOS server version requires an additional SSL port (8443*) for the enrollment process.

* Ports are customizable
** via HTTP (Port 80) and HTTPS (Port 443)

This is an overview of the ports involved:

- LANrev Server

  - 3971* (also for connections to the administrator application and to local Agents, not shown)
  - 8443* (macOS server only)
- LANrev MDM Server
  - 443*
- Apple push notification server
  - 2195
  - 5223 via ports 80 and 443
- Google Cloud Messaging server
  - 443 (for LANrev Server)
  - 5228 (for Android devices in the intranet)

An asterisk (*) indicates ports that can be reassigned.

Ports for connections crossing the corporate firewall must be opened in the firewall to ensure proper operation of LANrev.

LANrev users

LANrev is used by two groups of people in very different ways:

- ‘Normal’ users – users of the administered devices – have no or very little interaction with LANrev.
- Administrators are the persons who actively use the system to manage remote devices.

Users

LANrev is transparent for users of administered devices. Neither is LANrev activity noticeable for them – except sometimes by its effects, such as new software being available on the device – nor is their active cooperation required for any of LANrev’s actions.

There are some exceptions to this:

- At the discretion of the administrator, users can be notified of some pending actions, such as restarts, that may affect their work. Furthermore, the administrator may give users the option to cancel these actions.
- Users may be given the option to view or edit certain bits of information (so-called client information) locally.
- Apps and media can be made available to users of managed mobile devices to be installed or viewed at their leisure. (Apps can also be installed without requiring any user action.)

Administrators

Administrators use the LANrev Admin application to manage client devices via the LANrev system.

Administrator access requires a password-protected account on the LANrev Server. This ensures both that LANrev cannot be used by unauthorized persons and that an administrator has the same use of LANrev no matter from where he or she accesses the system.

As a general rule, administrators do not have access to all client devices – they can manage only devices to which they have expressly been assigned in the LANrev system. (It is possible to configure individual administrator accounts so that they have access to all devices.)

There are two types of administrators:

- Standard administrators can perform any action that LANrev permits on the client devices to which they have been assigned. Optionally, their access to the assigned devices can be restricted to a specific list of functions.
- Superadministrators have access to all the same functions as standard administrators. In addition, they can create, configure, and delete administrator accounts and assign administrators to computers.

Details of managing administrator accounts are described in "Administrator accounts" on page 72.

Chapter 2 Installation

This chapter describes installing, updating, and uninstalling the components of the LANrev system.

For information on updating from earlier versions, see “Updating LANrev” on page 62.

Overview

LANrev should always be installed in the same order:

1. Server: First the LANrev Server is installed; it is the central element of the LANrev system without which it does not work.
2. Admin: Next, LANrev Admin is installed on at least one administrator workstation. As soon as it is installed, it is used to perform the initial configuration of the server, including entering the authorization code.
3. Agents: Finally, the LANrev Agents are installed. In many cases, this installation can be performed automatically using the LANrev system.

The installation procedures for all components are described below in this order.

Before you install

Before you begin the installation, these are some issues you might want to consider:

1. Check the system requirements (listed below).
2. Decide on a suitable server computer. Some relevant issues are discussed in “Choosing a computer for LANrev Server”, below the system requirements.
3. Decide whether to use the provided LANrev Agent installer or create a custom installer with preconfigured preferences.
4. Decide whether to use LANrev’s Agent Deployment Center to install LANrev Agent centrally on the administered computers.

   There must be suitable user accounts for remote installations:

   - macOS clients: SSH must be enabled and there must be an account for which you know the password.

- Windows clients: There must be an administrator account for which you know the password.

Note: Installation becomes even easier if the same account name and password can be used on all computers running the same operating system.

System requirements

System requirements for desktop software components:

Component	macOS	Windows
LANrev Server	macOS 10.6 or above	Windows Vista or Server 2003 or above On Windows Server 2016, PowerShell 2.0 or above is required.
Support for remotely reinstalling Windows computers	A LANrev PXE server or a FOG server in your network. FOG is open-source software running on Linux. The LANrev PXE server has the same requirements as LANrev Server. For the FOG server requirements, see www.fogproject.org. If FOG is used, an ODBC driver capable of connecting to the FOG MySQL server must be installed on the computer on which LANrev Server is running. The distribution points used to distribute the Windows disk images must run on Windows computers. Any Windows system on which LANrev Server is installed must include .NET 3.5.	

<table>
<tr><th>Component</th><th>macOS</th><th>Windows</th></tr>
<tr><td rowspan="2">MDM server for managing mobile devices</td><td colspan="2">A computer that can be reached from the Internet by HTTP and HTTPS connections. (This can be a computer on which LANrev Server is running or a separate computer.)
An SSL certificate for the computer on which you will be installing the MDM server. The certificate cannot be self-signed. (See step 1 of “Preparation” on page 26 for details.)</td></tr>
<tr><td>macOS 10.6 or above
Intel processor
Property List Editor utility (part of the macOS developer software)</td><td>Windows Server 2003, 2008 R2, 2012, or 2016
On Windows Server 2016, PowerShell 2.0 or above is required and HTTP/2 must be deactivated.
Microsoft Internet Information Services (IIS) 6.0 or above. The WebDAV Publishing role must not be installed.
ASP.NET 2.0
.NET 3.5</td></tr>
<tr><td>MDM for Windows Phone devices (in addition to the general MDM requirements above)</td><td>(Not available: Windows Phone MDM requires a Windows installation of LANrev Server.)</td><td>Exchange Server 2007 or Exchange Server 2010 (only one Exchange server is supported, which cannot be installed externally, for example, as part of Office 365)
PowerShell 2.0 or above</td></tr>
<tr><td>Support for NDES (Microsoft’s SCEP implementation)</td><td>(Not available: NDES support requires a Windows installation of LANrev Server.)</td><td>Windows Server 2008 R2 or 2012
Exchange Server 2007 or Exchange Server 2010
Java Runtime on the computer on which LANrev Server is running.</td></tr>
<tr><td>Support for Cisco ISE (both for mobile and desktop devices)</td><td colspan="2">Cisco ISE 1.2 or above. An MDM server must be available. See above for MDM system requirements.</td></tr>
<tr><td>LANrev Admin</td><td>macOS 10.10 or above
Screen with a resolution of at least 1440 by 900 pixels
For distributing Android apps, a Java runtime (JRE) is required.</td><td>Windows Vista or Server 2003 or above
Screen with a resolution of at least 1440 by 900 pixels
For distributing Android apps, a Java runtime (JRE) is required.</td></tr>
</table>

Component	macOS	Windows
InstallEase	macOS 10.7 or above Xcode 3.2.5 through 4.6.3 (only for PKG support) Iceberg 1.2.2 or above (only for Iceberg project support)	Windows Vista or Server 2003 or above Microsoft .NET 3.5 SP 1
LANrev Agent (Linux requirements are described below this table)	macOS 10.5 or above Intel processor (Agent 4.0.4 for macOS 10.2 or above, Agent 4.5.1 for macOS 10.3 or above, Agent 6.1.5 for macOS 10.3.9, Agent 6.7.1 for macOS 10.4 or above; with reduced functionality Agent 6.1.3 for PowerPC-based Macintosh computers; with reduced functionality)	Windows XP or Server 2003 or above For reporting disk encryption information, .NET 2.0 or .NET 3.5 is required on Windows XP and 8, and Server 2003 and 2012.
LANrev Remote	macOS 10.5 or above Intel processor	Windows Vista or Server 2003 or above

Features requiring MDM

Certain features require an MDM server to be installed:

- Storing the FileVault recovery key and retrieving it, for example, for remotely unlocking a target computer.
- Locking and erasing macOS computers.
- Support for Apple’s volume purchase program (VPP).
- Support for Apple’s device enrollment program (DEP). This feature requires MDM running on Windows.
- Enrolling computers in MDM. (For computers running OS X 10.9 Mavericks, this feature requires MDM running on Windows.)
- Managing mobile devices, that is, devices running iOS, Android, or Windows Phone.
- Using the Web Admin and the self-service portal.

Linux system requirements

LANrev Agent for Linux requires any of these Linux distributions:

- CentOS 6.4
- Debian 7 “Wheezy”
- Fedora 18 or 19
- Mint 15
- Ubuntu 12.04 LTS, 12.10, or 13.04

Furthermore, to install the Agent for Linux, LANrev Admin must be running on macOS 10.8 or above. This requirement concerns only the initial installation, not the later operation of the Agent for Linux. For an overview of the provided functionality, see “Functionality of LANrev Agent for Linux” on page 45.

System requirements for mobile components

Component	iOS	Android	Windows Phone
LANrev Apps	iOS 6.0 or above For iOS 4.x and 5.x, LANrev Apps is available from the Resource Center.	Android 2.3.3 or above	(not available)
LANrev Find	iOS 6.0 or above	(not available)	(not available)
LANrev Remote	(not available)	Samsung SAFE 2.1 or above	(not available)
LANrev Safe	iOS 6.0 or above	Android 3.0 or above	(not available)
Samsung KNOX support	(not available)	Samsung KNOX 1.1 or above	(not available)

All LANrev components also require a working IP network connection. The built-in firewalls of macOS and Windows are fully supported.

Windows and macOS components can be freely mixed between the platforms; for example, an admin running on Windows can control a server running on macOS to work with agents running on Windows.

Choosing a computer for LANrev Server

LANrev Server does not technically have special requirements beyond the system requirements listed above. However, some aspects should be considered when choosing a computer on which to install LANrev Server:

- Dedicated server: To maximize operational reliability of the LANrev system, it is helpful to install the server application on a computer that is not used as a workstation (that is, worked on by a local user).
- Network bandwidth: When LANrev is used to administer a large number of computers, there may be substantial network traffic from and to the server at peak times. In such cases, it is helpful to have as much bandwidth as possible, for example, by providing a high-bandwidth link to the switch.
- Processor power and disk space: LANrev Server has no special requirements regarding processor power or disk space. Any modern computer should more than suffice. Note, though, that database operations require processor power in proportion to the number of administered computers. Also, the more administrators are active at the same time, the more processor power is required.

- Other server processes: Other server processes running on the same computer as LANrev Server are not normally a problem. However, if they put a strain on resources – in particular processor power and network bandwidth – they may impair the performance of LANrev.

Installing LANrev Server

For the system requirements of LANrev Server, see “System requirements” on page 12.

Installing LANrev Server on macOS

To install LANrev Server on a macOS computer:

1. Copy the LANrev Server installation package to the hard disk of the computer on which you want to install the server.

2. Open the installation package and follow the on-screen instructions.

There is no need to restart the server computer after the installation.

Installing LANrev Server on Windows

To install LANrev Server on a Windows computer:

1. Copy the LANrev Server installation folder to the hard disk of the computer on which you want to install the server.

2. Open the folder and double-click the **Setup** application

3. Follow the on-screen instructions.

After the installation

When you are done installing the server, you should immediately install LANrev Admin and configure the server.

NOTE When you are transferring a server from computer to another (as opposed to setting up a server for the first time), you can import the settings from the existing server, as described in “Exporting and importing server settings” on page 91.

After installing the admin, you can optionally install two additional components:

- Support for remotely reinstalling Windows computers, as described in “Installing support for reinstalling Windows computers” on page 22.
- Support for managing mobile devices (iOS or Android), as described in “Installing MDM support” on page 26.

Installing LANrev Admin

For the system requirements of LANrev Admin, see "System requirements" on page 12.

After you have installed it, you should immediately launch it to authorize and configure LANrev Server.

Installing LANrev Admin on macOS

Copy the LANrev Admin application file to a suitable place on your hard disk (for example, the **Applications** folder).

If you are planning on managing application packages for Android mobile devices, a Java runtime environment (JRE) is required. Versions of macOS up until 10.6.x include an JRE, but newer versions, starting with 10.7 (Lion), do not. At the time of this writing, Apple provides a JRE for installation on Lion at http://support.apple.com/downloads/#Java.

NOTE You can also install LANrev Admin on a USB stick to take with you for mobile diagnoses. The application is fully functional when so installed; the only limitation is that it reverts to default **Preferences** dialog settings and window positions when used on a different computer.

Installing LANrev Admin on Windows

To install LANrev Admin on a Windows computer:

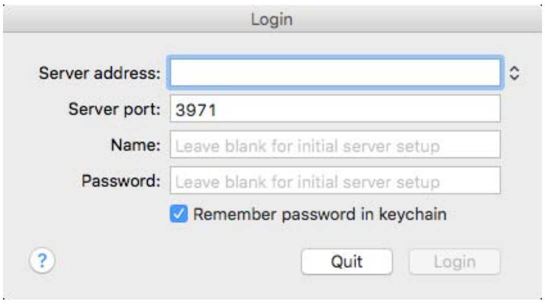
1. Copy the LANrev Admin installation folder to the hard disk of your computer.
2. Open the folder and double-click the **Setup** application
3. Follow the on-screen instructions.

Initial configuration of LANrev Server

After you have installed the first copy of LANrev Admin, you should start it immediately to configure the server. (Additional copies of LANrev Admin that you install can simply log in when the server has been configured and accounts been set up.)

This process involves specifying the LANrev Server and then entering registration and initial setup information in a setup wizard:

1. Start LANrev Admin. The **Login** dialog opens:



Server address:
Server port: 3971
Name: Leave blank for initial server setup
Password: Leave blank for initial server setup
☑ Remember password in keychain

2. Enter the server address – you can enter the IP number or a DNS name if the server computer has one.

   The pop-up menu beside the **Server address** field provides access to the most recently used servers.

   The port number should not normally be changed; however, if you have configured the server to use a different port number, enter that number.

   Do not enter a name or password.

3. Click **Login**.

   You are asked to verify the server identity. For security reasons, LANrev uses SSL certificates to identify all components. When you contact a server for the first time, LANrev Admin asks you to verify that the certificate that it presents indeed belongs to the server you want to contact (instead of, for example, a malicious server used for a man-in-the-middle attack).

4. Display the server certificate as described in “Displaying a server’s certificate” on page 19.

5. If the fingerprint of the certificate and the unique server identifier match the information in the LANrev Admin’s verification dialog, click **Connect**.

   The LANrev Setup wizard opens.

6. Start with entering your and your company’s names as well as the serial number and activation key that you have received with your copy of LANrev.

   Note: You can run LANrev as a demo by clicking the demo button. In this case, you are limited to ten clients and the software will stop working after 45 days.

7. Specify the ports that the server is to use for communicating with agents and with LANrev Admin.

You can use the same ports for both agents and LANrev Admin. Different ports are recommended when you place a LANrev Server in a demilitarized zone for access from the Internet, as explained in "Setting up computer tracking" on page 164

LANrev Server opens the specified ports in the built-in macOS or Windows firewall on its computer if the firewall is active.

Note: We recommend that you change the ports only when you have a specific need to do so.

8. If you do not want to create administrator accounts on this server but instead want to use existing accounts on another LANrev Server, check **Use administrator accounts from server** and specify the desired server.

   Note: If you use accounts from another server, you will not be prompted to create an initial account as described below.

   Click the **Set** button to open the SSL certificate for the specified server. (See "Exporting a server certificate" on page 21 for information on creating a certificate file.)

9. Create an initial superadministrator account for yourself.

   Note: Details of creating accounts are described in "Administrator accounts" on page 72.

When you finish the wizard, it sets up the server as specified and launches LANrev Admin, opening an empty browser window. Both LANrev Server and LANrev Admin are now installed.

Continue the installation process:

- If you want LANrev to be able to remotely reinstall Windows computers, continue with "Installing support for reinstalling Windows computers", below.
- If support for reinstalling Windows clients is not required but you want to use LANrev to administer mobile devices, continue with "Installing MDM support", below.
- If neither of these capabilities is required, continue with installing LANrev Agent on all computers that are to be administered, as described in "Installing LANrev Agent" on page 35.

Displaying a server's certificate

To ensure that it communicates only with the intended server, LANrev Admin uses SSL certificates.

When it contacts a server for the first time or when the server's certificate has changed (for example, after the server was reinstalled), you must verify that the presented certificate does indeed belong to the server it claims to identify.

To verify a certificate, you compare the fingerprint and server unique identifier that LANrev displays with the corresponding values you obtain from the server:

1. The procedure normally begins with LANrev displaying a verification dialog.

   Leave the dialog open on the admin workstation.

2. Go to the server computer.

   While it is possible to obtain the server certificate information remotely, doing so is less secure than physically accessing the server computer.

3. Depending on the platform, execute a command line instruction:

   - On a macOS server, launch the Terminal application and enter this command (on a single line): "/Library/Application Support/LANrev Server/LANrev Server.app/Contents/MacOS/LANrev Server" –ShowCertificateFingerprint
   - On a Windows server, launch the Command Prompt application and enter this command (on a single line): "C:\Program Files\Pole Position Software\LANrevServer\LANrev Server.exe" –ShowCertificateFingerprint (On x64 systems, use "C:\Program Files (x86)\…" instead.)

   Note: If you use --ShowCertificate instead of --ShowCertificateFingerprint, additional information is displayed, including the server's unique identifier. However, this is usually not needed, as the identifier is also part of the certificate and thus covered by the fingerprint verification.

   The certificate fingerprint is displayed.

4. Copy or write down the fingerprint and return to the admin workstation.

5. Compare the fingerprint you obtained from the server with the fingerprint displayed by LANrev Admin:

   - If the two fingerprints do not match, the server to which LANrev Admin is about to connect is not the server from which you obtained the fingerprint.
     Make sure that the server address LANrev Admin uses is correct. If the address is correct, there may be an attempt to compromise your LANrev installation by having another server masquerade as your server.
     Do not continue the connection! Doing so could severely compromise the security of your network.
   - If the two fingerprints match, click the **Connect** button in the verification dialog.

Exporting a server certificate

For security reasons, the individual components of LANrev (servers, administrator applications, and agents) require SSL certificates to verify the identities of other components with which they communicate.

This means that you must specify a certificate for any server that you assign to an agent (for example, as an inventory server). You can do so either by exporting a certificate from LANrev Admin or by copying the certificate file from the server computer. Both methods are described below.

Exporting a certificate in LANrev Admin

To create the required certificate for a server:

1. Make sure that your admin application is connected to the desired server.

   Connecting to a different server is described in “Switching accounts” on page 78.

1. In LANrev Admin, choose **Window** > **Server Center**.

   The **Server Center** window opens.

2. Click the **Server Settings** entry in the sidebar and click the **Save Certificate** button in the lower left of the window.

   A standard Save dialog opens.

3. Save the server certificate in a convenient location. You can give it any desired name.

Use this file whenever you are required to provide a certificate for a server that you want to assign to agents.

Copying a certificate from the server computer

After LANrev Server has been launched for the first time (which happens as part of the installation), it saves a copy of its certificate in it application support folder:

- macOS: /Library/Application Support/LANrev Server/Server Certificate.pem
- Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\Server Certificate.pem
- Windows Vista and above, Windows Server 2008 and above: C:\ProgramData\Pole Position Software\LANrev Server\Server Certificate.pem

Copy the certificate file from this location to the computer where it is needed.

Installing support for reinstalling Windows computers

Support for remotely reinstalling Windows computers from LANrev Admin requires the installation of additional components.

NOTE Remote reinstallation of macOS computers is supported out-of-the-box by LANrev. If you need to be able to remotely reinstall macOS computers but not Windows computers, you can skip this procedure.

LANrev offers two ways for supporting reinstalling Windows computers: With the included solution for a Windows PXE server, or with the popular FOG Linux server solution.

Both are described below in:

- "Setting up the LANrev PXE solution" on page 22
- "Setting up the FOG solution" on page 24

Setting up the LANrev PXE solution

To set up the LANrev PXE support for reinstalling Windows computers:

1. Set up your LANrev servers for software distribution, as described in "Setting up distribution points" on page 296.

   Note that Windows reinstallation requires distribution points running on Windows computers for distributing the disk images.

2. Create a reinstallation disk image.

   This disk image is based on the Microsoft Automated Installation Kit but includes additional files needed by LANrev. You can find these files and instructions for building the disk image online at http:/www.heatsoftware.com/support.

3. In LANrev Admin, choose **Window** > **Server Center** to open the Server Center.

4. Right-click in the sidebar and choose **Software Distribution** > **New Disk Image** from the context menu to upload the boot disk image.

   In the **Disk Image** dialog that opens, specify:

   - **Disk image name**: AMWinPE
   - **Disk image file**: Click **Select** and choose the disk image file you created in step 2.
   - **Disk image password**: not applicable
   - **Distribution point**: Choose the desired option. If you are unsure, choose **Any**.

   Click **OK** to upload the image.

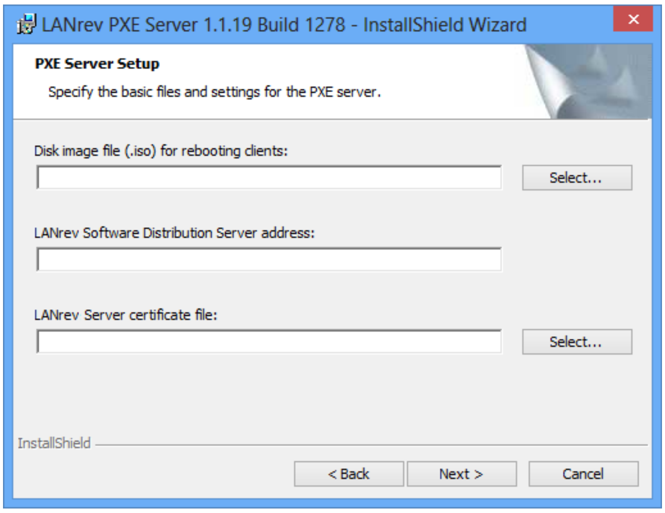
5. Export the LANrev Server certificate, as described in “Exporting a server certificate” on page 21.

6. Launch the PXE server installer.

   This installer is included with the LANrev Windows installer in the “LANrev PC Imaging PXE Server” folder.

   Note that the PXE server must not be installed on the computer that is used as the DHCP server.

7. Follow the instructions on screen until you reach the setup screen:



LANrev PXE Server 1.1.19 Build 1278 - InstallShield Wizard

PXE Server Setup

Specify the basic files and settings for the PXE server.

Disk image file (.iso) for rebooting clients:
Select...
LANrev Software Distribution Server address:
LANrev Server certificate file:
Select...
InstallShield
< Back
Next >
Cancel

8. Specify this information:

   - **Disk image file**: The disk image you created in step 2. *Note: This image is (in certain circumstances) required to boot a Windows computer that is about to be reinstalled and is not used as the source for the new installation on the computer. (You specify a different disk image in the Reinstall Windows Computer command dialog.) Do not modify the contents of this image.*
   - **LANrev Software Distribution Server address**: The IP adress or fully qualified DNS name of the LANrev Server in you network on which the disk image is located.
   - **LANrev Server certificate file** The certificate file you have exported in step 5.

9. Click **Next** and continue to follow the on-screen instructions.

10. Configure the DHCP server to allow network booting from the PXE server. (The following instructions apply to a Windows Server 2003 Enterprise Edition; adapt them as necessary for other servers.)

    - Open the DHCP server console.
    - Display the scope options.
    - Right-click anywhere in the list of options and choose **Configure Options** from the context menu.

- Set option “066 Boot Server Host Name” to the IP address of the PXE server you have installed in the previous steps.
- Set option “067 Bootfile Name” to “pxelinux.0” (without the quotes).
- Save the changed options and close the server console.

11. Make sure that the client Windows computers are not set to boot from the network.

LANrev now supports remotely reinstalling Windows computers.

Continue the installation process:

- If you want to use LANrev to administer mobile devices, continue with “Installing MDM support”, below.
- Otherwise, continue with installing LANrev Agent on all computers that are to be administered, as described in “Installing LANrev Agent” on page 35.

Setting up the FOG solution

To set up the FOG support for reinstalling Windows computers:

1. Install the FOG server and configure it.

   For details, see the FOG documentation. The FOG software and documentation is available from www.fogproject.org.

   In particular:

   - Configure the FOG server to have a static IP address.
   - Configure DHCP to use FOG.

2. Configure MySQL for network access.

   For details, see the FOG documentation and MySQL documentation for your platform, as required.

3. If you have installed LANrev Server on a Windows computer, install .NET 3.5, if it is not already present.

   Skip this step when you have installed LANrev Server on macOS. Also, you do not need to upgrade any computers running LANrev Admin (but not Server) to .NET 3.5.

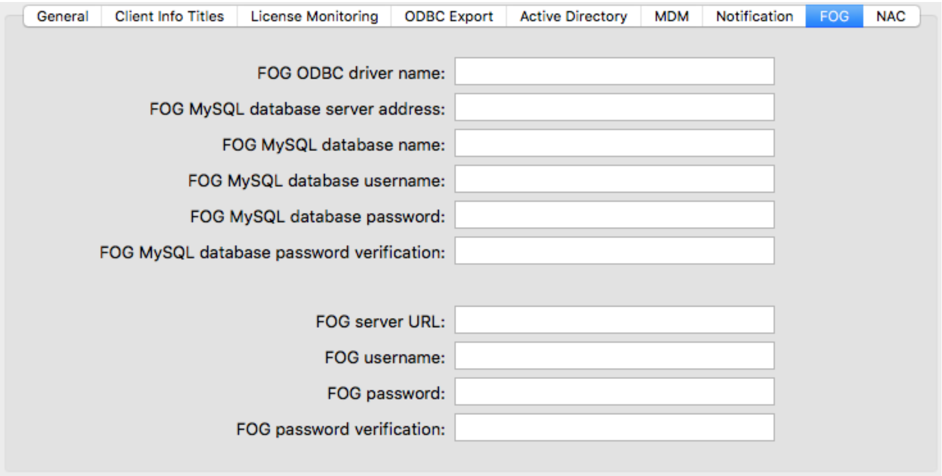
4. Make sure that, on the LANrev Server computer, an ODBC driver capable of accessing the MySQL database used by FOG is installed.

   If no such driver is present, install it.

Setting LANrev Server up for FOG support

Reinstalling Windows computers requires a one-time setup of LANrev Server to allow it to control the FOG server:

1. In LANrev Admin, open the Server Center, click **Server Settings**, and click the **FOG** tab:



2. Fill in the required information to access the MySQL database that FOG uses:

    - Enter the name of the ODBC driver on the LANrev Server computer that LANrev is to use to access the MySQL database in **FOG ODBC driver name**.
    - Enter the IP address or DNS name of the MySQL server in **FOG MySQL database server address**.
    - Enter the name of the MySQL database that FOG uses in **FOG MySQL database name**.
    - Enter your access credential for the MySQL database in **FOG MySQL database username**, in **FOG MySQL database password**, and **FOG MySQL database password verification**.

3. Fill in the required information to access the FOG server:

    - In **FOG server URL**,enter the IP address or DNS name of the FOG server and the path of the FOG server management directory, for example, “http://myfogserver.company.com/fog/management/”.
    - Enter your access credential for the MySQL database in **FOG username**, in **FOG password**, and **FOG password verification**.

4. Choose **Server** > **Save Server Settings**.

You have now configured LANrev to allow reinstallation of administered Windows computers, as described in “Reinstalling a Windows computer” on page 340.

If there are already disk images on the FOG server, you can verify the correctness of the setup by choosing (in LANrev Admin) **Commands** > **Reinstall Windows Computer**. If LANrev can properly access the FOG server, the disk images are visible in the **Image** pop-up menu.

LANrev now supports remotely reinstalling Windows computers.

Continue the installation process:

- If you want to use LANrev to administer mobile devices, continue with “Installing MDM support”, below.
- Otherwise, continue with installing LANrev Agent on all computers that are to be administered, as described in “Installing LANrev Agent” on page 35.

Installing MDM support

Support for managing mobile devices from LANrev requires the installation and configuration of an MDM (mobile device management) server.

The MDM server is also required if you plan to offer enrollment for desktop devices (instead of manually installing or push-installing the Agent), as described in “Enrolling computers using the MDM server” on page 45.

The requirements for the MDM software are listed in “System requirements” on page 12.

There are three installation steps, with a fourth step required only if you plan to manage Windows Phone devices:

- Preparation
- Installing the MDM server
- Configuring the MDM server
- Configuring the Exchange server

Managing a mobile device also requires it to be enrolled in the MDM administration. This is described later in “Enrolling mobile devices” on page 50.

Preparation

1. Obtain an SSL/TLS certificate for the computer on which you will be installing the MDM server.

   The certificate must come from a root certification authority (CA) or signed by a CA with authorization from a root CA. In the latter case, you also need the signer certificate of the CA.

   The certificate must either be a wildcard certificate for the domain under which the computer on which the MDM server will be installed can be reached from the Internet (for example, *.mycompany.com) or specific to the server’s DNS name.

2. Set up your firewall to allow connections from your LANrev Server to the notification servers of Apple and Google, respectively:

   - gateway.push.apple.com on port 2195 for iOS devices
   - android.apis.google.com on port 443 for Android devices

   If you do not manage a particular kind of device, you do not need to allow the corresponding connection. (For example, if you do not manage iOS devices, you do not need to allow connections to gateway.push.apple.com.)

   For a full overview of the ports involved, see "Ports used" on page 8.

Continue with "Installing the MDM server", below.

Installing the MDM server

The installation process differs slightly between Windows and macOS. Both processes are described in separate sections below.

Installing the MDM server on Windows

1. From LANrev Admin, export the certificate of the LANrev Server, as described in "Exporting a server certificate" on page 21.

2. Run the Setup.exe application from the "LANrev MDM Server" folder.

   You are guided through the installation.

3. When prompted for the website SSL certificate, choose the certificate described in step 1 of the "Preparation" procedure, above.

4. When prompted for the LANrev Server certificate, use the certificate you exported in step 1 of this procedure.

   As the DNS address, provide the fully qualified domain name, i.a., the name including the top-level domain. For example, use "mdm.mycompany.com" (instead of just "mdm").

   As explained in "Preparation", above, this can be the computer on which LANrev Server is running but does not have to be.

After you have installed the MDM server, continue with "Configuring the MDM server", below.

Installing the MDM server on macOS

1. Run the provided installer package.

2. By default, MDM communications use port 443. If you want to use a different port, edit the "server.port" entry in the /private/etc/lighttpd/lighttpd.conf file.

3. Copy the SSL certificate for the MDM server (see step 1 of "Preparation") to /etc/lighttpd/certs on the MDM server computer and name it "lighttpd.pem".

   If you have received a certificate that does not contain the SSL private key (for example, a certificate in .p12 format), you must convert it to include the key, as described in "Importing the SSL key into the certificate", below.

4. From LANrev Admin, export the certificate of the LANrev Server, as described in "Exporting a server certificate" on page 21.

5. Copy this certificate to /etc/lighttpd/certs on the MDM server computer and name it "TrustedCertificates.pem".

   As explained in "Preparation" on page 26, this can be the computer on which LANrev Server is running but does not have to be.

6. If the certificate was signed with an intermediate certificate (as opposed to a CA root certificate), append the content of the intermediate certificate to the content of your certificate.

   You can do so, for example, by executing the command

   ```
   cat IntermediateCA.pem >> TrustedCertificates.pem
   ```

   (This assumes that your intermediate certificate is named IntermediateCA.pem.)

7. On the computer on which the MDM server is installed, open the /Library/Preferences/com.heatsoftware.LANrevMDMServer.plist file (using the Property List Editor utility) and enter in the LANrevServerHostname key the IP address or DNS name of the LANrev Server.

8. On the computer on which the MDM server is installed, run the Start_MDM_Server.command shell script provided on the LANrev installation disk.

   This starts the MDM server.

Continue with "Configuring the MDM server", below.

Importing the SSL key into the certificate

If you have received an SSL certificate that does not contain the SSL private key (for example, a .p12 certificate), you must convert it. This procedure is not required if you already have a .pem certificate.

1. Import the certificate into the macOS Keychain, for example, by dragging it into the main window of Keychain.

2. Export the certificate and key to disk in Personal Information Exchange (.p12) format.

3. Convert the resulting file to Privacy Enhanced Mail (.pem) format using the ConvertSSLCertificate.command script provided in the Extras folder on the LANrev installation image.

Configuring the MDM server

The MDM server is configured from LANrev Admin. Configuration is required only for managing iOS devices, not for Android devices.

1. If you plan to make users agree to a legal agreement as part of the enrollment process, copy the agreement as an HTML file to the LANrev Server application support folder:

   - macOS: /Library/Application Support/LANrev Server/
   - Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\
   - Windows Vista and above, Windows Server 2008 and above: C:\ProgramData\Pole Position Software\LANrev Server\

   Different agreements can be presented for different types of devices.

   For desktop devices:

   - DesktopEnrollmentLegalAgreement_PersonalDevice.html: For personal devices
   - DesktopEnrollmentLegalAgreement_CompanyDevice.html: For company devices
   - DesktopEnrollmentLegalAgreement_GuestDevice.html: For guest devices
   - Additional legal agreements can be displayed for custom device
   - DesktopEnrollmentLegalAgreement.html: The default agreement for desktop devices.

   For mobile devices:

   - DesktopEnrollmentLegalAgreement_PersonalDevice.html: For personal devices
   - DesktopEnrollmentLegalAgreement_CompanyDevice.html: For company devices
   - DesktopEnrollmentLegalAgreement_GuestDevice.html: For guest devices
   - DesktopEnrollmentLegalAgreement.html: The default agreement for desktop devices.

   You can provide some or all of these agreements; LANrev searches for them in the order given above until it finds a matching agreement and displays that. If no matching agreement is found, enrollment proceeds without an agreement being presented to the user.

2. In LANrev Admin, open the Server Center, display the server settings, and click the **MDM** tab.

3. Enter this information:

- **Profile name**: A descriptive name for the deployment profile. This name will be displayed on iOS devices during the enrollment process.
- **Profile identifier**: A unique identifier for the profile. It is needed to distinguish it from other profiles you may create on the server.
- **Description**: A brief explanation of the profile's purpose. It is displayed on the iOS device in the first screen of the enrollment process.
- **MDM server**: The full DNS name of the server on which you have installed the MDM server.
- **Port**: The port over which the MDM server communicates. By default, this is 443, but if you have edited the server port in step 2 of "Installing the MDM server", you must specify the custom port here as well.
- **Microsoft Exchange Server**: If you do not want to set up MDM for Windows Phone devices now, choose **None** and continue with step 4. Otherwise, choose the version of the Exchange server you have installed.
- **Exchange server**: Enter the IP address or fully qualified DNS name of the Exchange server.
- **Username**: Enter the username of an account on the Exchange server. Depending on the version of Exchange you are using, the account must have certain privileges.
  Exchange 2007 accounts must have all of these privileges:
  - View-only administrator
  - Recipient administrator
  - Organization administrator
  - Server administrator
  - Local administrator (for the Exchange server used)

  Exchange 2010 accounts must have all of these privileges:
  - Server management
  - Organization management
  - Recipient management

  Irrespective of the Exchange version, the account you specify must be a member of the Admin group on the computer on which LANrev Server is running.
- **Password**: The password for the specified account.

4. Click the **Configure** button in the **Certificates** section.

   The Push Service Certificates dialog opens.

5. Click the **Configure** button at the upper right of the panel and let the assistant guide you through the creation of a new push notification certificate.

   If you already have this certificate, the assistant lets you select it.

6. Select an MDM profile signing certificate and, if needed, an accompanying intermediate certificate.

   While enrollment will work without these certificates, users of enrolling devices will encounter alerts about untrusted certificates in the process.

Whether you need to specify an intermediate certificate depends on how the certificate was created. In case of doubt, contact the issuing authority.

7. Choose **Server** > **Save Server Settings**.

8. Make sure to open the required ports in your firewall. (The following assumes that the MDM server is outside the firewall, as recommended.)

   For outgoing connections:

   - 443* (This port can be reassigned for contacting the MDM server but not for contacting the Android notification server.)
   - 2195 (Not needed if you do not want to manage iOS devices.)
   - 5223 (Not needed if you do not want to manage iOS devices.)

   For incoming connections:

   - 3971*

   Functions marked with an asterisk can be reassigned to other ports. If you have done so, open the customized ports in your firewall instead. (Note that you always must open port 443 for outgoing connections if you want to manage Android devices.)

   See “Ports used” on page 8 for more information on port usage.

If you plan on managing Windows Phone devices, continue with setting up the Exchange server as described below.

Otherwise, continue with installing LANrev Agent on all computers that are to be administered as described in “Installing LANrev Agent” on page 35.

Configuring the Exchange server

To allow LANrev to administer Windows phone devices, additional setup steps are necessary:

1. If PowerShell 2.0 is not available on the computer on which LANrev Server is running, install it.

2. When you are using Exchange 2007, install the Exchange 2007 Management Tools on the computer on which LANrev Server is running.

   If you are using Exchange 2007, you are now done with the setup and can skip to the end of the procedure.

3. If you are using Exchange 2010, continue with this procedure. Enable access to the PowerShell virtual directory:

- Open Server Manager for the Exchange server.
- Click **Roles** > **Web Server** > **Internet Information Server**.
- Click **Sites** > **Default Web Site**.
- Click the virtual directory **PowerShell**.
- Open the authentication settings and set **Windows Authentication** to **Enabled**.

4. Enable the Windows Remote Management (WinRM) service:

    - On the computer running the Exchange server, start PowerShell.
    - Enter `winrm quickconfig`.
    - Accept all proposed settings by pressing `Y`.

5. Export the SSL certificate of the Exchange server:

    - Open the IIS Manager on the computer on which the Exchange server is running.
    - Click the server's entry and click **Server Certificates**.
    - Open the view pane for the certificate you want to export, click **Details** and click **Copy to File**.
    - Follow the on-screen instructions to export the certificate to a file.

6. Add the Exchange server's SSL certificate to the LANrev server:

    - On the computer running the LANrev server, open the mmc.exe management console.
    - In the console, choose **File** > **Add/Remove Snap-in**.
    - In the **Add/Remove Snap-in** window, click **Add**.
    - Choose **Certificates** and click **Add**.
    - Choose **Computer Account** and click **Next**.
    - Choose **Local computer** and click **Finish**.
    - Close the **Add Standalone Snap-in** and **Add/Remove Snap-in** windows.
    - In the **Console Root** window, right-click **Certificates (Local Computer)** > **Trusted Root Certification Authorities** > **Certificates** and choose **All Tasks** > **Import** from the context menu.
    - Follow the steps of the wizard to import the SSL certificate of the Exchange server.

If you want to enable support for SCEP (Simple Certificate Enrollment Protocol), continue with "Installing LANrev Agent", below.

Otherwise, continue with installing LANrev Agent on all computers that are to be administered as described below.

Setting up SCEP (NDES) support

You can set up LANrev so that you can enable mobile devices' SCEP (Simple Certificate Enrollment Protocol) access by simply assigning a configuration profile.

The requirements for the SCEP support are listed in “System requirements” on page 12.

To set up SCEP support:

1. Make sure that MDM support is set up, as described in “Installing MDM support” on page 26.

2. LANrev requires NDES (Microsoft’s SCEP implementation) for SCEP support. On the NDES server, configure an account for LANrev Server.

   See the NDES documentation for details.

3. In Active Directory, configure an account with administrator privileges for LANrev Server.

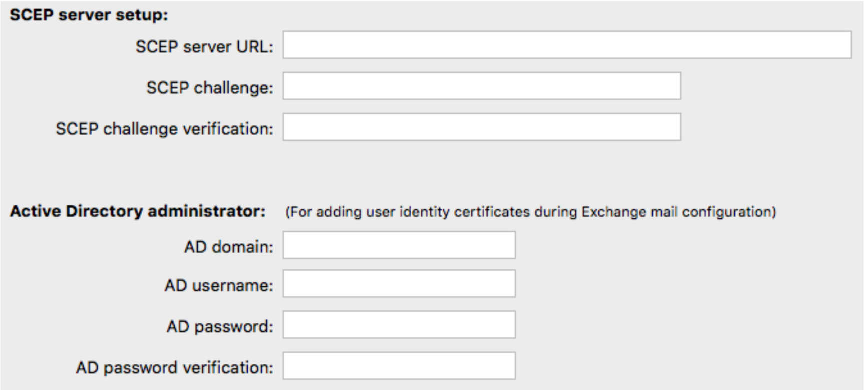
   See the Active Directory documentation for details.

4. Configure the Exchange server to support authentication through certificates.

   See the Exchange documentation for details.

5. In LANrev Admin, choose **Window** > **Server Center** and click **Server** > **Certificate Settings** in the sidebar.

   The settings needed to specify the SCEP access are displayed in the main part of the Server Center window.



SCEP server setup:

SCEP server URL:

SCEP challenge:

SCEP challenge verification:

Active Directory administrator: (For adding user identity certificates during Exchange mail configuration)

AD domain:

AD username:

AD password:

AD password verification:

6. Specify the NDES and Active Directory access settings (from the accounts set up in step 2 and step 3, respectively).

Enabling managed mobile devices to authenticate themselves with certificates requires setting up and deploying an appropriate profile. (This is described later in “Enabling SCEP on managed mobile devices” on page 61.)

If you want to configure Cisco ISE support, continue with the next section. Otherwise, continue with installing LANrev Agent on all computers that are to be administered, as described in “Installing LANrev Agent”.

Setting up Cisco ISE support

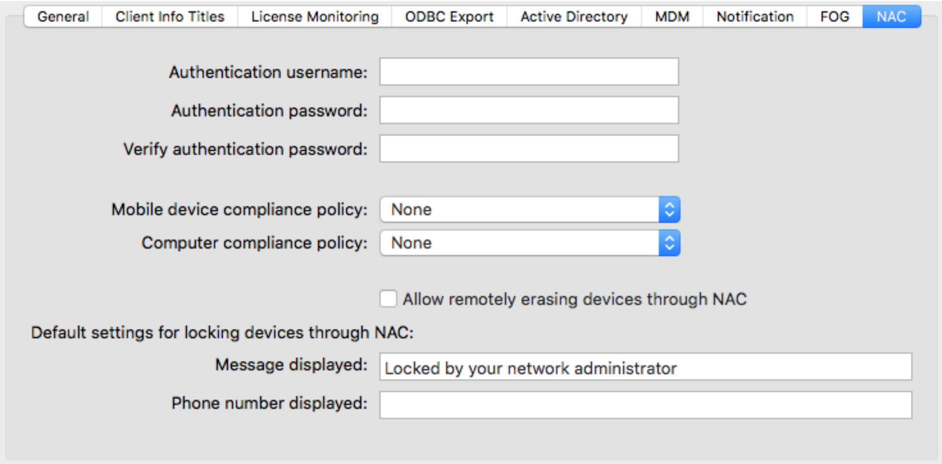
You can set up LANrev so that it can respond to inquiries from Cisco ISE whether a given device is compliant or not.

The requirements for the Cisco ISE support are listed in “System requirements” on page 12.

To set up Cisco ISE support:

1. Make sure that MDM support is set up, as described in “Installing MDM support” on page 26.

2. In LANrev Admin, choose **Window** > **Server Center**, click **Server** > **Server Settings** in the sidebar, and click the **NAC** tab:



Authentication username:

Authentication password:

Verify authentication password:

Mobile device compliance policy: None

Computer compliance policy: None

□ Allow remotely erasing devices through NAC

Default settings for locking devices through NAC:

Message displayed: Locked by your network administrator

Phone number displayed:

3. Specify a username and password that the Cisco ISE server can use to authenticate itself when sending any queries.

4. Choose the desired compliance policies for computers and mobile devices from the two pop-up menus.

   The menus list all policies and computer groups defined in LANrev. Any device that is part of the specified policy or computer group will be reported to the Cisco ISE server as being compliant; any device that is not part of either will be reported as being noncompliant.

   Computer groups are described in “Setting up computer groups” on page 324. Policies are described in “Working with policies” on page 245.

5. On the Cisco ISE server, configure an account for LANrev Server and specify the credentials you set up in step 3.

   See the Cisco ISE documentation for details.

6. If LANrev Server runs on Windows, you are done now. On macOS, open the file /etc/lighttpd/lighttpd.conf and check that it contains these lines in the fastcgi.server section:

```
"/ciscoise/" =>
((
    "socket" => "/var/run/lighttpd-mdm-fastcgi.socket",
    "bin-path" => "/usr/local/sbin/LANrevMDMServer.app/
Contents/MacOS/LANrevMDMServer",
    "max-procs" => 10,
    "check-local" => "disable"
))
```

   These lines are added automatically in new installations but not when you have upgraded from an earlier version of LANrev.

7. If the lines described in step 6 are missing, add them to the fastcgi.server section and save the /etc/lighttpd/lighttpd.conf file.

Continue with installing LANrev Agent on all computers that are to be administered as described below.

Installing LANrev Agent

LANrev Agent has the same system requirements as the other LANrev components, as described in “System requirements” on page 12.

Installation method

There are different methods of installing LANrev Agent:

- Automatically as part of enrolling the computer in MDM. This applies only to computers running macOS 10.10 or above. When these computers are enrolled in MDM, as described in “Enrolling computers” on page 48, the Agent is automatically installed; no additional steps are required.
- Automatically, using the Agent Deployment Center. This is described in “Installing LANrev Agent using the Agent Deployment Center” on page 39.
- By letting users of desktop computers enroll using the MDM server. This is described in “Enrolling computers using the MDM server” on page 45.
- For administered Windows computers: Automatically, using a login script. The details of setting this up depend on the specifics of your systems; providing them goes beyond the scope of this manual.
- Manually, executing the installer locally. This is described below. Note that manual installation requires the admin application to run on the same operating system platform as the agents. In other words, if you want to install agents on both macOS and Windows, you need to also install LANrev Admin on both platforms.

In most situations, the automatic methods will be preferable to the manual installation, particularly in cross-platform setups.

Installing LANrev Agent manually on macOS

To install LANrev Agent manually on macOS:

1. Make the LANrev Agent installation package available on the computer on which you want to install – on a server volume accessible from the computer, on a removable medium or by copying it to the local hard disk.

2. Open the installation package and follow the on-screen instructions.

   There is no need to restart the computer after the installation.

3. Make sure that Remote Login is enabled in the Sharing system preference.

4. Repeat these three steps on all other computers on which you want to install LANrev Agent.

5. In LANrev admin, choose **Window** > **Agent Deployment Center**.

   The **Agent Deployment Center** window opens.

6. Select the computers on which you have just installed agents.

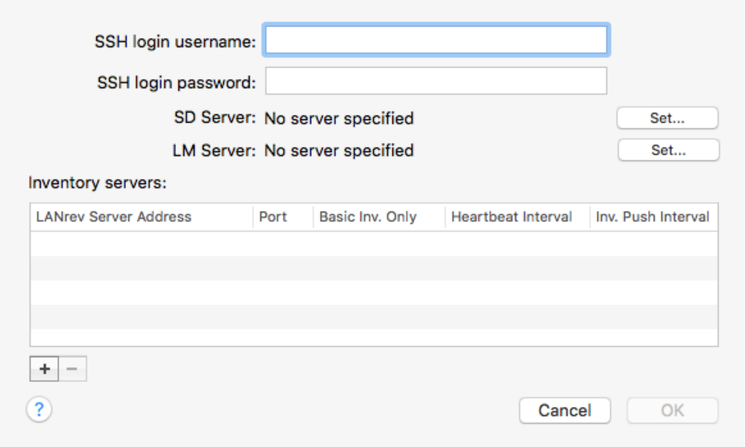
   You can select multiple computers together if there is a user account with the same name and password on each of them.

   Computers with current versions of the Agent are indicated by green dots.

   In large networks, you may need to create custom zones to see all agents. See “Creating zones in the Agent Deployment Center” on page 40 for details on doing so.

7. Right-click and choose **Set Inventory Server** from the context menu.

The **Inventory Server Properties** dialog opens.



SSH login username:

SSH login password:

SD Server: No server specified

LM Server: No server specified

Inventory servers:

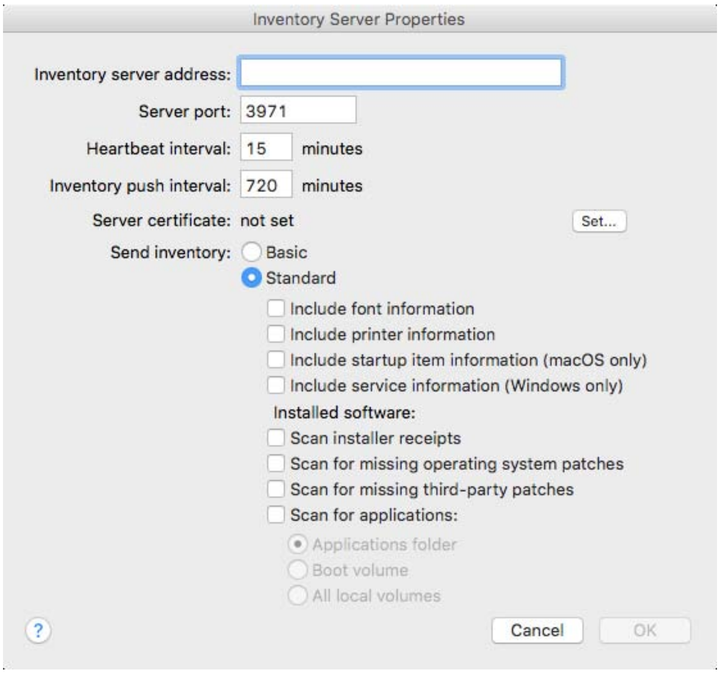
LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

8. Enter the SSH username and password required to access the clients.

   Note that this means that all selected clients must have SSH accounts with the same usernames and passwords. If not all of your clients have such similar accounts, select them in multiple groups, with the clients in each groups having similar accounts.

9. If the server you want to assign is not present in the list, click the + button to add it.

10. The **Inventory Server Properties** dialog opens.



Inventory Server Properties

Inventory server address:

Server port: 3971

Heartbeat interval: 15 minutes

Inventory push interval: 720 minutes

Server certificate: not set

Send inventory: ○ Basic
● Standard
☐ Include font information
☐ Include printer information
☐ Include startup item information (macOS only)
☐ Include service information (Windows only)
Installed software:
☐ Scan installer receipts
☐ Scan for missing operating system patches
☐ Scan for missing third-party patches
☐ Scan for applications:
● Applications folder
○ Boot volume
○ All local volumes

11. Enter the DNS name or IP address of your LANrev Server in the **Inventory server address** field.

For most installations, you can leave the other settings at their defaults. More detailed considerations are found in “Assigning inventory servers to agents” on page 79. Recommended values for very large installations are provided in the separate LANrev Optimization Guide.

12. If the **Inventory server certificate** field does not display “valid”, click the **Set** button to select the certificate for the server you are specifying.

    Creating a certificate is described in “Exporting a server certificate” on page 21.

    Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

13. Click **OK** to create the new server specification.

14. In the **Inventory servers** list, select all servers that you want to use to manage the selected agents.

    Optionally, you can also assign software distribution and license monitoring servers at this time, but it is often more efficient to do so later, as described in “Assigning software distribution or license monitoring servers to agents” on page 81.

15. Click **OK** to close the dialog and assign the specified servers to the agents.

When the servers have been successfully assigned, the agent appears in the Computers window of any LANrev Admin that is connected to one of these servers.

Installing LANrev Agent manually on Windows

Installing LANrev Agent manually on a Windows computer requires LANrev Admin for Windows. For details, see the documentation for LANrev Admin for Windows.

Installing LANrev Agent using the Agent Deployment Center

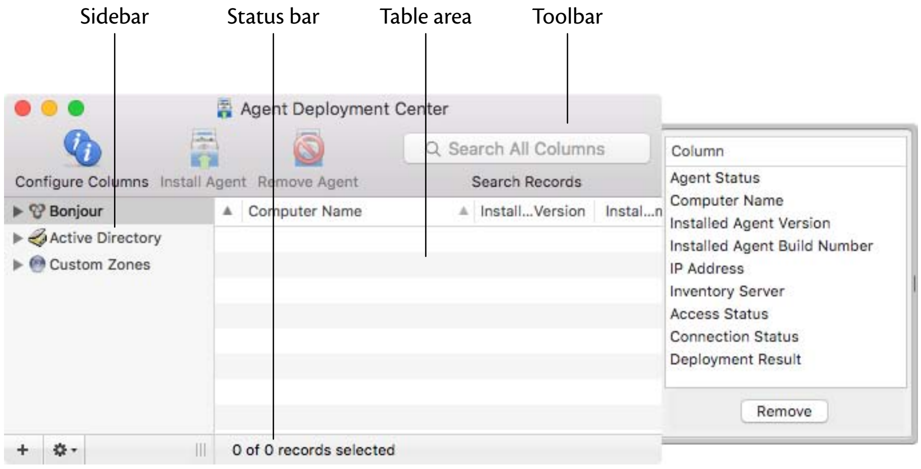
The Agent Deployment Center is a LANrev Admin module that lets you install and update LANrev Agent on computers in your network as well as review the currentness of installed agents.

NOTE Installing agents as described in this procedure is possible only for administrators with the Deploy Agents right. See “New Administrator” on page 758 for details.

The Agent Deployment Center can be used to install agents on computers using the same operating system platform (macOS or Windows) as the administrator application; in addition, Linux clients can be installed from LANrev Admin running on macOS (10.8 or above). For agent deployment in mixed networks, you should therefore install at least one LANrev Admin application on each platform.

NOTE In contrast to the other parts of LANrev, the Agent Deployment Center does not work through LANrev Server. Installations are performed directly from LANrev Admin to the client computers; all settings are stored locally on the administrator workstation.

All its functions are controlled from the **Agent Deployment Center** window:



Prerequisites

Installing or updating LANrev Agent via the Agent Deployment Center requires your administrator account to have the **Deploy Agents** permission. (Creating administrator accounts is described in “Administrator accounts” on page 72.)

In addition, every computer on which LANrev Agent is to be installed must have SSH enabled and there must be an account that you can use (that is, for which you know the password).

Overview

To install or update LANrev Agent via the Agent Deployment Center, you perform these steps:

1. Create zones that list all relevant computers.

2. Select the computers on which you want to install or update LANrev Agent, specify the access parameters, and install the agents.

These steps are described below in detail.

You can also specify that agents be installed on all found computers where they are not already present. This is also discussed below.

Creating zones in the Agent Deployment Center

The Agent Deployment Center contains predefined network zones:

- Under **Bonjour**, all Bonjour (ZeroConf) zones defined in your network are automatically listed. In LANrev Admin for Windows, these zones are displayed only when you have installed Bonjour on your workstation.
- Under **Active Directory**, all Active Directory zones defined in your network are automatically listed. This entry is displayed only if there is an Active Directory server in your network.

If these zones do not list all computers that you want to administer or if you want to group the computers differently than they are grouped by the zones, you can define custom zones.

Custom zones are defined by IP address, IP address range, or by DNS name.

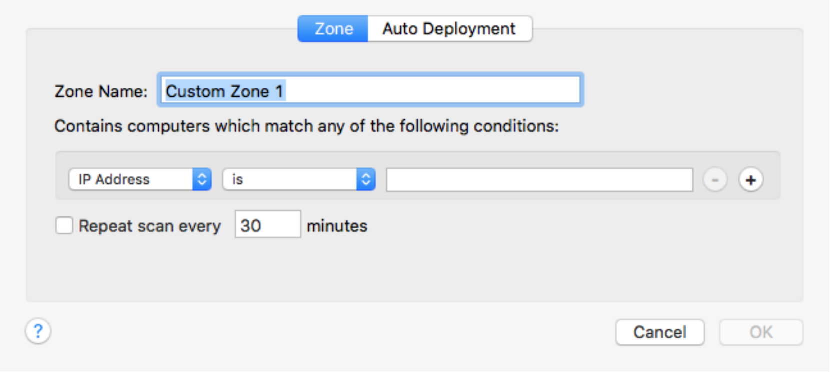
NOTE You can also import custom zone definitions from a text file, as described in “Import Zones File” on page 812.

To define a custom zone:

1. From the **Agent Deployment Center action menu**, choose **New Custom Zone**.

   The **Custom Zone** dialog opens.

2. Click the **Zone** tab:



Zone Name: Custom Zone 1

Contains computers which match any of the following conditions:

□ Repeat scan every 30 minutes

3. Enter a descriptive name for the zone and use the pop-up menus to define conditions for computers that are to be included in the zone.

   You can specify single IP addresses, ranges of IP addresses, and DNS names.

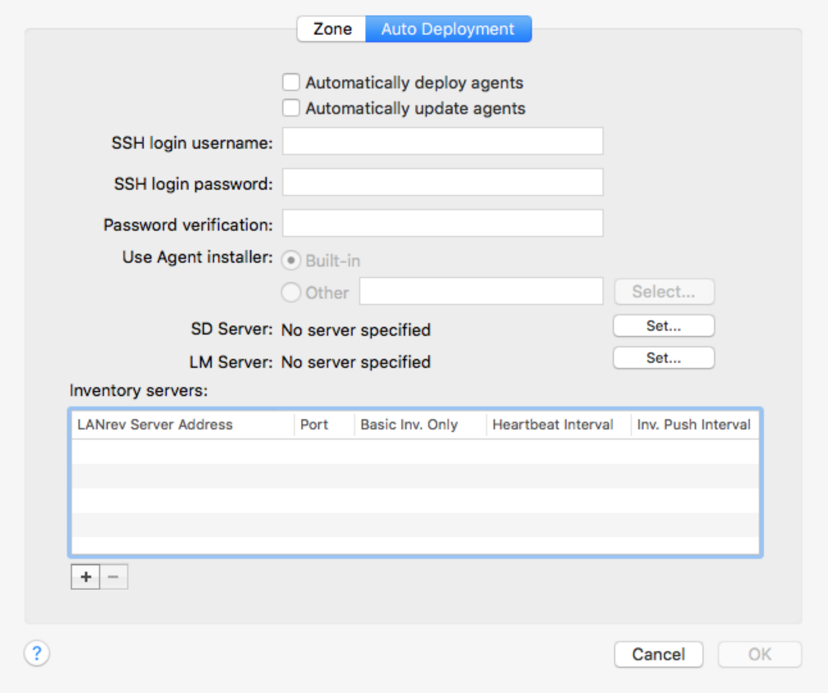
   Using the **+** button, you can create additional conditions. The zone will include any computer that meets at least one of the specified conditions.

   Use the **–** button to remove unwanted conditions.

4. If you want LANrev to regularly scan the zone (which is useful with automatic deployment as described below), check **Repeat scan every** and enter the desired interval in minutes.

5. If you do not wish LANrev to automatically install LANrev Agents without further interaction with you, skip to step 7.

Otherwise, click the **Auto Deployment** tab:



□ Automatically deploy agents
□ Automatically update agents

SSH login username:

SSH login password:

Password verification:

Use Agent installer: ● Built-in ○ Other

SD Server: No server specified

LM Server: No server specified

Inventory servers:

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

6. Fill in the fields as described in step 9 through step 14 of **Installing LANrev Admin on macOS**, above.

7. Click **OK** to create the zone.

8. To save the zone, choose **Save** from the **File** menu.

   Saving the zone is optional; however, if you do not do so, it is not available when you next start LANrev Admin.

The new zone appears in the drawer in the **Custom Zones** section.

If you have specified automatic scanning, LANrev scans the zone for computers. If you have also specified automatic deployment, LANrev Agent will be installed on all computers on which it is not yet present. This requires the computers to have the same operating system as your administrator workstation – LANrev Admin running on Windows can only automatically deploy LANrev Agent for Windows and LANrev Admin for macOS can only deploy LANrev Agent for macOS.

Linux is an exception: LANrev Agent for Linux must be installed from a computer running macOS (10.8 or above).

If you have not set the zone for automatic scanning, you will now want to search the zone for devices, as described below.

Searching zones

To search a zone, choose **Search Zone** from the action menu.

Searching a zone usually takes up to about one second per specified IP address or DNS name.

NOTE The exact time depends on the server connection timeout set in the **Preferences** dialog (see "Preferences" on page 366); each IP address where no device is found takes about a tenth of that time. IP addresses where devices are located are scanned much quicker.

You can cancel a search in progress by choosing **Cancel Search** from the zone's context menu.

The found devices are listed in the table area of the **Agent Deployment Center** window. Colored dots in front of their names indicate their status:

🟢 Green dot: LANrev Agent is current.

🟡 Yellow dot: LANrev Agent is present but outdated.

🔴 Red dot: No LANrev Agent. Installing an agent is possible.

⚪ Grey dot: No LANrev Agent, and no agent can be installed. A common reason is that you are trying to install across platforms (that is, from the macOS Admin to a Windows client or vice versa), which is not possible with the Agent Deployment Center. Other reasons include: The device is not a computer, or SSH is disabled on a macOS client.

On computers that have no agent (🔴) or an old version (🟡), you can install the current version, as described below.

If you have specified automatic deployment for the zone (see above), LANrev automatically installs LANrev Agent on all computers that have the same operating system as your administrator workstation and on which no LANrev Agent is present. (Automatic deployment from a macOS Admin also deploys agents to Linux clients.)

Editing zones

To edit a custom zone, select it and choose **Edit Custom Zone** from the action menu.

Predefined zones cannot be edited.

Deleting zones

To delete a custom zone, select it and choose **Remove Custom Zone** from the action menu.

Predefined zones cannot be deleted.

Installing or updating LANrev Agent

When the computers on which LANrev Agent is to be installed are listed in the **Agent Deployment Center** window (see above), you can install the agent on them.

NOTE For information on setting a zone up for automatic deployment, see step 5 of the procedure in "**Creating zones in the Agent Deployment Center**", above.

To install or update LANrev Agent:

1. In the **Agent Deployment Center** window, select all computers on which you want to update or install the agent. You can select computers that require installations and ones that require updates at the same time.

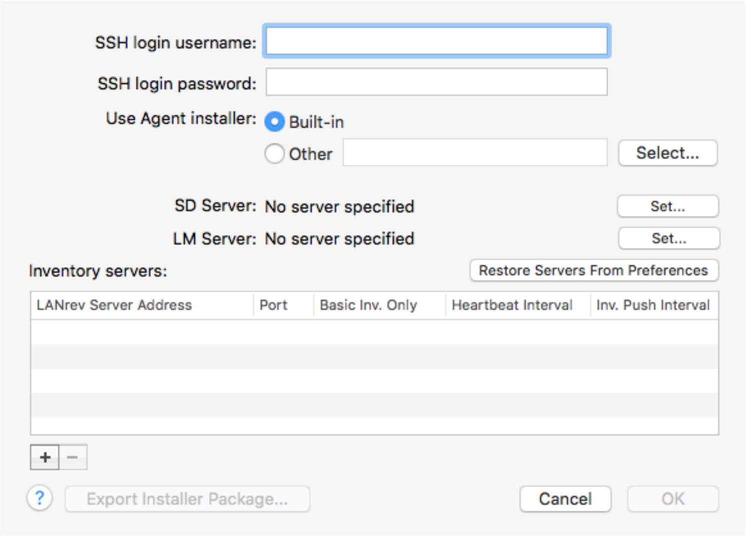
   Make sure to select only macOS or Linux computers; to install or update agents on Windows computers, use a Windows version of LANrev Admin.

   On all macOS or Linux computers that you select together, there must be an SSH account with the same name and password.

   Note that the Agent for Linux has only a subset of the functionality of the macOS and Windows versions. See "Functionality of LANrev Agent for Linux" on page 45 for an overview.

2. From the action menu, choose **Install Agent**.

   The **Agent Deployment Settings** dialog opens:



SSH login username:

SSH login password:

Use Agent installer: ● Built-in ○ Other

SD Server: No server specified

LM Server: No server specified

Inventory servers:

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

3. Fill in the fields as described in step 9 through step 14 of **Installing LANrev Admin on macOS**, above.

4. If you have prepared a custom installer package, click **Other** and then click **Select** to open it.

   You can create custom installer packages in the **Deployment Center** tab of the **Preferences** dialog and save them by clicking **Export Installer Package**, including the specified server settings and required certificates.

5. Click **OK**.

LANrev Admin now installs agents on the selected computers. The progress of the installation is displayed in the Agent Deployment Center's **Connection Status** column. Any errors that occur during an installation are logged in **~/Library/Logs/LANrev Agent Deployment/**.

If the built-in firewall is active on a client computer, installing the agent automatically opens the agent port as specified in the *Preferences* dialog (normally port 3970).

Enrolling computers using the MDM server

This method requires that you have set up the MDM server, as described in "Installing MDM support" on page 26.

To allow computer users to enroll using the MDM server:

1. Send an e-mail to all users whose computers are to be enrolled. Include the enrollment URL:
   https://<server address>/Profile/dtenrollment.mdm

   <server address> is the DNS name of your MDM server, for example, mdm.mycompany.com.

   Make sure to send the e-mail to addresses that these users read on the computers – enrollment is not possible if the e-mail is accessed from another device, such as a mobile device.

2. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

   They will need to enter their Active Directory or Open Directory (depending on which service you use) username and password in the process. If they also enter a domain, LANrev will assume that the account is an Active Directory account; if they do not enter a domain and LANrev Server runs on macOS, the account is assumed to be an Open Directory account.

Each computer on which users follow this procedure appears in the **Computers** window in LANrev Admin.

Functionality of LANrev Agent for Linux

LANrev Agent for Linux supports a subset of the commands and information items available on other platforms, as described below.

Commands available for Linux agents:

- **Gather Inventory Information**
- **Gather Installed Software**

Information items available for Linux agents:

- Agent Information, General
  - Agent Name
  - Agent Version
  - Agent Build Number
  - Agent Serial Number
  - Computer Online
  - Last Heartbeat
  - Record Creation Date
- Hardware Information, System Information, CPU Information
  - Physical Cores
  - Active Cores
  - Processor Speed
  - Processor Type
  - Processor Vendor
  - Processor L1 Data Cache
  - Processor L1 Instruction Cache
  - Processor L2 Data Cache
  - Processor L2 Instruction Cache
  - Processor L3 Cache
  - Processor Family
  - Processor Model
  - Processor Stepping
  - Processor Has MMX
  - Processor Has 3DNow
  - Processor Has SSE
  - Processor Has SSE2
  - Processor Has SSE3
  - Processor Supports Hyperthreading
  - Processor Hyperthreading Enabled
- Hardware Information, System Information (other)
  - Physical Memory
  - Primary MAC Address
  - Date & Time
  - Computer Serial Number
  - Computer Boot Time
  - Computer Uptime
  - BIOS Date
  - BIOS Vendor
  - BIOS Version
  - SMBIOS Version
  - Mainboard Manufacturer
  - Mainboard Product Name
  - Mainboard Serial Number
  - Mainboard Type
  - Mainboard Version
  - Mainboard Asset Tag
  - System Enclosure Manufacturer
  - System Enclosure Serial Number
  - System Enclosure Type
  - System Enclosure Version

  - System Enclosure Asset Tag
  - Computer Manufacturer
  - Computer Version
  - Computer Model
  - Computer Service Tag
  - Swap Space Total
  - Swap Space Used
  - Swap Space Free
  - Memory Slots
  - Memory Module Count
  - Volume Count
  - ATA Device Count
  - USB Device Count
  - PCI Device Count
- Hardware Information, Memory Slots
  - Memory Slot Name
  - Memory Size
  - Memory Speed
  - Memory Type
- Hardware Information, Volumes
  - Volume Name
  - Size
  - Volume Type
  - Free Space
- Hardware Information, ATA Devices
  - ATA Model
  - ATA Device Type
  - ATA Serial Number
  - ATA Revision
  - ATA Protocol
  - ATA Capacity
  - ATA Socket Type
- Hardware Information, USB Devices
  - USB Vendor
  - USB Model
  - USB Serial Number
  - USB Max. Power
  - USB Vendor ID
  - USB Product ID
- Hardware Information, PCI Devices
  - PCI Name
  - PCI Type
  - PCI Slot
  - PCI ROM Revision
- Software Information, System Information
  - Current User Name
  - Current User Account
  - Current User Is Admin
  - OS Platform
  - OS Version
  - OS Build Number
  - OS Language
  - OS Product ID
  - Virtual Machine
  - Daylight-Saving Time

  - GMT Delta
  - Firewall Enabled
  - Installed Software Count
- Software Information, Network Adapters
  - Adapter Name
  - Adapter IP Address
  - Adapter Subnet Mask
  - Adapter MAC Address
  - Router Address
  - Primary Interface
  - Device Name
  - Link Status
  - Adapter Speed
  - Adapter Vendor
  - Hardware
- Software Information, Installed Software
  - Inst. Software Name
  - Inst. Software Company
  - Inst. Software Version String

Enrolling computers

While installing LANrev Agent on managed computers provides a very wide range of management options, enrolling the devices gives you some additional capabilities. Notably, you can remotely lock or erase these computers, for example, in the event of a theft. Enrolling computers requires an MDM (mobile device management) server, into which the devices are enrolled. (Because of a limitation in OS X 10.9 Mavericks, an MDM server running on Windows is required for enrolling computers running OS X 10.9.)

Only computers running macOS 10.7 or above can be enrolled in MDM management. (For enrolling mobile devices, see “Enrolling mobile devices” on page 50.) For computers running macOS 10.10 or above, enrolling also installs LANrev Agent; no separate installation step is required.

Enrolling computers requires providing a special configuration profile on a web server and sending a link to this file to all computers you want to include in the MDM.

There are three basic enrollment techniques:

- Using the MDM server. This is automated to a larger degree and provides access to Active Directory data. This approach requires you to have an Active Directory server on which each user has an account. See “Enrollment using the MDM server”, below, for details.
- Using your own server. This requires more effort on your part and does not provide access to Active Directory data for enrolled users (the Device User Information information item category). However, no Active Directory server is required. See “Enrollment using a different web server”, below, for details.

- Using Apple’s device enrollment program (ADEP). This option is available only for computers purchased from Apple through this program. Enrolling devices in this way is more convenient and offers additional options, such as skipping setup steps or putting devices into supervised mode, but requires additional steps. See “Using ADEP” on page 56” for details.

If you have enrolled computers without tying them to Active Directory accounts, you can batch-assign these accounts to the devices later, as described in “Assigning Active Directory user accounts to enrolled devices” on page 53.

Enrollment using the MDM server

1. Send an e-mail to all users whose computers are to be enrolled. Include the enrollment URL:
   https://<server address>/Profile/enrollment.mdm

   <server address> is the DNS name of your MDM server, for example, mdm.mycompany.com.

   Make sure to send the e-mail to addresses that these users read on the computers – enrollment is not possible if the e-mail is accessed from another device, such as a mobile device.

2. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

   They will need to enter their Active Directory domain, username, and password in the process.

Each computer on which users follow this procedure appears in browser windows in LANrev Admin. You can manage it there using the context menu commands.

Enrollment using a different web server

1. Find the enrollment file.

   The file is named MDMEnrollmentBootstrap.mobileconfig and is located on the LANrev Server, with the exact location depending on the operating system of the server computer:

   - Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\
   - Windows Vista and above, Windows Server 2008 and above: C:\ProgramData\Pole Position Software\LANrev Server\
   - macOS: /Library/Application Support/LANrev Server/

2. Make the enrollment file available on a web server.

   The file must be accessible with a standard http or https URL.

   We recommend that you put it in an area of the web server that requires logging in or provides another form of access control.

3. If you are using an IIS server, use IIS Manager to add the enrollment file’s MIME type to the server’s **Properties** page:

   The extension for the file is “mobileconfig” and the file type is “application/x-apple-aspen-config”.

4. Send an e-mail with the URL of the enrollment file to all users whose computers are to be managed.

   Make sure to send the e-mail to addresses that these users read on the computers – enrollment is not possible if the e-mail is accessed from another device, such as a mobile phone.

5. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

Each computer on which users follow this procedure appears in browser windows in LANrev Admin. You can manage it there using the context menu commands.

Enrolling mobile devices

Mobile devices (Android, iOS – including iPod touches and LAN-only iPads – and Windows Phone) can be administered by LANrev. This requires an MDM (mobile device management) server, into which the devices must be enrolled. This process serves a similar purpose as installing an agent on a desktop computer, but is different in detail.

Only devices meeting the following system software requirements can be enrolled in MDM management:

- iOS 4.0 or above
- Android 2.2 or above
  For many functions, the devices must be able to receive push messages, which requires either Android 4.0 or a Gmail account to be set up on the device.
- Windows Phone

Enrolling iOS devices requires providing a special configuration profile on a web server and sending a link to this file to all devices you want to include in the mobile device management. This step is not required for enrolling Android devices.

There are three basic enrollment techniques:

- Using the MDM server. This is automated to a larger degree and provides access to Active Directory and – if LANrev Server runs on macOS – Open Directory data. This approach requires you to have an Active Directory or Open Directory server, respectively, on which each mobile user has an account. See “Enrollment using the MDM server”, below, for details.
- Using your own server. This requires more effort on your part and does not provide access to Active Directory or Open Directory data for enrolled users (the Device User Information

information item category). However, no Active Directory or Open Directory server is required. See "Enrollment using a different web server", below, for details.

- Using Apple's device enrollment program (ADEP). This option is available only for iOS devices purchased from Apple through this program. Enrolling devices in this way is more convenient and offers additional options, such as skipping options during device setup or putting devices into supervised mode, but requires additional setup. See "Using ADEP" on page 56" for details.

NOTE Irrespective of the technique used, Android users must enable the installation of content obtained from sources other than Google Play to be able to complete the enrollment.

If you have enrolled mobile devices without tying them to Active Directory accounts, you can batch-assign these accounts to the devices later, as described in "Assigning Active Directory user accounts to enrolled devices" on page 53.

After the devices have been enrolled, you may want to install mobile apps that are part of LANrev to enable additional management features. This is discussed in "Installing mobile apps" on page 56.

Enrollment using the MDM server

1. Only if you want to enroll Windows Phone devices: Make sure that all Windows Phone devices you want to enroll are being synchronized via ActiveSync with the Exchange server that you have specified and that an Exchange mailbox ia configured on them. (See "Configuring the MDM server" on page 29 for details.)

2. Send an e-mail to all users whose mobile devices are to be managed. Include the enrollment URL:
   https://<server address>/Profile/enrollment.mdm

   <server address> is the DNS name of your MDM server, for example, mdm.mycompany.com.

   Make sure to send the e-mail to addresses that these users read on the mobile devices – enrollment is not possible if the e-mail is accessed from another device, such as a desktop or portable computer.

3. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

   They will need to enter their Active Directory or Open Directory (depending on which service you use) username and password in the process. If they also enter a domain, LANrev will assume that the account is an Active Directory account; if they do not enter a domain and LANrev Server runs on macOS, the account is assumed to be an Open Directory account.

They will also need to indicate whether the device belongs to them personally or to the company.

Android users will need to manually launch the downloaded file (LANrev Apps.apk), which we recommend to mention in the e-mail. If they have not done so before, they will also need to enable the installation of content from sources other than Google Play.

Each device on which users follow this procedure appears in the **Mobile Devices** window in LANrev Admin. You can manage it there using the context menu commands.

For Windows Phone users, the above procedure automatically enrolls all devices linked to the specified Active Directory account.

Enrollment using a different web server

This technique cannot be used for Windows Phone devices.

1. Find the enrollment file. Depending on the target platform (iOS or Android), it is found in different locations:

    - For iOS devices, the file is named MDMEnrollment-Bootstrap.mobileconfig and is found on the LANrev Server, with the exact location depending on the operating system of the server computer:
        - Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\
        - Windows Vista and above, Windows Server 2008 and above: C:\ProgramData\Pole Position Software\LANrev Server\
        - macOS: /Library/Application Support/LANrev Server/
    - For Android devices, the enrollment file is the LANrev Apps.apk app package, which is included with the LANrev installers in the Android folder.

2. Make the enrollment file – MDMEnrollmentBootstrap.mobileconfig or LANrev Apps.apk – available on a web server.

    The file must be accessible with a standard http or https URL.

    We recommend that you put it in an area of the web server that requires logging in or provides another form of access control.

3. If you are using an IIS server, use IIS Manager to add the enrollment file’s MIME type to the server’s **Properties** page:

    - The extension for the iOS file is “mobileconfig” and the file type is “application/x-apple-aspen-config”.
    - The extension for the Android file is “apk” and the file type is “application/vnd.android.package-archive”.

4. Send an e-mail with the URL of the enrollment file to all users whose mobile devices are to be managed.

Make sure to send the e-mail to addresses that these users read on the mobile devices – enrollment is not possible if the e-mail is accessed from another device, such as a desktop or portable computer.

5. In the e-mail, instruct the users to click on the link and follow the instructions this will display on the screen.

   Android users will need to manually launch the downloaded file (LANrev Apps.apk), which should be mentioned in the e-mail. If they have not done so before, they will also need to enable the installation of content from sources other than Google Play.

Each device on which users follow this procedure appears in the **Mobile Devices** window in LANrev Admin. You can manage it there using the context menu commands.

Assigning Active Directory user accounts to enrolled devices

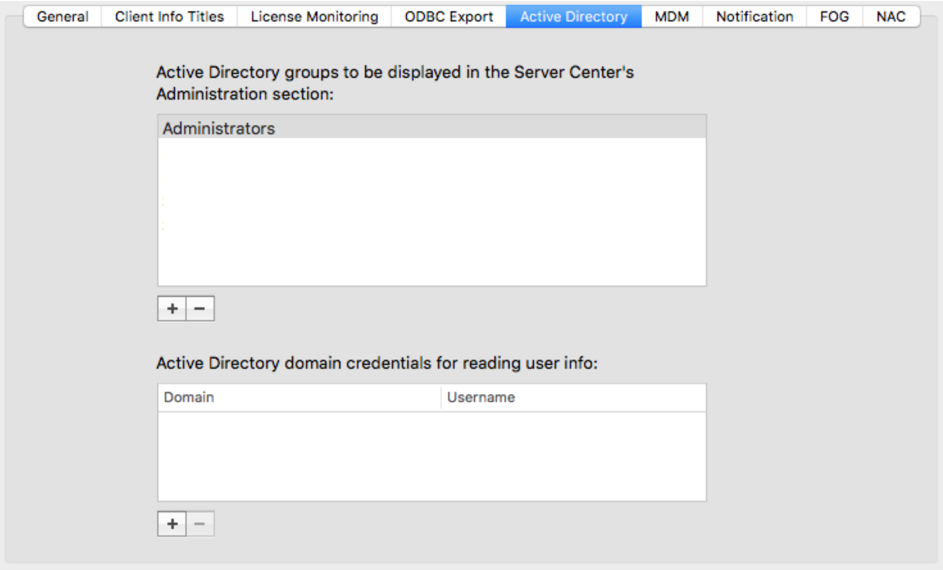
If you have enrolled devices to which you want to assign Active Directory users in a batch process:

1. Verify that the user account with which you (the LANrev administrator) access Active Directory has sufficient privileges to read the stored information for other users. (This is required to automatically fill in the user information for the managed mobile devices.)

   If your account has sufficient privileges, continue with step 5.

   If your account does not have sufficient privileges, continue with the next step. (If you have already performed these steps for this installation of LANrev on an earlier occasion, you do not need to repeat them and can continue with step 5 instead.)

2. In LANrev Admin, open the **Server Center** window, click the **Server** category in the sidebar, click **Server Settings**, and click the **Active Directory** tab.



Active Directory groups to be displayed in the Server Center's Administration section:

Administrators

Active Directory domain credentials for reading user info:

Domain	Username

3. Click the **+** button below the list of Active Directory accounts and fill in the access information for the account.

   The account you specify must have sufficient access privileges in Active Directory to read the user information for the user accounts you want to associate with enrolled mobile devices.

4. Click **OK**.

   If desired, you can repeat step 5 to specify additional accounts. LANrev will try all specified accounts until it finds one with sufficient privileges.

5. Prepare a list of the devices and their associated users.

   The list must be a text file with tabs, commas, or semicolons separating fields and returns separating records. The file must contain a column for the Active Directory user name, the user’s domain, and an identifier for the mobile device. It can contain additional columns, but these are not imported.

   The device identifier must be one of the following:

   - Bluetooth MAC address
   - WiFi MAC address
   - Device name, which must be unique in this case
   - Serial number
   - UDID
   - IMEI/MEID
   - SIMM ICC identifier

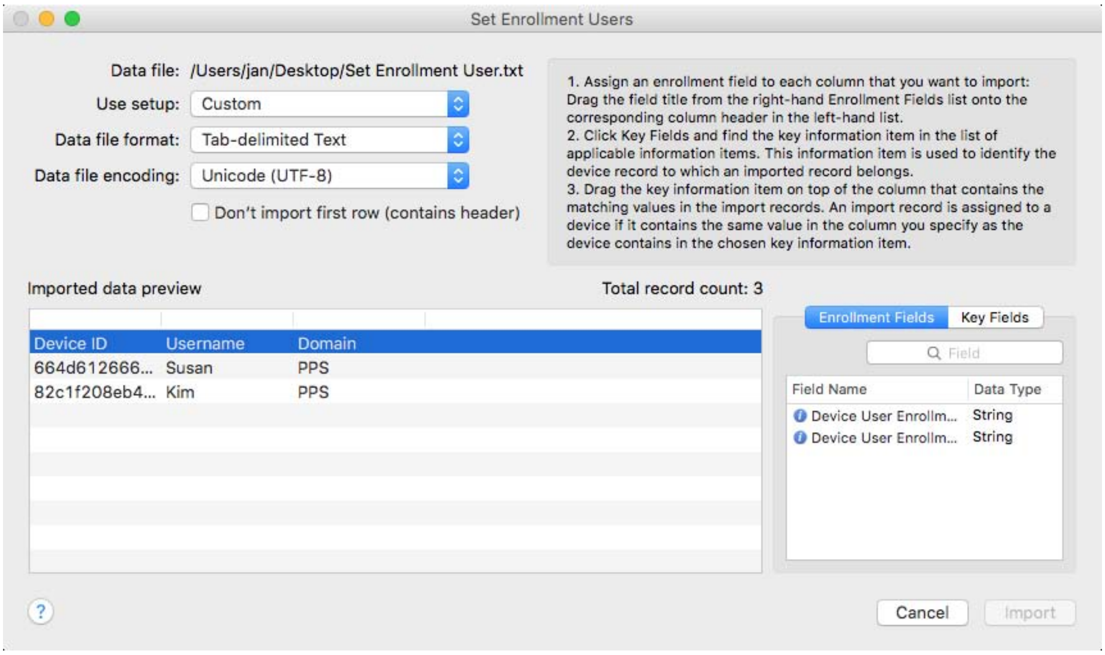
- The content of a custom information field that has been assigned to the device in LANrev and that is unique to the device

6. In LANrev Admin, choose **File** > **Import** > **Enrollment Users for Mobile Devices**.

   A standard Open dialog is displayed.

7. Choose the file you prepared in step 1 and click **Open**.

   The **Set Enrollment Users** dialog is displayed.



Set Enrollment Users

Data file: /Users/jan/Desktop/Set Enrollment User.txt

Use setup: Custom

Data file format: Tab-delimited Text

Data file encoding: Unicode (UTF-8)

□ Don't import first row (contains header)

1. Assign an enrollment field to each column that you want to import: Drag the field title from the right-hand Enrollment Fields list onto the corresponding column header in the left-hand list.
2. Click Key Fields and find the key information item in the list of applicable information items. This information item is used to identify the device record to which an imported record belongs.
3. Drag the key information item on top of the column that contains the matching values in the import records. An import record is assigned to a device if it contains the same value in the column you specify as the device contains in the chosen key information item.

Imported data preview

Total record count: 3

Device ID	Username	Domain
664d612666...	Susan	PPS
82c1f208eb4...	Kim	PPS

Field Name	Data Type
Device User Enrollm...	String
Device User Enrollm...	String

8. Click the **Enrollment Fields** tab. Drag the **Device User Enrollment Domain** information item on top of the column containing the domains and **Device User Enrollment Username** on top of the column containing the usernames.

9. Click the **Key Fields** tab. Drag the information item representing the information with which you identify the device in the text file on top of the device identifier column.

   For example, if you have used the Bluetooth MAC addresses to identify the devices, use the **Mobile Device Bluetooth MAC Address** information item.

   If you use custom information to identify the devices, you must have already defined the custom information field and populated it with information that is unique to each device.

10. Click **Import**.

The information from the text file is imported and the specified Active Directory users are automatically associated with the specified devices.

Installing mobile apps

Some mobile device management features require LANrev Apps or LANrev Safe to be installed on the devices. The details are noted in the discussion of the individual features elsewhere in this documentation. (For a description of the apps themselves, see "Mobile Apps" on page 950.)

You can distribute the apps as described in "Installing software on mobile devices" on page 197. Users can also download them from the appropriate app stores. (LANrev Apps is installed automatically on enrolled Android devices.)

When installing these apps on iOS devices, additional steps may be required:

- On devices running iOS 7 or above, no additional steps are required if the app is downloaded from the App Store and distributed via MDM.
- On devices running iOS 7 or above where the app has been downloaded from the App Store directly to the device, users must enter their Active Directory or Open Directory credentials to bind the app to their MDM account and pick their device from a list.
- On iOS 6 devices, users must enter their Active Directory or Open Directory credentials to bind the app to their MDM account and pick their device from a list.

NOTE These considerations apply only to LANrev Apps and LANrev Safe, not to other apps that are part of LANrev nor to app store or enterprise apps.

Using ADEP

Enrolling devices through Apple's device enrollment program (ADEP) is possible only for iOS and macOS devices that are purchased from Apple through the program. (Contact Apple for details on entering devices in the program.)

Enrolling devices in this way is more convenient and offers additional options, such as skipping setup steps or putting devices into supervised mode.

Enrolling devices through ADEP involves these general steps:

1. Setting up your accounts for the program. See "Setting up ADEP" on page 57 for details.

2. Associating devices with the accounts. This is done by Apple; it is not possible to do this in LANrev. Contact Apple for details on how to enter devices in the ADEP.

Once a device is associated with one of the accounts you have specified in LANrev, it appears automatically in a browser window or the **Mobile Devices** window; you do not need to do anything in LANrev.

3. Creating device enrollment profiles, as described in "Managing device enrollment profiles" on page 58.

   These profiles specify the enrollment settings; without them, devices in the enrollment program behave like standard devices.

4. Assigning profiles to devices, as described in "Assigning device enrollment profiles" on page 59.

When you have enrolled the devices in this way, you can optionally:

- Batch-assign Active Directory accounts as described in "Assigning Active Directory user accounts to enrolled devices" on page 53.
- Install LANrev mobile apps as described in "Installing mobile apps" on page 56.

Setting up ADEP

To set up LANrev for using ADEP to enroll devices:

1. Create an account for the program with Apple and download the account credentials file.

   Details on this process are available from Apple.

2. Make sure that the clock of the computer on which LANrev Server is running is accurate.

   If the server's clock deviates too much from the clock of Apple's device enrollment program's server (a few minutes or more), enrollment authentications may fail.

   The easiest way to ensure an accurate clock is by synchronizing the server's time with an NTP server.

3. In the Server Center, open the **MDM** tab of the server settings.

4. In the **Apple Device Enrollment Program Accounts** section of the tab, click the **Configure** button.

   The **Apple Device Enrollment Program Accounts** dialog opens.

5. Click the **+** button and follow the on-screen instructions to set up the account.

   If you have multiple accounts, repeat this step until you have added all accounts to LANrev.

6. Choose **Server** > **Save Server Settings** to upload the account information to LANrev Server.

You can now use these accounts to create device enrollment profiles, as described below.

Managing device enrollment profiles

To set enrollment options for a device, a device enrollment profile is assigned to it. You can create and delete these profiles in LANrev, as described below.

When you have set up the profiles as desired, you can assign them to devices, as described in “Assigning device enrollment profiles” on page 59, below.

Creating device enrollment profiles

To create a device enrollment profile:

1. In the sidebar of the **Mobile Devices** window or the **Server Center** window, right-click and choose **Device Enrollment Profiles** > **New Device Enrollment Profile** from the context menu.

   The **Device Enrollment Profile Editor** dialog opens.

2. Set the dialog options as desired and click **OK**.

   For details, see “New Enrollment Profile” on page 597.

The profile is now displayed in the sidebar of the **Mobile Devices** window, in the **Assignable Items** > **Device Enrollment Profiles** section. You can repeat this procedure to create as many profiles as desired.

Deleting device enrollment profiles

To delete a device enrollment profile:

1. In the sidebar of the **Mobile Devices** window, click **Assignable Items** > **Device Enrollment Profiles**.

   The main section of the window displays all device enrollment profiles that have been created in LANrev.

2. In the main section of the window, right-click the profile that you want to delete and choose **Remove Device Enrollment Profile** from the context menu.

   Note that deleting a profile that is still assigned to any devices removes it from those devices as well. This has different consequences depending on the statuses of the devices:

   - Devices that have not yet been enrolled will be activated as if they did not belong to the enrollment program.
   - Devices that have already been enrolled keep their current settings from the enrollment profile (for example, as a supervised device). However, they lose these settings when they are next reset to factory conditions and

thereafter behave as if they were not part of an enrollment program.

In both cases, you can assign a new device enrollment profile to the devices that will become effective when a device is set up or reset to factory conditions.

Editing device enrollment profiles

To change a profile's settings:

1. In the sidebar of the **Mobile Devices** window, click **Assignable Items** > **Device Enrollment Profiles**.

   The main section of the window displays all device enrollment profiles that have been created in LANrev.

2. In the main section of the window, right-click the desired profile that you want choose **Edit Device Enrollment Profile** from the context menu.

   The profile is opened in the **Device Enrollment Profile Editor** dialog.

3. Edit the settings as desired and save the profile.

If the profile is already installed on any devices, the edited profile is automatically installed on those devices. Note that this resets the device enrollment status and enrollment profile installation dates for those devices.

Assigning device enrollment profiles

The activation options for devices in an enrollment program are set by assigning device enrollment profiles.

These profiles can only be assigned to devices that are associated with your device enrollment program (ADEP) account. This association of devices with ADEP accounts is done by Apple and is outside the control of LANrev. Contact Apple for details.

Device enrollment profiles can be assigned automatically through a policy or computer group, or they can be assigned manually.

Automatically assigning device enrollment profiles

To assign a profile to devices in a device enrollment program through a policy or computer group:

1. For mobile devices, create a new policy to use for assigning device enrollment profiles or choose an existing policy for this purpose. For computers, create or choose a computer group.

   The profile will be assigned to all devices that are a member of this policy or group.

Creating a policy is described in “Working with policies” on page 245. Creating a computer group is described in “Setting up computer groups” on page 324

2. Expand the policy (in the sidebar of the **Mobile Devices** window) or group (in the sidebar of the **Server Center** window) and click on its **Device Enrollment Profile** subsection.

3. Choose the desired profile from the **Profile name** pop-up menu.

   Creating profiles is described in “Managing device enrollment profiles” on page 58.

The chosen device enrollment profile is immediately assigned to all devices that are members of the policy or group and will be assigned to each device that becomes a member. However, if any of these devices already has an enrollment profile that was assigned through another policy or group, that profile is left in place and the profile specified in the policy is not installed.

You can specify enrollment profiles in multiple policies or groups, for example, to assign different profiles to different types of devices. Note, however, that it is undefined which profile is installed on a device which belongs to multiple such policies or groups (that specify an enrollment profile).

We therefore recommend that you set up your profiles such that no device belongs to more than one policy or group that specifies a device enrollment profile.

Manually assigning device enrollment profiles

To assign a profile to devices in a device enrollment program manually:

1. Select the desired devices in the **Mobile Devices** window (for mobile devices) or **Server Center** window (for computers), right-click them, and choose **Device Enrollment** > **Assign Device Enrollment Profile** from the context menu.

   The **Assign Enrollment Profile** dialog opens.

2. Choose the desired profile from the **Enrollment profile** pop-up menu and click **OK**.

   Creating profiles is described in “Managing device enrollment profiles” on page 58.

This assigns the settings in the profile to the devices. Any existing profiles are overwritten.

When the devices are activated, the activation process follows the profile settings. If a profile is assigned to a device that has already been activated, the profile settings are not immediately applied; instead, they take effect when the device is next reset to factory conditions.

Removing device enrollment profiles from devices

To remove a device enrollment profile from managed devices, select the desired devices in the **Mobile Devices** window (for mobile devices) or **Server Center** window (for computers), right-click them, and choose **Device Enrollment** > **Unassign Device Enrollment Profile** from the context menu.

This has different consequences depending on the statuses of the devices:

- If the enrollment profile is removed from a device, it is no longer under MDM management. This may prevent you from performing actions on the device that have MDM management as a prerequisite. For example, the device is automatically removed from classroom management.
- Devices that have not yet been enrolled will be activated as if they did not belong to the enrollment program.
- Devices that have already been enrolled keep their current settings from the enrollment profile (for example, as a supervised device). However, they lose these settings when they are next reset to factory conditions and thereafter behave as if they were not part of an enrollment program.

In both cases, you can assign a new device enrollment profile to the devices that will become effective when a device is set up or reset to factory conditions.

Note that removing a device enrollment profile from a policy (see “Automatically assigning device enrollment profiles”, above) does not remove it from devices belonging to that policy.

Disowning devices

Unassigning device enrollment profiles from devices, as described above, does not remove the device from the enrollment program. You can at any time assign a different profile that takes effect normally.

If you want to release a device from the enrollment program, you must do so through Apple. For details, please contact Apple.

Enabling SCEP on managed mobile devices

Enabling managed mobile devices to use certificates to access Exchange servers requires setting up the SCEP support and sending suitable configuration profiles to all the devices:

1. Make sure that SCEP support is properly set up, as described in “Setting up SCEP (NDES) support” on page 32.

2. Make sure that all devices on which you want to enable certificate-based access are enrolled, as described in “Enrolling mobile devices” on page 50.

3. Create a new profile of an appropriate type (for example, iOS configuration profile or Android configuration profile) as described in “Creating a new configuration profile” on page 182.

4. In this new profile, enter the required information:

   - Specify the Exchange ActiveSync account for the devices to use in the **Exchange ActiveSync** section.
     Make sure to set the **Authentication Credential** option to **Automatically Generate**.
   - Specify the SCEP server and the settings to use in the **SCEP** section.

5. Complete and save the configuration profile.

6. Deploy the configuration profile to all appropriate devices, as described in “Overview of installing configuration profiles on mobile devices” on page 186.

The devices on which the profiles are installed can now authenticate themselves with the Exchange server without needing to specify a password.

Updating LANrev

When updating LANrev, you should update all components simultaneously. LANrev Server and LANrev Admin must always be the same version, and while older versions of LANrev Agent are supported in principle, some features will be unavailable.

See the installation sections for information on installing the update of LANrev Server and LANrev Admin:

- “Installing LANrev Server” on page 16
- “Installing LANrev Admin” on page 17
- “Installing LANrev Agent” on page 35

Updating the Agent

NOTE You must have set up the Software Distribution Center before beginning this procedure, and there must be at least one distribution point.

If you are using the Software Distribution Center, you can use it to update agents extremely easily:

1. Update LANrev Server and LANrev Admin.

2. Start LANrev Admin and open the **Server Center** window.

You find two automatically generated packages – **LANrev Agent (macOS)** and **LANrev Agent (Windows)** – under **Software Distribution** > **Software Packages**.

Note: If you have just installed or updated LANrev Server, these packages may take a few minutes to appear in the Software Distribution Center.

3. Drag the packages to the computer groups that contain the clients you wish to update. If you want to update all clients, doing which we highly recommend, drag them to **All Macs** and **All PCs**, respectively.

This updates the agents on all computers in the computer groups to which you have assigned the packages. Unless you later remove the packages from the groups, it also ensures that, in future, new version of LANrev Agent are automatically distributed to these computers. (You are asked for permission first in each case.)

Updating the Software Distribution Center from LANrev 1.x

When you have been using the Software Distribution Center in LANrev 1.x, you must update the server and software package definitions, as described below.

NOTE These updates are not necessary when you have already been using LANrev 2.0 or later.

Updating the Software Distribution Center

Because of a new architecture of the Software Distribution Center in LANrev 2.0 and later, the definitions of distribution points and software packages need to be updated when you have been using version 1.x before. You may also want to consider the choice of computers as distribution points. These issues are described below.

Choosing distribution points

Under the new Software Distribution Center architecture, distribution points do no longer need to be file servers. This means that you can now choose computers on which you cannot or will not run file server software.

We do, however, still recommend that only server computers are used as distribution points, that is, computers with no local users working on them.

Updating distribution points

To update an existing distribution point to be compatible with the new architecture:

1. Install LANrev Agent on the distribution point, same as you would on any client computer. See “Installing LANrev Agent” on page 35 for details.

2. If file server software on the computer was previously only used for distribution point purposes, you may want to disable it now.

3. In LANrev Admin’s **Server Center** window, double-click the distribution point definition in the **Software Distribution** > **Distribution Points** category.

   The **Distribution Point** window opens. (It is described in detail in “New Distribution Point” on page 725.)

4. Enter the packages root path. This is the local path on the server of the directory in which LANrev is to store software installers. This path may be different on each server.

5. If the distribution point the definition of which you are editing is to be the master server, check the **Is master distribution point** option.

   The master distribution point serves as the source of software installers for the other (mirror) distribution points, as discussed in “Structure” on page 294. There must always be exactly one master distribution point.

   Because the master distribution point gets traffic from the mirror distribution points in addition to the agents, it should have enough processor power and network bandwidth to not become a bottleneck.

6. Click **OK**.

7. Repeat the process for all other distribution point definitions. Continue with updating the software packages as described below.

Updating software packages

NOTE Because of limitations of the Windows operating system, macOS software packages must be updated from a LANrev Admin running under macOS.

To update an existing software package to be compatible with the new architecture:

1. Make sure that the software installer (including any auxiliary files it may need) is available in the Finder on your computer.

2. In LANrev Admin’s **Server Center** window, double-click the software package definition in the **Software Distribution** > **Software Packages** category.

   The **Software Package** window opens. (It is described in detail in “New Software Package” on page 700.)

3. Click the **Select** button and select the software installer.

   It does not matter where the installer is located, for example, it does not need to be on a server.

4. Click **OK**.

5. Repeat the process for all other software package definitions and upload the changes to the LANrev Server using the **Save Distribution and Licensing Info** command from the **Server** menu.

LANrev checks and uploads the installers to the master distribution point. From there, they are automatically and transparently distributed in the background to the mirror servers – you no longer need to manually copy the installers to all distribution points.

Uninstalling LANrev components

In general, components of LANrev are uninstalled using the standard mechanisms of the host operating systems or an included uninstaller, although there are some exceptions.

For details, see the description for each component:

- **LANrev Server** (page 65)
- **LANrev MDM Server** (page 66)
- **LANrev PXE Server** (page 66)
- **LANrev Admin** (page 66)
- **LANrev Remote (desktop application)** (page 66)
- **InstallEase** (page 66)
- **Configure iOS Apps** (page 66)
- **LANrev Agent** (page 66)
- **LANrev Apps** (page 67)
- **LANrev Find** (page 68)
- **LANrev Remote (mobile app)** (page 68)
- **LANrev Safe** (page 68)
- **Third-Party tools** (page 68)

LANrev Server

- macOS: Use the uninstaller included on the LANrev disk image.
- Windows: Use the **Programs** control panel (the name may be different, depending on the version of Windows).

If the server was used as a staging server, you must manually remove any software stored for installation on the server computer, if desired.

LANrev MDM Server

- macOS: Use the uninstaller included on the LANrev disk image.
- Windows: Use the **Programs** control panel (the name may be different, depending on the version of Windows).

If the server was used as a software distribution point, you must manually remove any software stored for installation on the server computer, if desired.

LANrev PXE Server

Use the **Programs** control panel (the name may be different, depending on the version of Windows).

LANrev Admin

- macOS: Move the following files and folders to the trash:
  - LANrev Admin.app
  - ~/Library/Application Support/LANrev Admin/
  - ~/Library/Preferences/com.poleposition-sw.lanrev_admin.plist
- Windows: Use the **Programs** control panel (the name may be different, depending on the version of Windows).

LANrev Remote (desktop application)

LANrev Remote is a part of the LANrev Admin installation and is also uninstalled together with it.

InstallEase

Drag the application file into the trash

Configure iOS Apps

Drag the application file into the trash.

LANrev Agent

You can use LANrev Admin to uninstall the agent from multiple administered computers in one step. For macOS and Linux computers, this must be done from a macOS computer running LANrev Admin; uninstalling the agent from a Windows computer must be done from a Windows computer running LANrev Admin.

To uninstall multiple agents in one step:

1. In the **Agent Deployment Center** window, select all computers from which you want to remove the agent.

   On each computer, there must be a user account with admin privileges. The accounts on the selected computers must have the same name and password.

If the names or passwords differ, select the computer in multiple batches, with each batch having an account with the same credentials.

On macOS and Linux computers, SSH must be enabled.

2. Right-click any of the selected computers and choose **Remove Agent** from the context menu.

3. Enter the access credentials for the admin account.

   For macOS and Linux, enter SSH credentials. For Windows computers, enter NetBIOS credentials.

4. Click **OK**.

To uninstall LANrev Agent from a computer manually:

- macOS: Use the uninstaller included on the LANrev disk image.
- Windows: Use the **Programs** control panel (the name may be different, depending on the version of Windows).
- Linux: Follow the procedure below.

To manually uninstall LANrev Agent from a Linux computer:

1. Copy the “LANrev Agent (Linux).lmp” file to the Linux computer.

2. In a terminal window, change to the directory to which you copied the file and enter:
   tar -zxvf "LANrev Agent (Linux).lmp"

3. In the terminal window, enter:
   sudo amlcd-installer.sh uninstall

LANrev Apps

You can remove LANrev Apps from managed devices in different ways, as described below. Note however, that devices remaining under MDM management must first be removed from any profiles that auto-install LANrev Apps. Otherwise, the app can be removed but may be immediately reinstalled.

To use LANrev Admin to uninstall LANrev Apps from multiple devices using a policy:

1. Create a new policy, as described in “Working with policies” on page 245.

   If desired, you can also modify an existing policy.

2. Add LANrev Apps to this policy as a forbidden app.

3. Add all devices from which you want to remove LANrev Apps to the policy.

To use LANrev Admin to uninstall LANrev Apps from a selected managed device:

1. In the **Mobile Devices** window, display the mobile device in the sidebar and click on its **Applications** subcategory.

   The applications installed on the device are listed in the main part of the window.

2. Right-click the copy of LANrev Apps and choose **Delete Application** from the context menu.

To uninstall LANrev Apps locally on the device, use the uninstallation mechanism of the mobile device’s operating system.

LANrev Find

LANrev Find can be uninstalled in the same ways as described for LANrev Apps, above.

LANrev Remote (mobile app)

LANrev Remote can be uninstalled in the same ways as described for LANrev Apps, above.

LANrev Safe

LANrev Safe can be uninstalled in the same ways as described for LANrev Apps, above.

Third-Party tools

For uninstalling a third-party tool that you may have installed as part of the LANrev system, such as FOG, see the documentation of the tool.

Part 2: Using LANrev

The Using LANrev part of the manual describes how to accomplish specific tasks with LANrev:

“Accounts and agent access” on page 70 covers the creation, administration, and appointing of administrator accounts and of agent access privileges.

“Gathering and managing information” on page 94 covers how to collect and display information with LANrev.

“Controlling computers” on page 144 describes performing a range of actions on administered computers from LANrev Admin.

“Working with mobile devices” on page 181 covers the management of mobile devices and the software on them through an MDM server.

“Working with files” on page 283 explains copying and manipulating files on administered computers

“Installing software” on page 293 describes using the Software Distribution Center for automated software installations.

“Monitoring licenses” on page 348 covers using the License Monitoring Center to ensure license compliance and finding prohibited software.

Chapter 3 *Accounts and agent access*

LANrev uses a system of accounts and access rights to control the flow of information and prohibit unauthorized access. Setting them up correctly is necessary to ensure that LANrev gathers and displays all the information you need.

Setting up and configuring these accounts and access rights is explained in this section:

Overview

LANrev's access control centers on two main issues:

- Which administrators can do what in the system?
- Which server can access which agents? This, of course, is only an issue in systems with multiple servers.

This is discussed in more detail below.

Administrator accounts

There are two types of administrator accounts in LANrev, standard accounts and superadministrator accounts.

The two types differ in two respects:

- Superadministrators can create, configure, and delete administrator accounts; normal administrators cannot do this (except for changing their own passwords).
  Superadministrators are indicated by yellow icons (👤) in the **Server Center** window's sidebar.
- Standard administrators can see – and send commands to – only those administered computers to which they have been expressly assigned. Depending on the preference settings, superadministrators may be able to see all computers on which an LANrev Agent is installed.
  Standard administrators are indicated by black icons (👤) in the **Server Center** window's sidebar.

All account information is stored on LANrev Server, so that an account has the same settings irrespective of the computer from which the administrator is logged in.

Exactly on which server the information is stored can be configured: By default, each LANrev server stores its own information. But by entering the address of another server in a server's settings, you can direct it to not keep its own administrator account information but instead use that from the specified server.

Any changes made to the information on the 'parent' server is automatically propagated to all 'child' servers, simplifying account management in large organizations.

Active Directory integration

LANrev automatically takes advantage of Active Directory if it is present in your network. Active Directory users from groups that you specify in the **Server Settings** dialog are listed in the **Server Center** window and can be assigned LANrev administrator privileges. Any changes to the user names or passwords in Active Directory are mirrored in LANrev.

Administrator privileges

All administrators can execute commands targeting the devices to which they have been assigned. Which commands an administrator is permitted to execute can be configured in the Administrator Center; by default, every administrator can execute all commands.

In addition, the program functions to which an administrator has access can also be configured in a finely-grained way. For example, you can prevent an administrator from creating or changing installation packages without restricting other options.

NOTE While these functions can be disabled for superadministrators as well, these administrators can – because of their ability to configure accounts – always re-enable them for their own accounts. Only standard administrators can really be prevented from using these functions.

The relation of agents to servers

Each agent can be accessed only from servers that are explicitly noted in the agent's settings (by IP address or DNS name). That means that other servers are unable both to send commands to these agent's computers or collect information from them.

These servers are called inventory servers. Each agent can have any number of inventory servers, all of which have the same level of access.

In addition, one server can be specified for software distribution and one for license monitoring. Only these servers can access the respective functions of the agents. They can be the same server or different ones. They may be among the specified inventory servers or may be separate LANrev servers.

Agent access

As noted above, not all administrators can access all agents. Except for administrators for whom the **Can manage all devices** setting has been enabled, administrators can see information only from administered devices to which they have been expressly assigned.

This makes it possible to, for example, have administrators that are responsible only for the devices of one team without setting up a separate LANrev server for this purpose.

Administrator accounts

A person must have an administrator account to be able to access LANrev Admin (and, by extension, LANrev Server). Accounts are created in LANrev Admin but account information is stored on the LANrev server.

NOTE You can edit administrator accounts on a particular server only if that server is not set to use another server's account information in the **Server Settings** dialog's **General** tab (see page 781).

Creating an administrator account from scratch

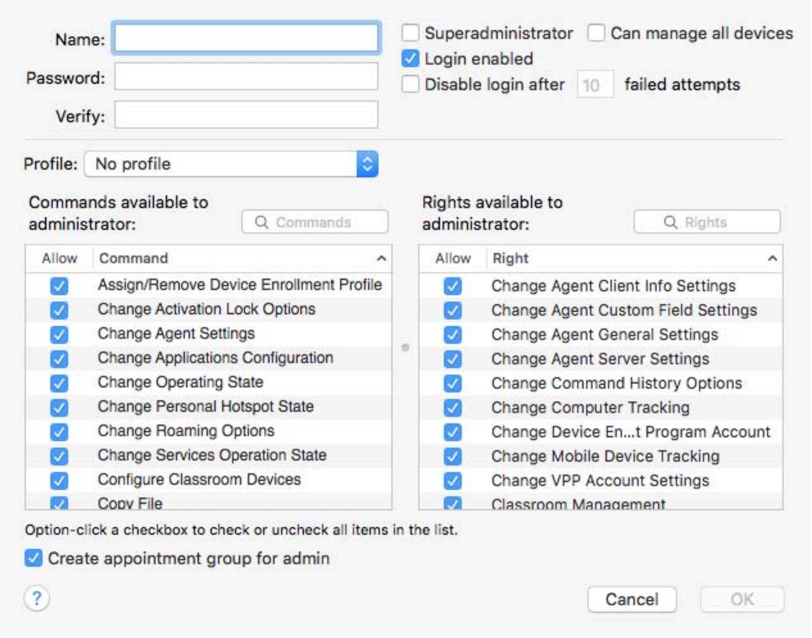
Administrator accounts can be created from scratch or you can assign administrator rights to an Active Directory user.

To create a new administrator account from scratch:

1. In LANrev Admin, open the **Server Center** window.

2. Choose **Administrator Setup** > **New Administrator** from the action menu to create a new account.

The **New Administrator** dialog opens:



Name:
Password:
Verify:

☐ Superadministrator ☐ Can manage all devices
☑ Login enabled
☐ Disable login after 10 failed attempts

Profile: No profile

Commands available to administrator:

Allow	Command
☑	Assign/Remove Device Enrollment Profile
☑	Change Activation Lock Options
☑	Change Agent Settings
☑	Change Applications Configuration
☑	Change Operating State
☑	Change Personal Hotspot State
☑	Change Roaming Options
☑	Change Services Operation State
☑	Configure Classroom Devices
☑	Copy File

Rights available to administrator:

Allow	Right
☑	Change Agent Client Info Settings
☑	Change Agent Custom Field Settings
☑	Change Agent General Settings
☑	Change Agent Server Settings
☑	Change Command History Options
☑	Change Computer Tracking
☑	Change Device En...t Program Account
☑	Change Mobile Device Tracking
☑	Change VPP Account Settings
☑	Classroom Management

Option-click a checkbox to check or uncheck all items in the list.

☑ Create appointment group for admin

3. Enter the name for the account and the password. Repeat the password in the **Verify** field.

   Both account names and passwords are case-sensitive.

4. Set the desired privileges for the account:

   - **Superadministrator**: The administrator has superadministrator privileges. (These privileges are explained in "Administrator accounts" on page 70.) If the option is unchecked, the account is a standard account.
   - **Can manage all devices**: If this option is checked, the administrator can access all devices that are managed on LANrev Server. If the option is unchecked, the administrator can manage only devices to which the account has been expressly assigned.
   - **Login enabled**: The account is active. If this option is not checked, the account is disabled.
   - **Disable login after**: If this option is checked, only a specified number of wrong passwords are permitted per login attempt. If more incorrect passwords are entered, the account is automatically disabled. To enable it again, another administrator must recheck the **Login enabled** option (see above).
     This option is not available for superadministrator accounts.

5. If desired, assign a profile from the **Profile** pop-up menu to the account and proceed with step 9. If you do not assign a profile, continue with the next step.

Assigning a profile sets the commands and rights available to the account. The **Profile** pop-up menu also offers commands to create and delete profiles as well as edit their names.

Note: Profiles are merely presets: You can change the settings for an individual account at any time without affecting the profile, and changing the profile does not affect existing accounts which are based on it.

6. In the commands list, uncheck all commands that you want the administrator not to be able to execute on client devices.

   The individual commands are described in "Commands menu" on page 399 and "Mobile Devices" on page 538.

   Note: Even if you set up a superadministrator account that cannot execute all commands, a superadministrator can always change his or her own account to regain those rights.

7. In the rights list, uncheck all rights that you want the administrator not to have.

   The individual rights are described in "New Administrator" on page 758.

   Note: If you uncheck the Manage Mobile Devices right, the administrator is unable to send commands to managed mobile devices, even if the commands themselves are enabled in the administrator account (see step 6).

   Note: As with commands, you cannot effectively deny rights to superadministrators.

8. If desired, save the configuration of commands and rights you have created as a profile by choosing **Save As** from the **Profile** pop-up menu.

   Creating a profile lets you later quickly create other accounts with the same commands and rights.

9. Check **Create appointment group for admin** if you want to have two groups in the **Server Center** window's sidebar listing, respectively, all computers and all mobile devices to which this administrator has been assigned.

10. Click **OK** to create the account locally.

11. Create more administrator accounts if desired, as described above, starting with step 2.

12. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on LANrev Server.

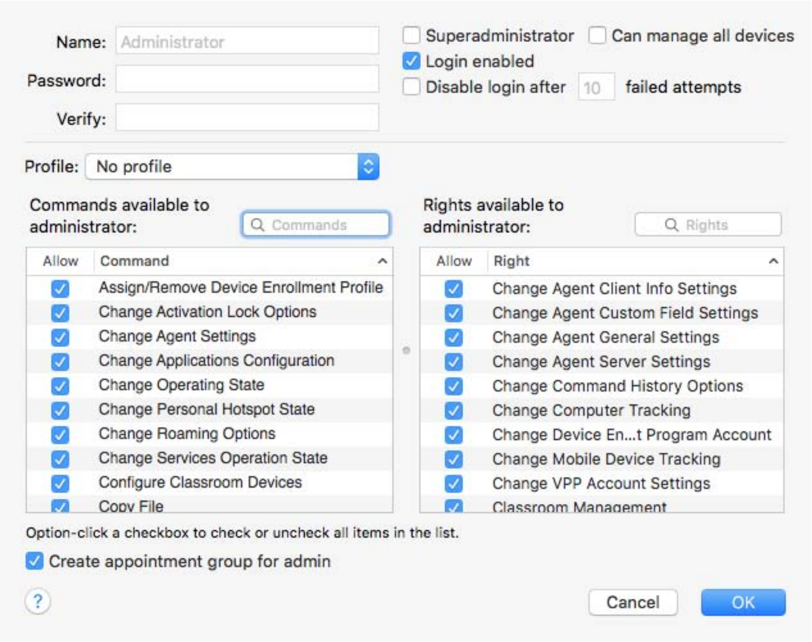
Giving administrator access to an Active Directory account

If you are connected to an Active Directory server, you can simply assign administrator rights to Active Directory users:

1. Make sure that the Active Directory group containing the Active Directory account in question has been activated in the **Server Settings** dialog’s **Active Directory** pane.

2. In the **Server Center** window, drag the desired users from the **Active Directory** group to the **Administrators** group.

   The **Administrator** dialog opens:



Name: Administrator

Password:

Verify:

☐ Superadministrator ☐ Can manage all devices

☑ Login enabled

☐ Disable login after 10 failed attempts

Profile: No profile

Commands available to administrator: Commands

Allow	Command
☑	Assign/Remove Device Enrollment Profile
☑	Change Activation Lock Options
☑	Change Agent Settings
☑	Change Applications Configuration
☑	Change Operating State
☑	Change Personal Hotspot State
☑	Change Roaming Options
☑	Change Services Operation State
☑	Configure Classroom Devices
☑	Copy File

Rights available to administrator: Rights

Allow	Right
☑	Change Agent Client Info Settings
☑	Change Agent Custom Field Settings
☑	Change Agent General Settings
☑	Change Agent Server Settings
☑	Change Command History Options
☑	Change Computer Tracking
☑	Change Device En...t Program Account
☑	Change Mobile Device Tracking
☑	Change VPP Account Settings
☑	Classroom Management

Option-click a checkbox to check or uncheck all items in the list.

☑ Create appointment group for admin

3. Set the desired privileges and other options for the account as described above in step 4 and following.

   Note: You cannot change from within LANrev the names or passwords of administrator accounts imported from Active Directory.

4. Click **OK** to create the account locally.

   The account is not yet saved on the server; this has to be done in a separate step as described below.

5. Create more administrator accounts if desired, as described above.

6. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on LANrev Server.

   LANrev uses Active Directory for this account’s log-in process.

Note that when the Active Directory user account from which you have created the administrator account is removed from Active Directory or is moved out of the Active Directory groups that have been specified in server settings, the administrator account will be deleted from LANrev.

Editing administrator accounts

To change the name, password, or access privileges of an existing administrator account:

1. Open the **Server Center** window.
2. Right-click the account that you want to edit and choose **Edit Administrator** from the contextual menu.

   In the window's table area – but not in the sidebar – you can also select and edit multiple accounts. Note, however, that editing the names or passwords is not possible in that case.

   Editing the names or passwords of accounts based on Active Directory users is never possible from within LANrev.
3. Set the account options as desired, as explained in "Creating an administrator account from scratch", above.
4. Click **OK**.
5. Edit more administrator accounts if desired, as described above.
6. When you are done, choose **Save Administrator Info** from the **Server** menu to store the new accounts on LANrev Server.

NOTE Administrators can change their own passwords using a different method, as described in "Changing your password" on page 78.

Disabling and enabling administrator accounts

To temporarily disable an administrator account, uncheck the **Login enabled** option for the account in the **Administrator** dialog that you can open using the **Edit Administrator** command.

To re-enable the account, check the option again.

NOTE At least one superadministrator account must be enabled at all times.

Disabling the account of an administrator who is currently logged in does not log out that user but prevents him or her from logging back in once having logged out.

Deleting administrator accounts

To delete an administrator account, right-click it and choose **Remove Administrator**.

NOTE At least one enabled superadministrator account must exist at all times.

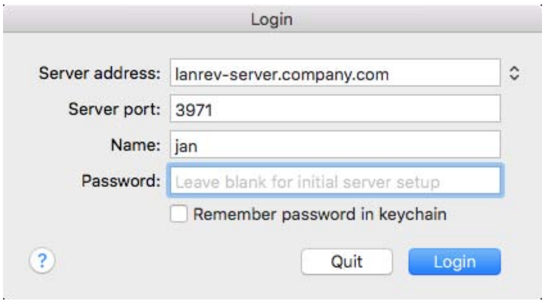
Deleting the account of an administrator who is currently logged in does not log out that user but prevents him or her from executing commands and from logging back in once having logged out.

Using administrator accounts

Once an administrator account has been set up, it can be used for logging in. Administrators can log in, log out, and change their passwords, as described below.

Logging in

When LANrev Admin is started, it presents a login dialog:



Server address: lanrev-server.company.com

Server port: 3971

Name: jan

Password: Leave blank for initial server setup

□ Remember password in keychain

To log in, make sure that the server address and port are correct. Enter your username and password, both of which are case-sensitive, and click **OK**. (There may be a limit on how many wrong passwords can be entered before the login capability of the account is disabled, as described in “New Administrator” on page 758.)

NOTE If the administrator account is based on an Active Directory user account, you can use the display name, the account name, or the login name to log in.

You are now logged in and can use LANrev according to the privileges of the specified account.

If you check **Remember password in keychain**, you can in future log in from this user account of your computer without having to enter a password.

IMPORTANT Setting this option gives everybody with access to your user account on the Macintosh automatic access to LANrev. You may want to disable the option if this could include unauthorized people.

NOTE There is no way to use LANrev Admin without logging in.

Logging out

There is no way to explicitly log out of LANrev. Logging out is automatic when you quit LANrev Admin; the only other way to log out of your account is to switch to another account, as described below.

Switching accounts

You can at any time switch to another administrator account without having to quit LANrev Admin.

To do so, choose **Switch Administrator and Server** from the **LANrev Admin** menu to open the **Login** dialog (see above). Enter the new account name and password.

You can also log in to a different server at the same time. The pop-up menu beside the **Server address** field provides access to the most recently used servers.

Changing your password

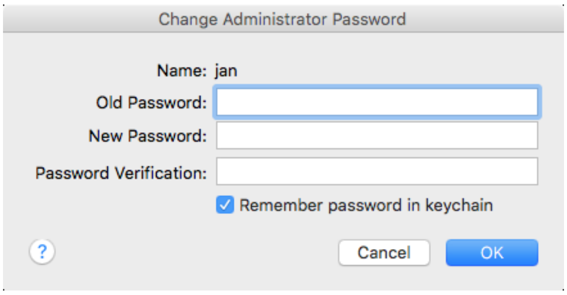
You can change your password irrespective of whether you are logged into a parent or a child server.

NOTE Passwords can only be changed for accounts that were created in LANrev. Passwords for Active Directory accounts must be changed on the Active Directory server.

To change the password of your own account:

1. Choose **Change Administrator Password** from the **LANrev** menu.

   The **Change Administrator Password** dialog opens:



Change Administrator Password

Name: jan
Old Password:
New Password:
Password Verification:
☑ Remember password in keychain

2. Enter your current password and your new password. Re-enter the new password in the Password verification field.

   Note: Passwords are case-sensitive.

3. If desired, you can store the new password in the keychain. Doing so has security implications that are described in "Logging in", above.

4. Click **OK**.

The new password is effective immediately. If you were logged into a slave server, the password is propagated to the master server (and from there to any other slave servers there may be).

NOTE For changing passwords of other administrator, see "Editing administrator accounts" on page 76. Only superadministrators can change other administrators' passwords.

Assigning servers to agents

LANrev Agents communicate only with servers that have been expressly assigned to them. This prevents unauthorized access to the administered computers using the considerable capabilities of agents.

Agents can be assigned any running LANrev Server as their inventory server (the main server through which they are managed). They can also be assigned to multiple inventory servers and, if desired, to software distribution and license monitoring servers.

You can assign servers to agents when you install the agents, as described in "Installing LANrev Agent" on page 35. Assigning the servers at any time after the installation is explained below.

Assigning inventory servers to agents

Inventory servers are the 'normal' LANrev Servers with which agents communicate to receive commands and send information. Each agent can be configured to communicate with any number of inventory servers.

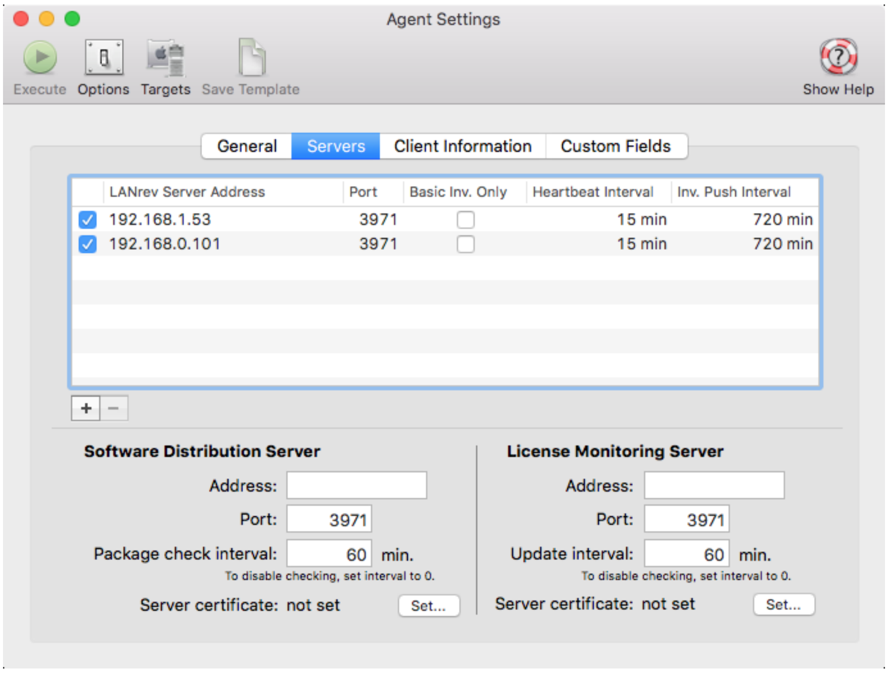
To assign inventory servers to agents:

1. In any browser window, select the computers to which you want to assign servers.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Agent Settings**.

The **Agent Settings** dialog opens; click the **Servers** tab:



	LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval
☑	192.168.1.53	3971	□	15 min	720 min
☑	192.168.0.101	3971	□	15 min	720 min

Software Distribution Server

Address:

Port: 3971

Package check interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

License Monitoring Server

Address:

Port: 3971

Update interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

In this dialog pane, you can add and remove inventory servers as well as change the communication settings.

3. To add a server, click the **+** button.

   A new line is added to the table of servers and the **Inventory Server Properties** dialog is opened. Enter the IP address or DNS name of the server.

4. If desired, you can edit the other settings for the server:

   - The port number is the port on which the server communicates with agents (and the LANrev Admin). This should not normally be changed.
     Note: If the built-in macOS or Windows firewall is active on the server computer, the specified port is automatically opened in the firewall.
   - The heartbeat interval is the interval in which the agent lets the server know that it is still running.
   - The inventory push interval is the interval in which the agents sends changes in the state of its computer – in any information item, except those in the processes, fonts, files, printer, and startup item information.
   - If a server is to act only as the software distribution server or license monitoring server for this server, set **Set Inventory** to **Basic**. This prevents unneeded inventory information from being sent to the server from the agent and so both reduces the network load and keeps the server from becoming bogged down by unneeded data. For administered client computers, set it to **Standard**. If desired, check any additional categories, such as **Include**

font information, that you want automatically transmitted with every inventory update.

5. If the **Server certificate** field does not display "valid", click the **Set** button and choose the certificate for the server.

   Creating server certificates is described in "Exporting a server certificate" on page 21.

   Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

6. Click **OK** to close the **Inventory Server Properties** dialog.

7. If desired, create more servers to add.

8. To remove a server, that is, to stop agents from communicating with it, select it in the list and click the **–** button.

9. To rearrange servers in the list, drag them.

   The topmost server in the list is the main inventory server; this server acts as the software distribution server and/or license monitoring server if no dedicated servers are specified for these roles.

   The order of the other servers has no effect.

10. Before changing the agents' settings, review the table:

    - All target agents will communicate with checked servers.
    - Only target agents will communicate with unchecked servers that already communicate with them. (That is, the status of these servers with regard to the target agents will not be changed.)
    - None of the target agents will communicate with servers that are not in the list. (That is, any server not in the list will be removed from all target agents.)

11. Click **Execute**.

The agents are reconfigured according to the command settings.

Assigning software distribution or license monitoring servers to agents

For each agent, there is at most one software distribution server (which it contacts for software installations handled by LANrev) and one license monitoring server (to which it sends reports on licensed software).

If no servers are specified for this function in the initial installation, the main inventory server (the topmost one the list in the Server tab of the Agent Settings dialog) is set to take on these roles as well. If you configure the servers manually on an agent and leave out the address for the software distribution server and/or the license monitoring server, the respective function is disabled on that agent.

If another setup is intended, you can assign one software distribution server and one license monitoring server to each agent. These servers can be the same or different servers; they may be among the inventory servers assigned to the agent, but need not be.

These servers can be assigned during the installation of the agent, as described in "Installing LANrev Agent" on page 35, or later, as described in "Assigning inventory servers to agents", above.

If desired, you can at the same time adjust the intervals in which the selected agents are to check for new software and report on installed software, respectively.

Appointing administrators to devices

Only administrators for whose accounts the **Can manage all devices** option is set can access all agents on computers and all mobile devices. All other administrators can only access devices to which they have been expressly assigned. This means that they can send commands only to these computers and mobile devices and display information only from them.

Appointing administrators to devices is done via appointment groups. An appointment group contains either a list of computers or a list of mobile devices. When administrators are added to an appointment group, they get access to all devices in that group. Both administrators and devices may belong to more than one appointment group.

Managing appointment groups and appointing administrators is described in detail in:

- "Working with appointment groups" on page 82
- "Appointing administrators" on page 85

Working with appointment groups

Appointment groups combine a number of devices with one or more administrators, thereby giving these administrators access to the computers.

Setting up a standard appointment group

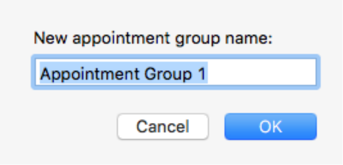
There are standard appointment groups – where administrators are manually added and removed – and smart appointment groups that automatically include all computers meeting specified criteria.

Managed computers and mobile devices have different appointment groups – you cannot mix the two types of devices in one group.

To set up a standard appointment group:

1. Open the **Server Center** window.
2. From the action menu, choose **Administrator Setup** > **New Computer Appointment Group** or **Administrator Setup** > **New Mobile Devices Appointment Group**, depending on the type of device you want to manage in this group.

   The **Administrators Group** dialog opens:

   New appointment group name:

   Appointment Group 1

3. Enter the desired name and click **OK**.

   The new group appears in the **Server Center** window's sidebar.

4. To add devices to the group, drag them on top of the group icon from a browser window or the **Mobile Devices** window.

   To remove devices, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

5. To store the appointment group specification on LANrev Server, choose **Save Administrator Info** from the **Server** menu.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new appointment group is lost unless you save the changes at some point before quitting LANrev. Also, other administrators can use the group only after you have saved it to the server.

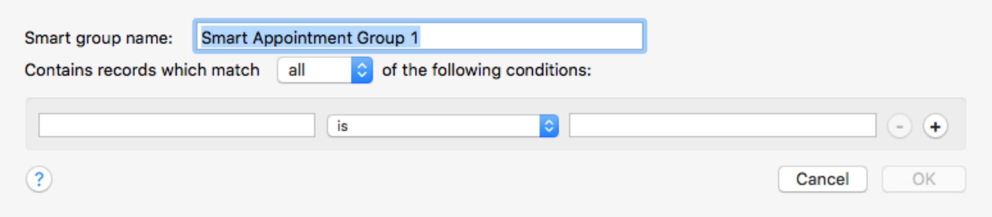
Setting up a smart appointment group

Smart appointment groups automatically include all computers or mobile devices meeting criteria that you specify when setting up the group.

To create a new smart appointment group:

1. Open the **Server Center** window.
2. From the action menu, choose **Administrator Setup** > **New Smart Computer Appointment Group** or **Administrator Setup** > **New Smart Mobile Devices Appointment Group**, depending on the type of device you want to manage in this group

The **Smart Group** dialog opens:



Smart group name: Smart Appointment Group 1

Contains records which match all of the following conditions:

3. Enter the name for the new appointment group and specify the conditions that devices must meet to be included in the group.

   To define a condition, specify an information item in the left-hand text field, choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

   When the text insertion mark is in a field, you can drag a column from the Columns drawer into the field.

   With the **+** and **–** buttons, you can add and remove conditions.

4. If you have specified more than one condition, specify through the upper pop-up menu whether devices must meet one or all of the conditions.

5. Click **OK**.

   The new group appears in the **Server Center** window's sidebar.

6. To store the appointment group specification on LANrev Server, choose **Save Administrator Info** from the **Server** menu.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new appointment group is lost unless you save the changes at some point before quitting LANrev. Also, other administrators can use the group only after you have saved it to the server.

Reusing smart groups

You can drag any custom smart computer group from other browser windows or from within the **Server Center** window to the **Appointments** category in the **Server Center** window's sidebar to create a new computer appointment group with the same specifications as the smart group. In the same way, you can reuse smart mobile device groups from the **Mobile Devices** window.

Editing appointment groups

You can change the names of all appointment groups by double-clicking them in the **Server Center** window's sidebar or by selecting them and choosing **Edit Appointment Group** command from the context menu.

For smart appointment groups, you can also change the selection criteria:

1. Double-click the group in the **Server Center** window's sidebar.
2. The Smart Group dialog opens.
3. Change the selection criteria as described above in **Setting up a smart appointment group**.

Deleting appointment groups

To delete an appointment group, right-click it and choose **Remove Appointment Group** from the context menu.

As described for setting up groups, above, you must update the information stored on the LANrev server using the **Save Administrator Info** command for the change to become permanent.

Appointing administrators

To appoint an administrator to a device:

1. Make sure that the **Server Center** window is open.
2. In any browser window, select the computers to which you want to appoint administrators. Or select mobile devices in the **Mobile Devices** window.

   Note: The **Agent Deployment Center** *window cannot be used for this purpose.*
3. Drag the selected devices to the appointment group through which it is to be managed.

   This appoints all administrators belonging to the group to the selected devices.

Removing administrators from agents or mobile devices

To stop all administrators of an appointment group from managing a particular device:

1. In the **Server Center** window, select the appointment group to which the device belongs.

   All devices in the group are listed in the main part of the **Server Center** window.
2. Right-click the device and choose **Remove from Group** from the context menu.

The administrators in the appointment group can no longer access the removed computer or mobile device.

NOTE If some of the group's administrators also belong to other appointment groups that contain the device in question, they can still administer the device based on their membership in that other group.

To stop an administrator from managing the devices in an appointment group:

1. In the **Server Center** window, expand the appointment group and select the **Assigned Administrators** subcategory.

   All administrators that are assigned to the group are listed in the main part of the **Server Center** window.

2. Right-click the administrator and choose **Remove from Group** from the context menu.

The administrator can no longer access the computer or mobile devices in the appointment group (unless he is assigned to another group that also contains some or all of the devices).

Viewing the device to which an administrator is appointed

To see the devices to which an administrator is currently assigned, select the administrator account in question in the **Server Center** window's sidebar.

The devices are listed in the table area; computers are listed in the upper half and mobile devices in the bottom half.

Viewing the administrators who are appointed to a device

To see the administrators who are currently appointed to administer a given device, expand the device in the sidebar of a browser window (such as the **Computers** window or the **Mobile Devices** window) and select its **Administrators** subcategory. The assigned administrators are listed in the main part of the window.

To view the administrators assigned to multiple devices at a glance, add the **Administrator Name** information item to any browser window displaying computer information or the **Mobile Devices** window.

Note that in both cases only administrators are listed who are specifically assigned to the devices. Administrators who can access the device because the **Can manage all devices** setting has been activated for their account are not listed.

Setting MDM access rights for mobile devices

Performing actions on managed mobile devices requires the corresponding access rights to be set when the devices are enrolled. This is done in the **MDM** tab of the server settings.

Should these privileges later be changed, devices must be re-enrolled for the changes to become effective on them.

These procedures are described in:

- "Specifying MDM access rights" on page 87
- "Updating MDM access rights on enrolled iOS devices" on page 89

NOTE Setting MDM access rights does not apply to Android devices.

Specifying MDM access rights

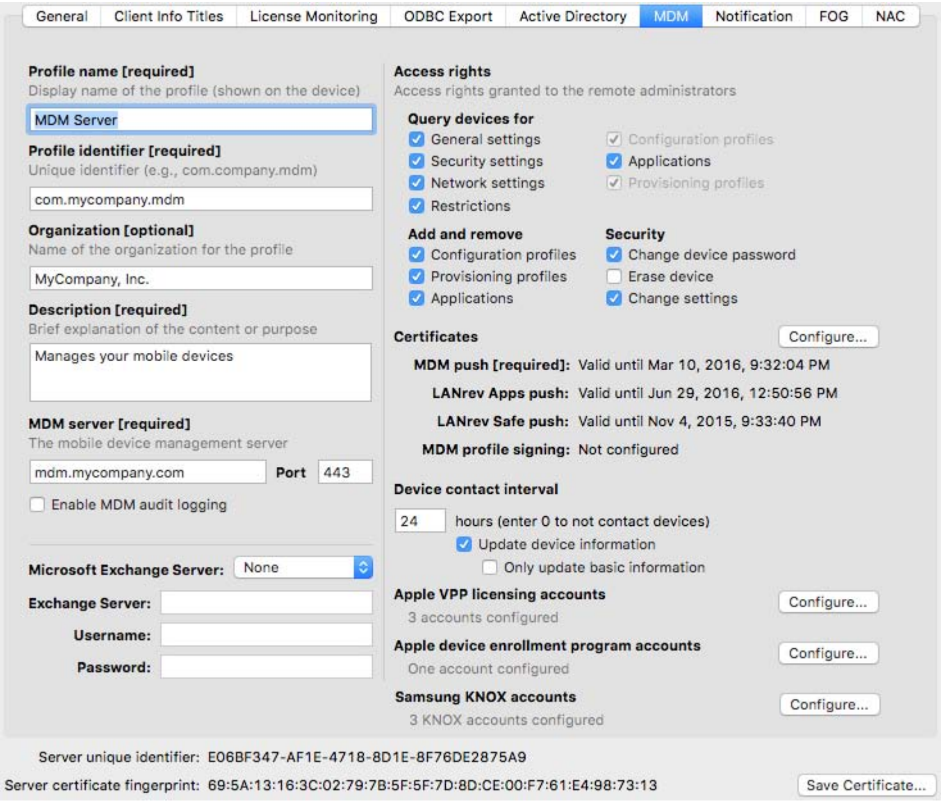
To specify the access rights that administrators may have on the mobile devices managed through this LANrev server:

1. Open the **Server Center** window.

2. In the sidebar, click **Server** > **Server Settings**.

3. In the main part of the window, click the **MDM** tab.

The MDM settings are displayed:



Profile name [required]
Display name of the profile (shown on the device)
MDM Server

Profile identifier [required]
Unique identifier (e.g., com.company.mdm)
com.mycompany.mdm

Organization [optional]
Name of the organization for the profile
MyCompany, Inc.

Description [required]
Brief explanation of the content or purpose
Manages your mobile devices

MDM server [required]
The mobile device management server
mdm.mycompany.com **Port** 443

□ Enable MDM audit logging

Microsoft Exchange Server: None
Exchange Server:
Username:
Password:

Access rights
Access rights granted to the remote administrators

Query devices for
☑ General settings
☑ Security settings
☑ Network settings
☑ Restrictions
☑ Configuration profiles
☑ Applications
☑ Provisioning profiles

Add and remove
☑ Configuration profiles
☑ Provisioning profiles
☑ Applications

Security
☑ Change device password
□ Erase device
☑ Change settings

Certificates Configure...
MDM push [required]: Valid until Mar 10, 2016, 9:32:04 PM
LANrev Apps push: Valid until Jun 29, 2016, 12:50:56 PM
LANrev Safe push: Valid until Nov 4, 2015, 9:33:40 PM
MDM profile signing: Not configured

Device contact interval
24 hours (enter 0 to not contact devices)
☑ Update device information
□ Only update basic information

Apple VPP licensing accounts Configure...
3 accounts configured

Apple device enrollment program accounts Configure...
One account configured

Samsung KNOX accounts Configure...
3 KNOX accounts configured

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9
Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13 Save Certificate...

4. In the **Access rights** section, check all privileges that you want administrators to be able to have.

   The available privileges are described in “MDM” on page 787.

   Note that for a particular administrator to have a privilege, the appropriate option must be checked in her or his account setup, as described in “Administrator accounts” on page 72. However, privileges that are unchecked in the **MDM** tab are unavailable to all administrators (including superadministrators), irrespective of their individual account settings.

5. Choose **Server** > **Save Server Settings** to save the changes on the server.

6. If there are iOS devices already enrolled on the server, you must re-enroll them to update the access privileges on them. See “Updating MDM access rights on enrolled iOS devices”, below, for details.

You have changed the privileges that administrators can have on newly enrolled mobile devices. Privileges on already enrolled iOS devices will be updated once these devices are re-enrolled.

Updating MDM access rights on enrolled iOS devices

Any changes to the MDM access privileges for managed iOS devices (as set in the **MDM** tab of the server settings) require any devices that are already enrolled to be re-enrolled before the changes take effect on them.

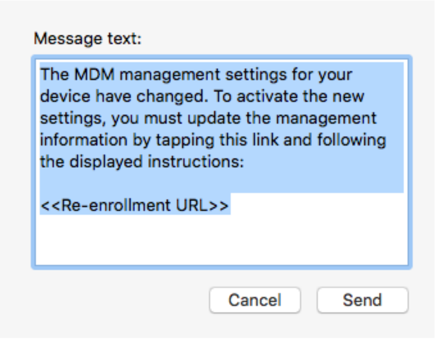
You are prompted to send re-enrollment messages to these devices whenever you change the MDM settings, but you also can do so manually at a later time:

1. In the **Mobile Devices** window, select all devices that need to be re-enrolled.

   To quickly find all affected devices, you can create a smart group that collects all devices where the **Mobile Device MDM Profile Up-to-date** has the value "No".

2. Right-click the selected devices and choose **Send Re-enrollment Message to Device** from the context menu.

   The **Message** dialog is displayed:



Message text:

The MDM management settings for your device have changed. To activate the new settings, you must update the management information by tapping this link and following the displayed instructions:

<<Re-enrollment URL>>

3. Enter a text that you want to send to your users.

   Make sure not to delete the URL placeholder; it will automatically be replaced with the actual enrollment URL including the device identifier in the message sent to the users.

   If you accidentally delete the placeholder, the URL will be appended to the end of the message.

4. Click **Send** to send the message to all selected devices.

All users will receive the message the next time they contact mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If they are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

When a user taps the URL, the device will be re-enrolled in a process that is similar to the original enrollment process. When that process is finished, the new MDM privileges are in effect on the device.

Creating placeholder records for computers

For the most part, LANrev can only work with computers on which LANrev Agent has been installed. However, a very limited subset of the functionality is also available for computers on which no agent is installed.

To use this capability, you must manually create a placeholder record for each computer in question, as explained below.

Functions available for placeholder records are limited to:

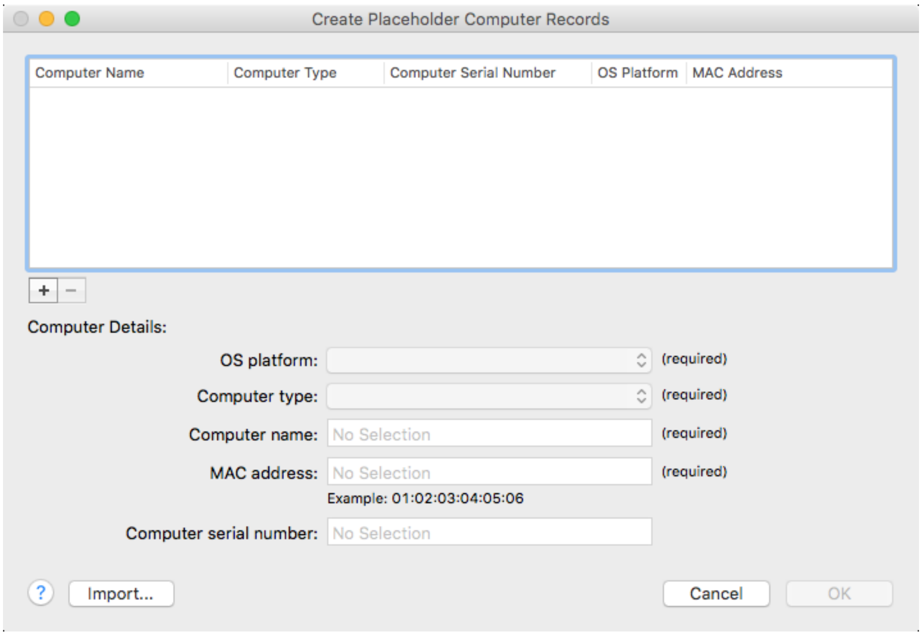
- Displaying them in browser windows. No information is displayed beyond the data that was entered when the placeholder record was created.
  Display-related functions of browser windows – such as sorting, finding, or exporting – also extend to placeholder records, but functions that actually access the device – such as gathering information – do not.
- The only command that is available for computers represented by placeholder records is **Reinstall Windows Computer**.

Creating placeholder records for computers

To create placeholder records for one or more computers without agents:

1. Choose **Server** > **Create Placeholder Computer Records**.

   The **Create Placeholder Computer Records** dialog opens:



2. Click the **+** button.

   The entry fields in the dialog become active.

3. Enter the information for the placeholder record you are about to create.

   The serial number is optional, all other information is required.

   Instead of manually entering the information from each record, you can also click the **Import** button to import the data from a tab-delimited text file. The file format is described in “Create Placeholder Computer Records” on page 493.

4. To create additional placeholder records, repeat step 2 and 3.

5. Click **OK** to save the placeholder records displayed in the dialog.

Deleting placeholder records

To delete existing placeholder records:

1. In any browser window, select the records you want to delete.

2. Right-click the selected records and choose **Remove from Server** from the context menu.

The records are deleted after you have confirmed that you want to do so.

Exporting and importing server settings

If you want to migrate an LANrev Server installation from one computer to another, most of the data, such as the database tables, can be transferred easily by copying the relevant files from the LANrev Server folder. (This folder is found at “/Library/Application Support/LANrev Server” on macOS systems and “Program Files\Pole Position Software\LANrev Server” on Windows systems.)

Transferring custom field definitions and server settings, however, is less straightforward (except between macOS systems, where you can simply copy the “/Library/Preferences/com.poleposition-sw.lanrev_server” file).

There is a command line option that lets you save the server settings and custom field definitions as an XML file and import it into any other server instance. The file is compatible with both the macOS and Windows versions of the server.

Exporting server settings on macOS

To export server settings and custom field definitions from a server installed on macOS:

1. On the computer on which the server is installed, launch Terminal.

2. In the Terminal window, enter this command and press Return:

```
sudo /Library/Application\ Support/LANrev\
Server/LANrev\ Server.app/Contents/MacOS/LANrev\
Server --ExportPreferences <export file>.plist
```

<export file> is the path and name of the settings file you want to create.

3. When prompted, enter the password to execute the command with superuser privileges.

The settings file is created with the specified name at the specified location.

Exporting server settings on Windows

To export server settings and custom field definitions from a server installed on Windows:

1. On the computer on which the server is installed, launch cmd.exe with administrator privileges.

2. In the terminal window, browse to the Program Files\Pole Position Software\LANrev Server directory.

3. In the terminal window, enter this command and press Enter:

   ```
   LANrev Server.exe --ExportPreferences <export
   file>.plist
   ```

   <export file> is the path and name of the settings file you want to create.

The settings file is created with the specified name at the specified location.

Importing server settings on macOS

To import server settings and custom field definitions into a server installed on macOS:

1. On the computer on which the server is installed, launch Terminal.

2. In the Terminal window, enter this command and press Return:

   ```
   sudo /Library/Application\ Support/LANrev\
   Server/LANrev\ Server.app/Contents/MacOS/LANrev\
   Server --ImportPreferences <import file>.plist
   ```

   <import file> is the path and name of the settings file you want to import.

3. When prompted, enter the password to execute the command with superuser privileges.

The specified settings file is imported and the existing server settings and custom field definitions are overwritten.

Importing server settings on Windows

To import server settings and custom field definitions into a server installed on Windows:

1. On the computer on which the server is installed, launch cmd.exe with administrator privileges.
2. In the terminal window, browse to the Program Files\Pole Position Software\LANrev Server directory.
3. In the terminal window, enter this command and press Enter:

   ```
   LANrev Server.exe --ImportPreferences <import file>.plist
   ```

   <import file> is the path and name of the settings file you want to import.

The specified settings file is imported and the existing server settings and custom field definitions are overwritten.

Chapter 4 Gathering and managing information

LANrev helps you manage your network by gathering a wide range of information on the administered computers. This section describes how to use this feature:

Overview

The gathering and managing of information by LANrev centers on the central database integrated in LANrev Server: The server collects information from the agents and stores it in its database. When you want to see specific information, the LANrev Admin application queries the server for it and displays it on your workstation.

In principle, the flow of information is very simple: It is gathered by the agents, stored by LANrev Server, and displayed by LANrev Admin.

Gathering information

Information collection by the server is mostly automatic. Some types of information – on processes, fonts, startup items, services and files – are collected on request only to avoid wasting local processing power and network bandwidth.

This is described in more detail in “Gathering information” on page 95.

Custom information

If LANrev’s extensive list of information items does not provide the data you are looking for, you can extend it by creating custom information items.

This is described in detail in “Custom information” on page 106.

Information storage on the server

LANrev Server stores the collected information in an internal relational database. There are a number of tables in this database, among them for storing computer, process, file, font, and LANrev account information. There also are numerous subtables for information on volumes, memory slots, and other objects that can appear multiple times per computer.

The columns in these tables are called information items; they are the basic unit of information display in LANrev.

Displaying information

Information is displayed by LANrev Admin is so-called browser windows. These windows consist mainly of a table where the columns are information items and the rows represent computers or other objects such as files.

You request particular pieces of information in two basic ways from the server:

- To compare the same information for several administered computers, you put the respective information items into browser windows.
- To view in-depth information on one computer, you select that computer in the sidebar of a browser window.

This is described in more detail in “Displaying information” on page 132.

Rearranging information

You can narrow down and rearrange information in a browser window by searching for text, creating groups of related computers, and sorting browser windows.

This is described in more detail in “Searching, filtering, and sorting” on page 138.

Custom information

LANrev provides ten text fields for storing any kind of information on client computers and retrieve it from there. These fields are intended for information, for example, inventory numbers, that cannot automatically be determined by the software.

This is described in more detail in “Manually edited information” on page 118.

Gathering information

Gathering information is performed by the LANrev agents which then forward this information to all inventory servers (that is, LANrev servers) that are specified for them.

Some types of information are gathered and forwarded automatically in regular intervals; other types – information on files, processes, fonts, printers, and startup items – are gathered only on request.

In addition, updates for the automatically gathered information can be requested manually in cases where you do not want to wait for the next scheduled update.

This is discussed in detail in:

- “Configuring automatic information gathering” on page 96
- “Gathering and updating information manually” on page 98 (includes gathering information on computers, processes, fonts, printers, and startup items)
- “Gathering information on files” on page 102
- “Gathering information on registry entries” on page 103
- “Collecting USGCB SCAP compliance reports” on page 105

Information can also be gathered from administered computers by adding an action to a computer group. See “Working with actions” on page 178 for details.

Configuring automatic information gathering

Information on the computers’ hardware and software is gathered automatically by the LANrev agents and transmitted to the servers. The interval in which these transmissions happen can be configured.

NOTE The LANrev agents are smart about their transmissions: They send only changed information to the server, not everything they collect.

To configure the update interval:

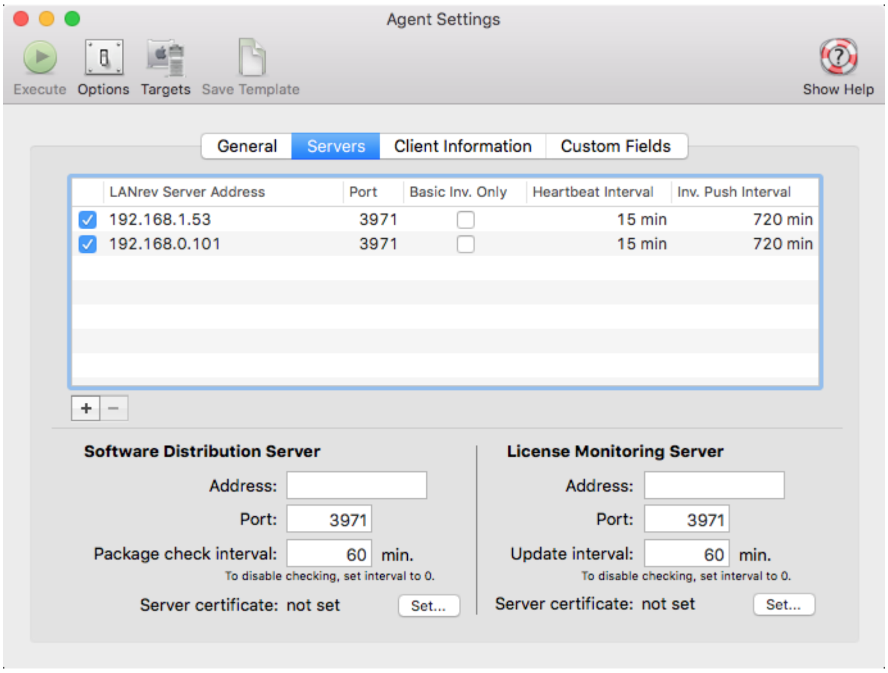
1. In any browser window, select the computers on which you want to configure the update interval.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Agent Settings**.

   The **Agent Settings** dialog opens.

3. Click the **Servers** tab:



	LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval
☑	192.168.1.53	3971	□	15 min	720 min
☑	192.168.0.101	3971	□	15 min	720 min

Software Distribution Server

Address:

Port: 3971

Package check interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

License Monitoring Server

Address:

Port: 3971

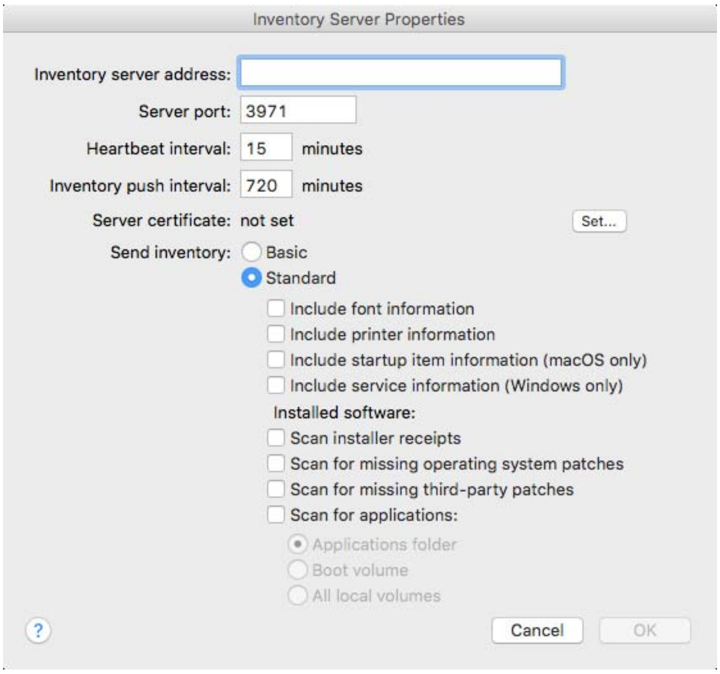
Update interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

4. Select the desired LANrev Server in the table, double-click the entry in the **Inventory Push Interval** column, and enter the desired update interval in minutes.

   Double-click the desired LANrev Server in the table.The **Inventory Server Properties** dialog opens:



Inventory server address:

Server port: 3971

Heartbeat interval: 15 minutes

Inventory push interval: 720 minutes

Server certificate: not set Set...

Send inventory: ○ Basic

● Standard

□ Include font information

□ Include printer information

□ Include startup item information (macOS only)

□ Include service information (Windows only)

Installed software:

□ Scan installer receipts

□ Scan for missing operating system patches

□ Scan for missing third-party patches

□ Scan for applications:

● Applications folder

○ Boot volume

○ All local volumes

5. Enter the desired update interval in minutes.

If several servers are specified in the table – that is, the selected agents are sending inventory information to several LANrev Servers – the interval can be set separately for each of them.

6. Make sure that the servers you have updated have a checkmark in the table and click **Execute**.

The new interval is set on all target computers.

Gathering and updating information manually

While most information that LANrev provides is gathered automatically, some of it is only provided on request to avoid using up too much network bandwidth. This applies to information on:

- Fonts
- Printers
- Processes
- Startup items
- Installed software (including missing patches)

NOTE While information on files also is collected in a manually triggered procedure, the process is somewhat different, as described in "Gathering information on files" on page 102.

This information can be requested manually, as detailed below. By the same process, information that is normally gathered automatically can be updated before the next automatic update is due.

While the server sends all information it receives to the admin application when required, information can also be manually loaded from the server to LANrev Admin. This is also described below.

Manually gathering computer, font, printer, or startup item information

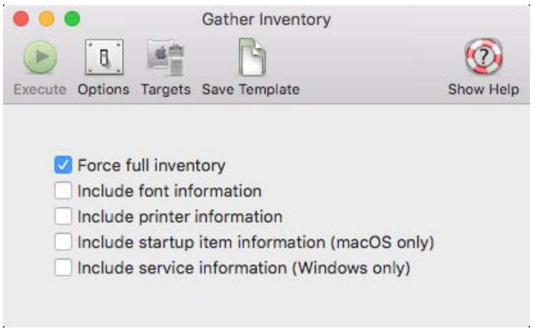
To collect this information manually:

1. In any browser window, select the computers from which you want to gather the information.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Gather Inventory Information**.

The **Gather Inventory** dialog opens:



☑ Force full inventory
□ Include font information
□ Include printer information
□ Include startup item information (macOS only)
□ Include service information (Windows only)

3. To cause the agents on the target computers to transmit all computer information (that is, not just information that has changed) to the server, check **Force full inventory**.

   To gather font, printer, startup item, or service information, check the appropriate option.

   Note: Changed computer information is always transmitted when the **Gather Inventory Information** *command is executed, even if none of the options in the dialog is checked.*

4. Click **Execute**.

The agents on the target computers collect the requested information and send it to the server, where it is entered in the appropriate tables. The server automatically forwards the information to the admin application if any browser windows display corresponding information items.

Manually gathering process information

To collect process information manually:

1. In any browser window, select the computers from which you want to gather the information.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Gather Process Information**.

   The **Gather Processes** dialog opens.

3. Click **Execute**.

The agents on the target computers collect the process information and send it to the server, where it is entered in the Processes table. The server automatically forwards the information to the admin application if any browser windows display process-related information items.

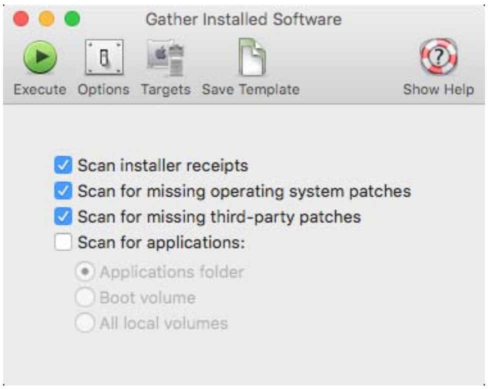
Manually gathering information on installed software

To collect information on installed software:

1. In any browser window, select the computers from which you want to gather the information.

2. From the **Commands** menu, choose **Gather Installed Software**.

   The **Gather Installed Software** dialog opens.



☑ Scan installer receipts
☑ Scan for missing operating system patches
☑ Scan for missing third-party patches
□ Scan for applications:
● Applications folder
○ Boot volume
○ All local volumes

3. Check the desired options:

   - **Scan installer receipts**: LANrev checks the target computers for installer receipts and lists the corresponding software. Note that only some installers generate such receipts.
   - **Scan for missing operating system patches**: If this option is checked, LANrev scans target computers for operating system patches. The Agent queries the operating system for any applicable patches that are available but not yet installed and reports them back. *Note: Patches that have been rejected by you or another administrator are not reported as missing.*
   - **Scan for missing third-party patches**: LANrev compares its internal list of applicable third-party patches with the patches that are actually installed on the computer and notes all patches that are missing. (A list of supported applications is available in article 22276 in the knowledge base.)
     Only computers for which **Include in third-party patch management** has been checked in the **Agent Settings** dialog are scanned.
     Note: Patches that have been rejected by you or another administrator are not reported as missing.
   - **Scan for application**: LANrev scans the specified locations and their subfolders for applications:
     - **Applications folder**: the **Applications** folders (on macOS targets) or the **Program Files** folders (on Windows targets; folder chosen according to the local environment variable settings)
     - **Boot volume**: the entire startup volume

- **All local volumes**: all volumes currently mounted on the target computer, except server volumes

Note: Scanning entire hard disks can create a huge amount of data. We recommend scanning the boot volume or all local volumes only when really required.

You must check at least one option.

If one method of searching for software is deselected, any software from the target computers that has been previously found by this method is deleted from LANrev's database.

For example, if **Scan installer receipts** is unchecked, LANrev will delete any software on the current target computers that was identified by its installer receipts from the Installed Software table. That software will no longer be displayed in the **Installed Software** window.

4. Click **Execute**.

The agents on the target computers collect the installed software information and send it to the server, where it is entered in the Installed Software table. On Windows clients, available App-V applications are also gathered. The server automatically forwards the information to the admin application if any browser windows display related information items.

Note that previously collected installed software information is deleted before the targets are searched: If one method of searching for software is deselected, any software from the target computers that has been previously found by this method is deleted from LANrev's database.

For example, if **Scan installer receipts** is unchecked, LANrev will delete any software on the current target computers that was identified by its installer receipts from the Installed Software table. That software will no longer be displayed in the **Installed Software** window.

Manually requesting information from the server

LANrev Server automatically notifies any connected admin applications when new information arrives and forwards the information that is displayed in browser windows.

If such transmissions are interrupted, for example, due to abnormal network conditions, you can force a reupdate by choosing **Synchronize All Tables** from the **Server** menu. You can also update just some records by selecting them in any browser window and choosing **Synchronize Selected Records**, which updates all information for the selected computers.

Synchronizing causes the server to send just updated information. When you suspect that some information in LANrev Admin is out of date and is not getting updated through synchronizing, you can press the Option key and choose **Reload All Tables** or **Reload Selected**

Records, respectively, to force a complete update of the information stored locally by LANrev Admin.

Gathering information on files

Gathering information on files is different from the other information gathering methods – except gathering information on registry entries – in that it is always done selectively, that is, not on all files on a target computer but only on those meeting specified conditions.

NOTE Viewing files is not covered in this section; see “Viewing files from administered computers” on page 286 for information on how to view the contents of a file on an administered computer.

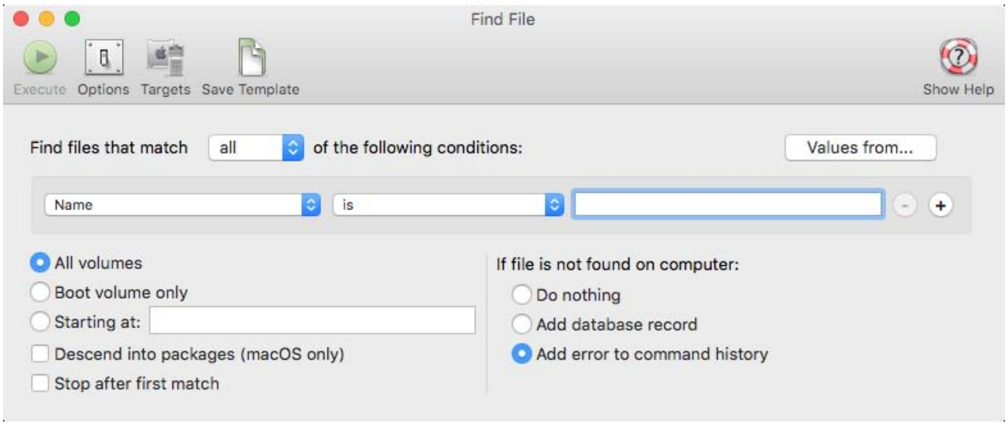
To gather information on files:

1. In any browser window, select the computers from which you want to gather the file information.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Find File**.

   The **Find File** dialog opens:



Find files that match all of the following conditions:

Name is

● All volumes
○ Boot volume only
○ Starting at:
□ Descend into packages (macOS only)
□ Stop after first match

If file is not found on computer:
○ Do nothing
○ Add database record
● Add error to command history

3. Specify the parameters of the files you want to find.

   The available parameters are described in “Files” on page 867, except for **Checksum**.

   Checksum lets you select files by the MD5 checksums, making sure that files are really the desired version, without changes. Note that the checksum has to be calculated dynamically; doing so for a large number of files requires a huge amount of processing power on the client computer and should therefore be avoided. Always combine the **Checksum** criterion with other criteria that make sure that the checksum needs to be calculated only for a small number of files. Checksums are not available for folders.

When you search for files by version number, make sure to observe the platform conventions:

- On macOS, version numbers often have one or two dots, for example, 2.0, 2.0b1, or 2.0.1.
- On Window, version numbers usually have three dots, for example, 1.2.123.54 or 2.120.43.3.

In general, you should specify the more selective criteria (for example, name or bundle identifier) first and less selective criteria (for example, **Is File**) later to speed up the search.

Note: By default, LANrev finds both visible and invisible files. If you wish to find only visible files, specify an additional condition "Is invisible No," making sure to search for files fulfilling "all" conditions (see next step).

4. Choose whether you want to find files that meet at least one of the specified conditions (logical OR) or only files that meet all of them (logical AND).

5. Specify the other options:

   - Whether to search all volumes, just the boot volume, or just a specific folder and its subfolders.
   - Whether to search inside packages on macOS targets.
   - Whether to search just the first matching file on each target computer or all matching files.

6. Specify the behavior when no file matching your specifications is found on a particular target computer:

   - Choose **Do Nothing** to disregard the result. This simply causes neither a record for the non-existing file nor an error to be generated.
   - Choose **Add database record** to create an entry in the file database for the missing file. Entries for missing files are distinguished in particular by having the value "No" in the **File Found** information item.
   - Choose **Add error to command history** to create an entry in the command history noting that the specified file could not be found on the target computer in question.

7. Click **Execute**.

The agents on the target computers search their local hard disks for matching files and send information on them to the server, where it is entered in the Files table. The server automatically forwards the information to the admin application if any browser windows display corresponding information items.

Gathering information on registry entries

Gathering information on registry entries is different from the other information gathering methods – except gathering information on files – in that it is always done selectively, that is, not on the entire registry contents of target computers but only on those entries that meet specified conditions.

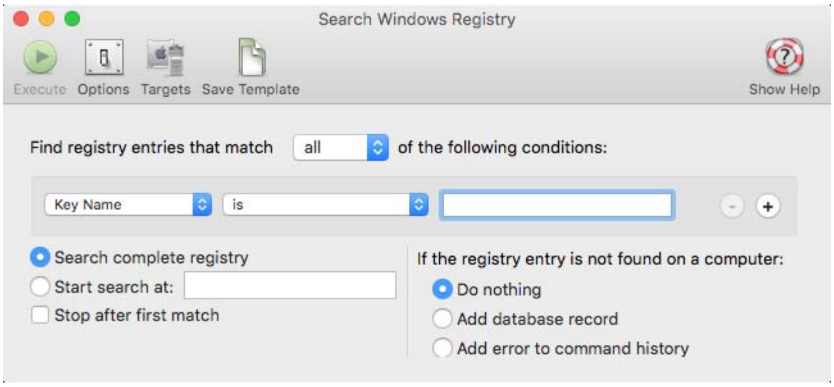
To gather information on registry entries:

1. In any browser window, select the computers from which you want to gather the registry entry information.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Search Windows Registry**.

   The **Search Windows Registry** dialog opens:



Find registry entries that match all of the following conditions:

Key Name is

● Search complete registry
○ Start search at:
□ Stop after first match

If the registry entry is not found on a computer:
● Do nothing
○ Add database record
○ Add error to command history

3. Specify the parameters of the registry entries you want to find.

   You can search for keys and values by name or path.

   When you specify a path, you can use environment variables, as described in "Environment variables" on page 176.

4. Choose whether you want to find registry entries that meet at least one of the specified conditions (logical OR) or only entries that meet all of them (logical AND).

5. Specify the other options:

   - Whether to search the entire registries or just the subset at a specified path.
   - Whether to find just the first matching entry on each target computer or all matching entries.
   - What to do when no matching registry entry is found on a target computer. You can specify that nothing happens, an error message is inserted in the command history, or a special entry is created in LANrev's Registry Entries database table.

   These special entries specify the registry entry that was searched for and have a value of "No" in the **Registry Entry Found** information item. This allows you, for example, to easily find all computers missing a particular entry.

6. Click **Execute**.

The agents on the target computers search their local registries for matching entries and send information on them to the server, where it is entered in the Registry Entries table. The server automatically forwards the information to the admin application if any browser windows, for example, the **Registry Entries** window, display corresponding information items.

Collecting USGCB SCAP compliance reports

Using LANrev, you can execute and collect USGCB SCAP compliance reports on administered computers.

NOTE It is beyond the scope of this manual to discuss the theory, purpose, or use of USGCB SCAP reports. For details on these reports, consult the relevant section of NIST's website at http://usgcb.nist.gov/index.html or other applicable documentation.

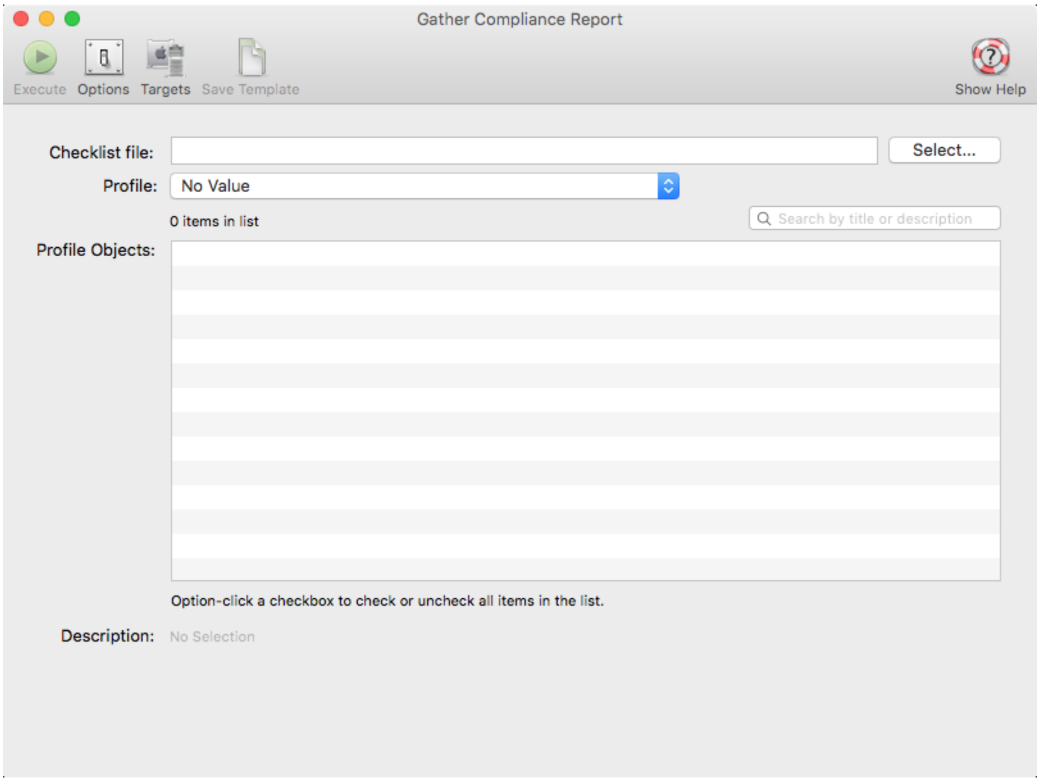
To collect USGCB SCAP reports:

1. In any browser window, select the computers for which you want to collect the compliance reports. Compliance reports can only be collected from Windows clients.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Gather Compliance Report**.

The **Gather Compliance Reports** dialog opens:



Checklist file:

Profile: No Value

0 items in list

Profile Objects:

Option-click a checkbox to check or uncheck all items in the list.

Description: No Selection

3. Click the **Select** button to choose the file containing the report definition or drag the file into the **Checklist file** field from the desktop.

4. From the **Profile** menu, choose the desired profile from the list of profiles available in the chosen report definition file.

5. In the **Profile objects** list, uncheck all options that you do not want to include in the profile.

6. Click **Execute**.

The specified target computers are evaluated according to all chosen report options. The results, along with the calculated scores and the overall pass result, are stored in LANrev’s internal Compliance Report database table and can be displayed in the **Compliance Reports** window.

Custom information

In addition to LANrev’s extensive list of predefined information items, you can create your own custom information fields to support special requirements. The data for these custom information fields is gathered by the agents and transmitted to the server together with standard inventory information.

Preparing and using custom information fields is a multi-step process:

1. First, you define the fields on the server. Fields can be either manual or dynamic.

   Data is entered manually into manual fields or it is imported from text files.

   Defining a dynamic field involves specifying scripts or other data sources for macOS and Windows clients that will be evaluated on the administered computers to gather the desired information. The return values are used as the dynamic custom fields' values.

   Creating either type of custom information field is described in "Defining custom information fields" on page 108.

2. If desired, you can share custom information fields among multiple LANrev servers. This is done by setting servers up to not keep their own field definitions but mirroring those of a specified other server.

   Details are available in "Setting up custom information field mirroring" on page 111.

3. Then, assign the custom information fields to agents.

   Custom information fields can gather information only from agents to which they are assigned.

   This is described in "Assigning custom information fields" on page 112.

4. If desired, import data for manual information fields from text files.

   This is described in "Importing data into custom information fields" on page 115.

5. Finally, insert the custom information fields in browser windows in the same way as standard information items or use them as variables in text that is displayed on or sent to client devices.

   This is described in "Using custom information fields" on page 114.

6. Optionally, you can export or import the definitions of custom information fields.

   This is described in "Exporting and importing custom information field definitions" on page 117.

To gather the information for a dynamic custom information item, LANrev evaluates the specified data sources on the assigned administrated computers.

Defining custom information fields

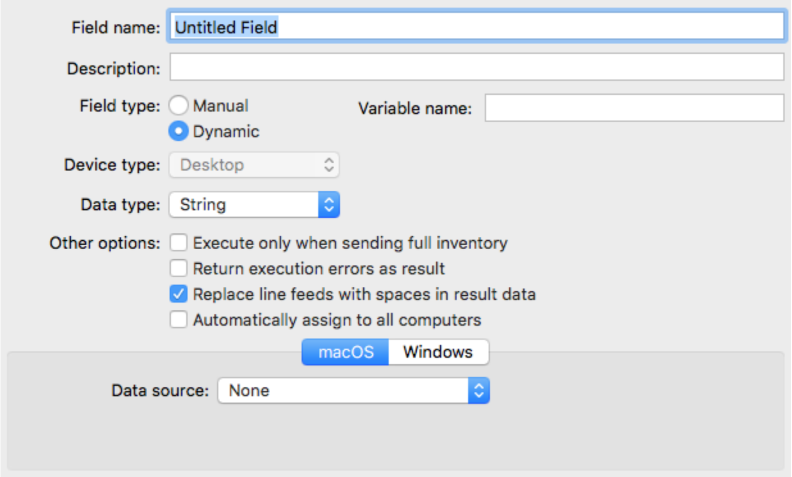
Custom information fields are defined on the LANrev server, making them available to all administrators.

To define a custom information field:

1. Open the **Server Center** window.

2. Choose **Custom Information Fields** > **New Custom Information Field** from the action menu.

   The **Custom Information Field** dialog is displayed in the main part of the **Server Center** window:



Field name: Untitled Field

Description:

Field type: ○ Manual ● Dynamic

Variable name:

Device type: Desktop

Data type: String

Other options:
- □ Execute only when sending full inventory
- □ Return execution errors as result
- ☑ Replace line feeds with spaces in result data
- □ Automatically assign to all computers

Data source: None

3. Enter a name and a description for the new custom information field.

   The description will be displayed as a tooltip for the field.

4. Specify whether the field is to be a manual or a dynamic field:

   - Manual fields are for humans to individually enter data into. (Although data can be imported from external text files, as described in “Importing data into custom information fields” on page 115.)
   - Dynamic fields receive their data from automated sources such as scripts or registry entries on the client computers. They behave much like standard information items.

5. Specify whether the custom information field is intended for desktop devices or mobile devices.

   Dynamic fields can only be used for desktop devices; custom fields intended for mobile devices must be manual fields.

   If desired, you can enter a variable name in the **Variable name** field. If you do so, this custom field can then be used as an information variable in commands, actions, and configuration profiles in the form `${<VariableName>}`, as described in “Information variables” on page 175.

6. Specify the desired data type of the field:

   - **String**: Any unformatted text
   - **Number**: Any number. You can choose from several display formats.
   - **Boolean**: True or false
   - **Date**: A point in time
   - **File Version**: A version number according to the conventions of the target platform
   - **IP Address**: An IPv4 address (for example, 192.168.0.1)
   - **Enumeration**: A value from a predefined list. Specify the list of possible values using the + and - buttons. (All values are treated as strings.)
     Enumeration is not available for dynamic fields; choose **String** instead.

7. If you have specified a manual field, continue with step 13.

8. Decide on when the data sources should be evaluated:

   - When they are to be executed only when a full inventory report is made, check the **Execute only when sending full inventory** option.
     Note: Full inventory reports are made by the agents when they are first contacted by a server, when they start up, or when they are sent the **Gather Inventory Information** *command with the "Force full inventory" option.*
   - When the scripts are to be executed every time the inventory is updated, uncheck the option.

   Having data sources evaluated only for full inventory reports is especially useful in the case of scripts taking a long time to run, involving user interaction, or gathering information that changes only rarely.

9. If you want execution errors to be returned, check the **Return execution errors as result** option.

   This will cause the agents to send any execution errors of a script as if they were the actual results. These values are then stored normally in the custom field.

   If the option is unchecked, no values are returned in case of execution errors and the field remains empty.

10. If the entire result is to be stored as a single line of text in the field, check the **Replace line feeds with spaces in result data** option.

11. If you want the custom field to always be available for all client computers (much as built-in information items are), check the **Automatically assign to all computers** option.

    If this option is unchecked, you have to assign the field manually to computers, as described in "Assigning custom information fields", below. This allows you, however, to give each computer only applicable fields, which may be useful if you have a large number of fields that each is relevant only for a subset of the administered computers.

12. Specify the scripts, other programs, or other data sources that are to be executed by choosing the desired option from the **Data Source** pop-up menu.

    Data sources are specified separately for macOS and Windows computers; each platform is optional but at least one must be specified.

    Because of limitations in the Windows operating system, it is not possible to specify programs with the **Other Executable** type for macOS clients in LANrev Admin for Windows. You can, however, edit custom information fields with this specification in LANrev Admin for Windows as long as you do not change the executable (or change it to one of the script types).

    Depending on the type of data source you specify, different options become available. These options are described in "New Custom Information Field" on page 767.

    Note: Any executables you specify must be available on your computer – either locally or on a mounted server volume – when you define the field. They do not need to be available later outside of the LANrev system, as they are stored on LANrev Server.

    The line endings of any specified scripts are automatically converted to the conventions on the target platform during the upload to LANrev Server. (However, LANrev does not convert line endings in any additional files that are upload as a consequence of you checking the **Transfer all files in folder containing the executable** option.)

13. If desired, create additional custom information fields.

14. From the **Server** menu, choose **Save Custom Information Fields** to upload the new field definitions to LANrev Server.

LANrev Admin uploads the field definition and the specified scripts or executables, if any, to LANrev Server.

The new custom information fields are available in the **Agent Information** > **Custom Fields** section of the **Information Items** window. For information on adding the fields to browser windows and entering information into manual fields, see "Using custom information fields" on page 114.

New dynamic custom information fields are used to actually gather information only if you have checked the **Automatically assign to all computers** option in step 11. Fields for which this option is not checked must be assigned to agents as described in "Assigning custom information fields", below. (This does not apply to manual custom information fields, which are always assigned to all computers.)

Editing custom information fields

To edit a custom information field, proceed as described above but click the field in the sidebar of the **Server Center** window in step 2.

Changes in custom information field definitions are propagated to affected clients (that is, clients to which the old field definition had been assigned) either upon their next ‘heartbeat’ contact with LANrev Server, when the **Gather Inventory Information** command is issued from LANrev Admin (your copy or somebody else’s), or when a different custom information field is assigned to that client. Any information gathered for the custom information field before any of these three events occurs will still use the old field definition.

Deleting custom information fields

To delete a custom information field, select it in the sidebar of the **Server Center** window and choose **Delete Custom Information Field** from the action menu.

Setting up custom information field mirroring

You can set up LANrev servers such that they receive their custom field definitions from a different server.

To make a server mirror another server’s custom information field definitions:

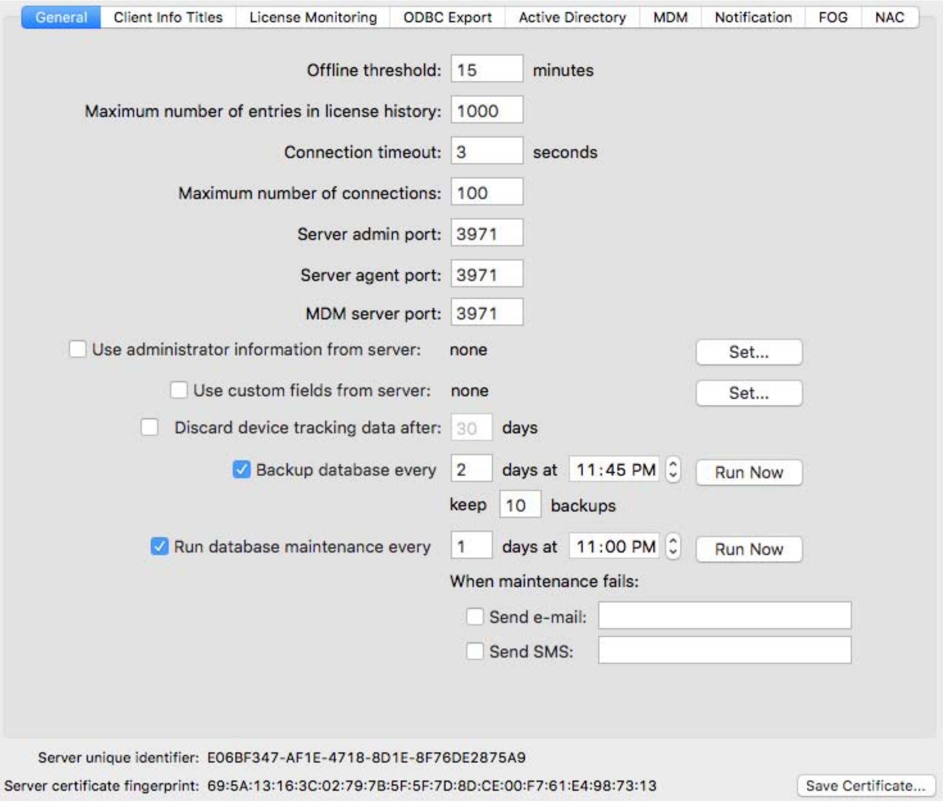
1. Make sure that you are connected to the server that you want to set up as a mirror.

   If you are not, use the Switch Administrator and Server command to connect to it.

2. Open the **Server Center** window.

3. Click the **Server** > **Server Settings** category in the sidebar.

The **General** pane of the **Server Settings** dialog is displayed in the main part of the **Server Center** window:



Offline threshold: 15 minutes

Maximum number of entries in license history: 1000

Connection timeout: 3 seconds

Maximum number of connections: 100

Server admin port: 3971

Server agent port: 3971

MDM server port: 3971

□ Use administrator information from server: none Set...

□ Use custom fields from server: none Set...

□ Discard device tracking data after: 30 days

☑ Backup database every 2 days at 11:45 PM Run Now

keep 10 backups

☑ Run database maintenance every 1 days at 11:00 PM Run Now

When maintenance fails:

□ Send e-mail:

□ Send SMS:

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9

Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13 Save Certificate...

4. In the **Use custom fields from server** field, enter the DNS name or IP address of the server that is to be mirrored. If the server communicates over a non-standard admin port, change the port accordingly.

   The description will be displayed as a tooltip for the field.

5. From the **Server** menu, choose **Save Server Settings** to upload the new settings to the LANrev server.

LANrev Admin uploads the settings. This overwrites any custom field definitions that are currently in effect on the server and overwrites them with the definitions from the specified server.

In future, changes on the mirrored server will automatically update this server.

Assigning custom information fields

LANrev gathers information for dynamic custom information fields only from computers to which these fields have been specifically assigned. Only fields with the **Automatically assign to all computers** option checked (and manual custom information fields) are assigned automatically; all other fields have to be assigned manually according to this procedure.

Not assigning fields automatically can have two benefits: First, scripts do not need to be executed on computers for which you are not interested in the information they produce. And second, you can use scripts that may not be compatible with all administered computers sharing a particular platform.

To assign a custom information field to computers:

1. Make sure that the custom information field has been defined, as described in “Defining custom information fields” on page 108.

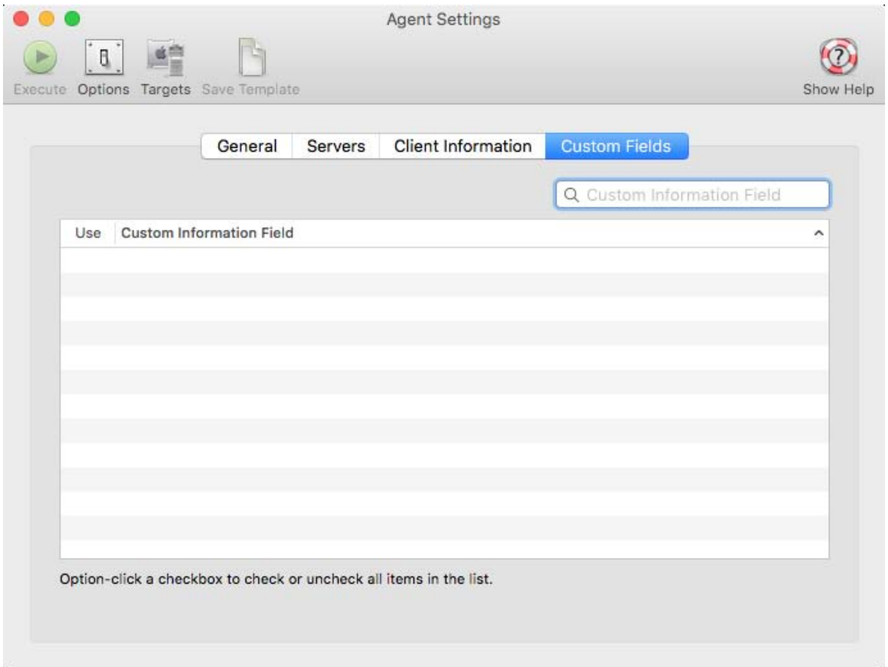
2. In any browser window, select the computers to which you want to assign the field.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

3. From the **Commands** menu, choose **Agent Settings**.

   The **Agent Settings** dialog is displayed.

4. Click the **Custom Fields** tab:



Option-click a checkbox to check or uncheck all items in the list.

5. Check all fields that you want to assign to the target computers and uncheck all fields that you do not want to be assigned to them.

   The assignment status of fields with the checkbox in the third state (⊟) remains unchanged.

6. Click **Execute**.

The checked fields are assigned to all computers in the target list. From now on, information from these fields is gathered from the target computers (either with each inventory update or only with full inventory reports, as specified in the fields' definitions).

The assigned fields are also displayed when the single computer view of one of the target computers is opened in a browser window as described in "Displaying an overview of a single computer" on page 135.

Unassigning custom information fields

To unassign a custom information field – preventing it from being evaluated on particular client computers – proceed as described above and make sure to uncheck the field in step 5.

Using custom information fields

Custom fields are used like normal information items.

Desktop custom fields are listed in the **Agent Information** > **Custom Fields** section of the **Information Items** window and can be used in browser windows like standard information items. (This is described in "Displaying information" on page 132.) Remember, however, that dynamic custom fields gather information only from computers to which they have been explicitly assigned, as described in "Assigning custom information fields" on page 112.

Custom fields for mobile devices are listed in the **Mobile Device Information** > **Custom Fields** section of the **Information Items** window. They are always manual information fields, not dynamic, and so do not need to specifically be assigned to devices.

All custom fields can also be used as variables in text that as is sent to or displayed on client devices, as long as a variable name has been specified for them, as described in "Defining custom information fields" on page 108. For more information on using custom information fields as variables, see "Information variables" on page 175.

Editing manual custom information fields

You can edit information in manual information fields (but not dynamic information fields) for one or for multiple computers or mobile devices.

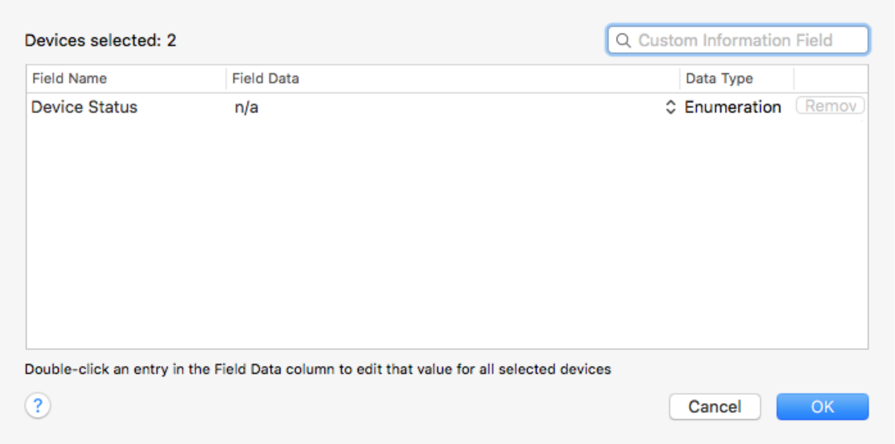
Note that you can also automatically assign values to manual custom information fields for devices that become members of computer groups and policies. This is described in "Working with actions" on page 178 and "Working with actions" on page 232, respectively.

To edit custom information fields manually:

1. In any browser window or the **Mobile Devices** window, select the computers or mobile devices for which you want to edit the field.

2. Right-click any of the selected computers and choose **Enter Custom Field Data** from the context menu.

The **Edit Custom Field Data** dialog is displayed:



Devices selected: 2

Field Name	Field Data	Data Type
Device Status	n/a	Enumeration

Double-click an entry in the Field Data column to edit that value for all selected devices

3. If you want to remove the content of a manual custom information field on all selected computers, click the **Remove** button in the row representing that field.

4. If you want to edit the content of a field, click in the **Field Data** column in the row of the field and enter the desired content.

5. Repeat step 3 or step 4 for other fields as desired.

6. Make sure that all fields that you want to modify for all selected computers are checked in the **Modified** column and all others are unchecked.

   Note: The **Modified** *column is not displayed if only one computer was selected before the dialog was opened.*

7. When you are done, click **OK**.

LANrev updates the content of the manual custom information fields on the selected computers.

Importing data into custom information fields

You can import data from text files into manual custom information fields.

(Note that you can also automate the import of this information, as described in “Automatically importing information” on page 122.)

To import data into custom information fields:

1. From the **File** menu, choose one of two commands, depending on the kind of custom information fields into which you want to import data:

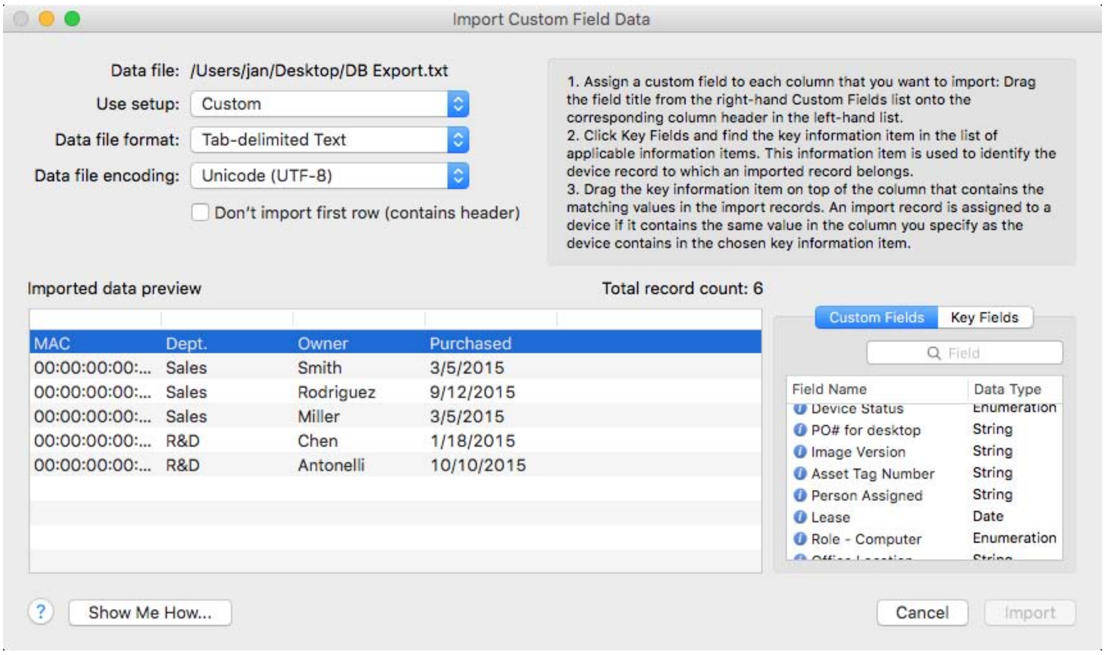
   - To import into custom information fields for desktop devices, choose **Custom Field Data for Desktop Devices**.
   - To import into custom information fields for desktop devices, choose **Custom Field Data for Mobile Devices**.

The operating system’s Open dialog is displayed.

2. Choose the desired text file and click **Open**.

   The text files must delimit records with returns and fields within records with tabs, commas, or semicolons. LANrev supports all common text encodings.

   When you click **Open**, the **Import Custom Field Data** dialog is displayed:



Import Custom Field Data

Data file: /Users/jan/Desktop/DB Export.txt

Use setup: Custom

Data file format: Tab-delimited Text

Data file encoding: Unicode (UTF-8)

□ Don’t import first row (contains header)

1. Assign a custom field to each column that you want to import: Drag the field title from the right-hand Custom Fields list onto the corresponding column header in the left-hand list.
2. Click Key Fields and find the key information item in the list of applicable information items. This information item is used to identify the device record to which an imported record belongs.
3. Drag the key information item on top of the column that contains the matching values in the import records. An import record is assigned to a device if it contains the same value in the column you specify as the device contains in the chosen key information item.

Imported data preview

Total record count: 6

MAC	Dept.	Owner	Purchased
00:00:00:00:...	Sales	Smith	3/5/2015
00:00:00:00:...	Sales	Rodriguez	9/12/2015
00:00:00:00:...	Sales	Miller	3/5/2015
00:00:00:00:...	R&D	Chen	1/18/2015
00:00:00:00:...	R&D	Antonelli	10/10/2015

Field Name	Data Type
Device Status	Enumeration
PO# for desktop	String
Image Version	String
Asset Tag Number	String
Person Assigned	String
Lease	Date
Role - Computer	Enumeration
Office Location	String

3. If you have saved a fitting setup, choose it from the **Use setup** pop-up menu.

4. Specify the format and encoding in the respective pop-up menus.

   LANrev usually detects these parameters automatically, but you can override it.

5. If the import file contains field names in the first row, check **Don’t import first row**.

6. Click the **Custom Fields** tab and drag each custom field into which you want to import data to the column in the import file (displayed in the **Import data preview** section of the dialog) that you want to import into the field.

   If you have dragged a field onto the wrong column, you can remove it by clicking the ⊗ button in the column title or right-clicking the column (not the title) and choosing **Remove Field**.

7. Click the **Key Fields** tab and drag the information item that LANrev is to use to assign import records to database records onto the column that LANrev is to use for this purpose.

During the import process, LANrev will, for each import record, take the value from the column that you specified (by dragging the field on top of it) and find the database records that contain the same value in the key field you specified.

The values from the other fields in the import record are then imported into the specified fields (from step 6) of the database record, overwriting any previous content.

It is possible for multiple database records to match the value from the import record, in which case the import values are imported into the fields of all matching database records. (This can be a powerful tool to quickly update many client computer records.)

The specified column in the import file, on the other hand, must be a true key field. That is, no two import records may contain the same value in this column. If they do, no data is imported.

If you have dragged the field onto the wrong column, you can remove it by clicking the ⊗ button in the column title or right-clicking the column (not the title) and choosing **Remove Field**.

8. If you want to reuse the settings you made, save them as a preset using the **Save As** command from the **Use setup** pop-up menu.

9. Click **Import** to perform the import.

LANrev imports the data from the import file into the specified manual custom information fields according to your settings. Any previous content of these fields is overwritten.

Exporting and importing custom information field definitions

You can export the definitions of custom information fields and import them.

Note that you can also export or import all custom field definitions together with the server settings. This is mostly useful when migrating a server from one computer to another. See “Exporting and importing server settings” on page 91 for details.

Exporting custom information field definitions

To export custom information field definitions:

1. In the **Server Center** window, select the custom information fields the definitions of which you want to export.

2. Right-click in the sidebar and choose **Custom Information Fields** > **Export Selected Fields** from the context menu.

   The operating system’s Save dialog is displayed.

3. Choose a name and location for field definition file and click **Save**.

LANrev exports the field definitions to the specified file.

You can also drag the fields from the **Server Center** window to the desktop.

Importing custom information field definitions

To import custom information field definitions:

1. In the **Server Center** window, right-click in the sidebar and choose **Custom Information Fields** > **Import Fields** from the context menu.

   The operating system's Open dialog is displayed.

2. Choose the desired field definition file and click **Open**.

   You can import files with the ".lanrevcfdef" file name extension that have previously been exported from LANrev.

LANrev imports the field definitions from the specified file. If there are any conflicts between the imported fields and existing fields, LANrev informs you of the problem and offers several options to resolve it.

You can also drag the fields from the desktop into the **Server Center** window.

Manually edited information

LANrev provides ten so-called client information fields on each managed computer. These are text fields in which you can manually store arbitrary information, enabling you to note information such as inventory numbers, assigned owners, or maintenance dates.

Information can be edited remotely (from LANrev Admin) and optionally locally (by the user of the managed computer) as well. You can configure whether local access is possible; you can also set the names of the ten fields.

These procedures are described below in:

- **Using client information fields** (page 118)
- **Naming client information fields** (page 121)
- **Configuring local access to client information fields** (page 121)

Using client information fields

Information can be stored in client information fields in two ways:

- By the administrator, using LANrev Admin.
- By the local user, using the LANrev control panel. This access can be prevented, as described below in "Configuring local access to client information fields" on page 121.

Displaying the information is likewise possible for both the administrator and the local user. (It is not possible to prevent the local user from viewing client information fields' contents.)

Editing client information fields

To edit client information fields remotely:

1. In any browser window, select the computers on which you want to enter information in the client information fields.

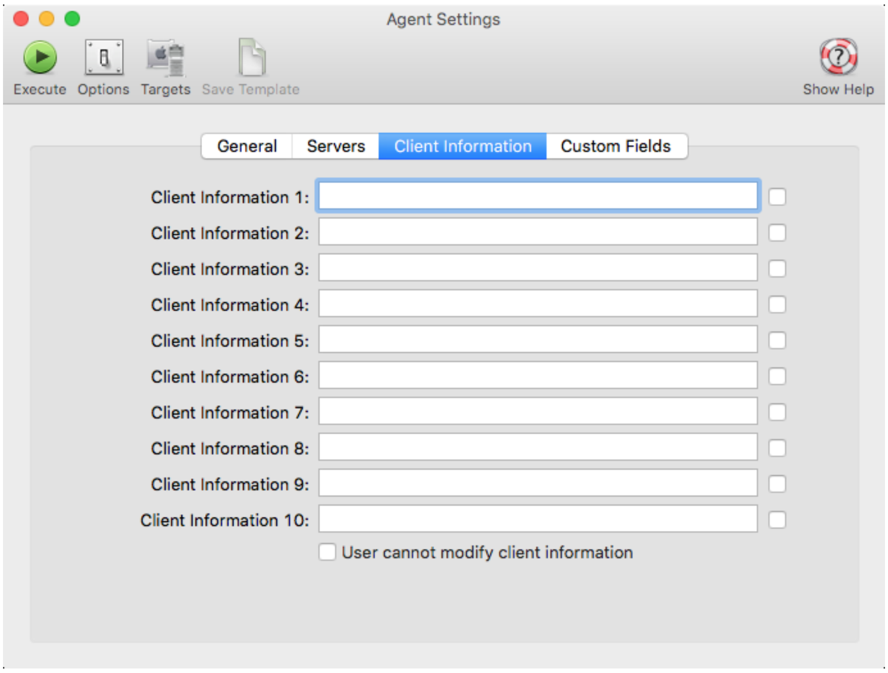
   You can select one or more computers.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Agent Settings**.

   The **Agent Settings** dialog opens.

3. Click the **Client Information** tab:



Client Information 1: □
Client Information 2: □
Client Information 3: □
Client Information 4: □
Client Information 5: □
Client Information 6: □
Client Information 7: □
Client Information 8: □
Client Information 9: □
Client Information 10: □

□ User cannot modify client information

4. Make the desired changes to the fields' contents.

5. Click **Execute**.

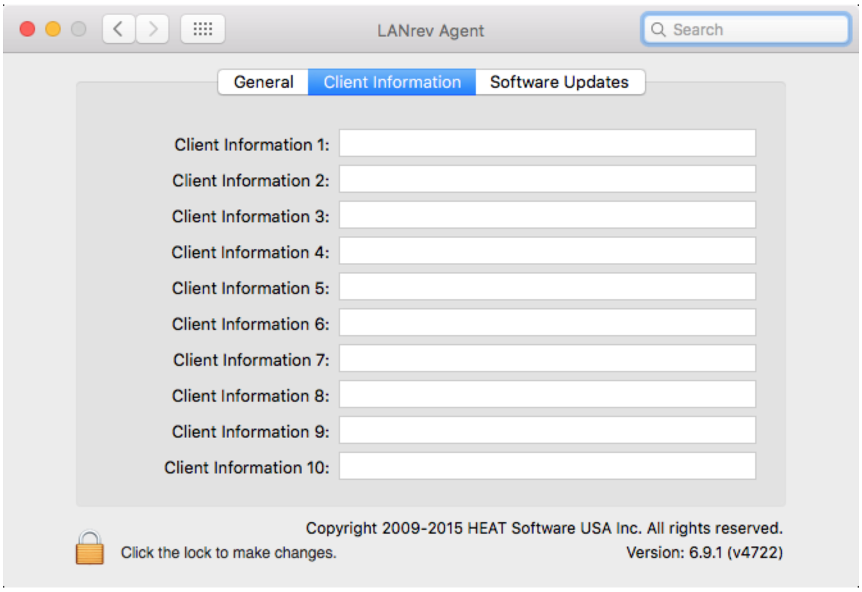
The fields' contents are set on all selected computers.

Editing client information fields locally on the administered computer requires an admin password for the computer as well as the fields to be unlocked for local modification (as described in "Configuring local access to client information fields" on page 121).

To edit client information fields locally:

1. On the administered computer, open **System Preferences** and click the **LANrev Agent** preference pane.

2. In the panel, click the **Client Information** tab.



Client Information 1:
Client Information 2:
Client Information 3:
Client Information 4:
Client Information 5:
Client Information 6:
Client Information 7:
Client Information 8:
Client Information 9:
Client Information 10:

Copyright 2009-2015 HEAT Software USA Inc. All rights reserved.

Click the lock to make changes.

Version: 6.9.1 (v4722)

3. Click the lock icon at the bottom left to unlock the preference pane and enter an administrator account name and password for the computer (not for LANrev) when so prompted.

4. Make the desired changes to the fields' contents.

5. Close the preference pane.

Displaying the contents of client information fields

The contents of client information fields can be displayed in various ways:

- To display the fields' contents for multiple computers in LANrev Admin, put the information items for the desired fields into any browser window.
  These information items are always named the same as the fields themselves and are found in the **Agent Information** > **Agent Settings** category of information items.
- To display the fields' contents for a single computers in LANrev Admin, select that computer in any browser window, open the **Agent Settings** dialog as described above in **Editing client information fields**.
- To display the fields' contents for a single computers on that computer, open the **LANrev Agent** preference pane on that computer, as described above in **Editing client information fields**.

Naming client information fields

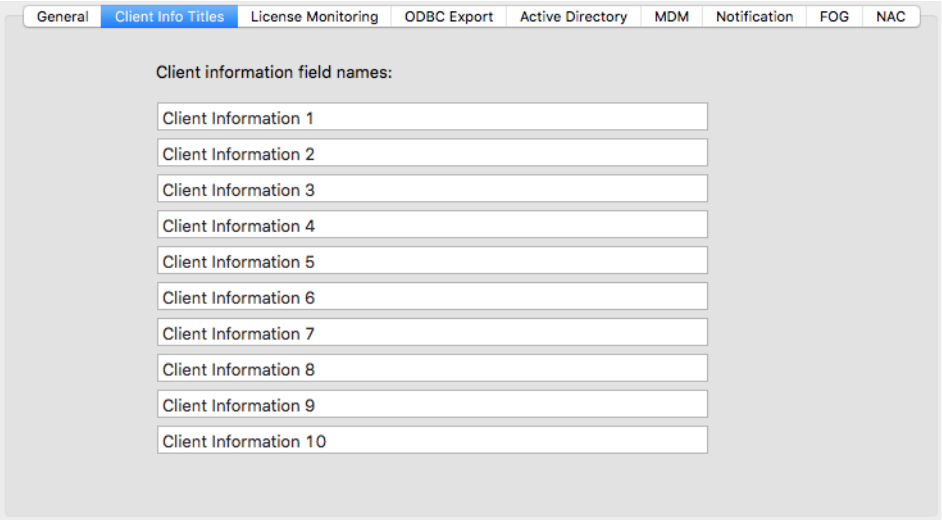
By default, client information fields have generic names. There is no need to rename them to use them; however, you may want to do so to indicate the kind of information that is stored in a field.

To set the name of a client information field:

1. In the **Server Center** window, click the **Server** > **Server Settings** category.

   The **Server Settings** dialog is displayed.

2. Click the **Client Info Titles** tab:



Client information field names:

Client Information 1
Client Information 2
Client Information 3
Client Information 4
Client Information 5
Client Information 6
Client Information 7
Client Information 8
Client Information 9
Client Information 10

3. Enter the desired names for the ten fields.

4. Click **OK**.

The new names are sent to the server; all agents connected to this server now use these field names.

NOTE If multiple inventory servers are specified for an agent, it uses the client info titles of the first one in the list in the **Servers** pane of the **Agent Settings** dialog. (For more details, see “Servers” on page 408.)

The information items that display the fields’ contents are also renamed, as noted in “Client Information 1 … 10” on page 835.

Configuring local access to client information fields

By default, local users of administered computers can edit the contents of client information fields through the **LANrev Agent** preference pane. If desired, you can prevent them from doing so.

To enable or disable local editing of client information fields:

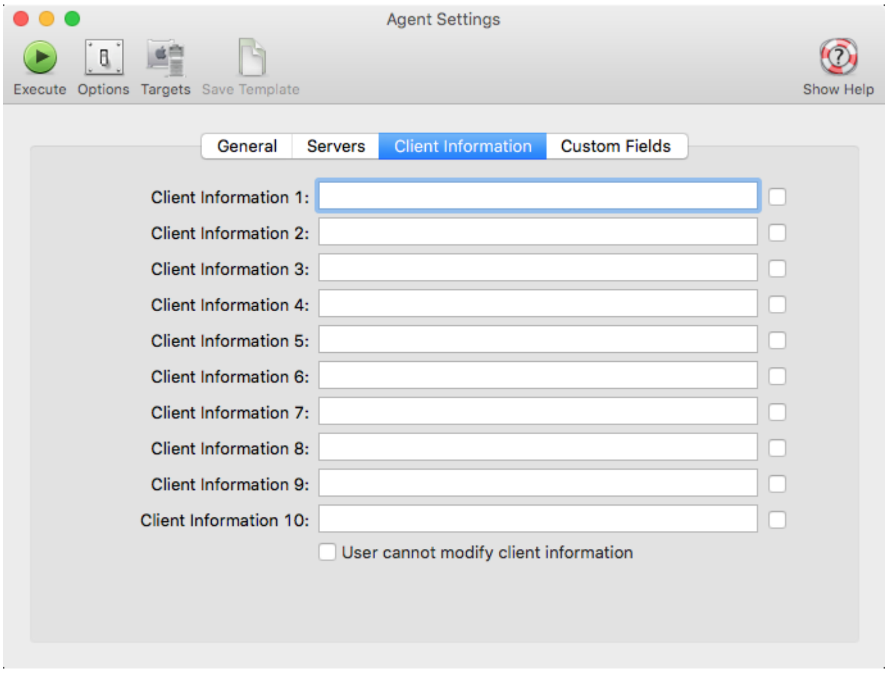
1. In any browser window, select the computers that you want to configure.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Agent Settings**.

   The **Agent Settings** dialog opens.

3. Click the **Client Information** tab:



Client Information 1: □
Client Information 2: □
Client Information 3: □
Client Information 4: □
Client Information 5: □
Client Information 6: □
Client Information 7: □
Client Information 8: □
Client Information 9: □
Client Information 10: □
□ User cannot modify client information

4. To prevent local users from editing client information fields, check the **User cannot modify client information** option.

   To allow local users to edit the fields, uncheck the option.

5. Click **Execute**.

The fields' are locked or unlocked as specified on all selected computers.

Automatically importing information

Certain types of information that is normally entered manually in the Admin can also be imported automatically by placing it in a specially prepared folder on the server.

This applies to:

- The enrollment user and enrollment domain information
- Device ownership information
- Content for manual custom information fields

The information is imported when a text file is placed in either of two folders (one for computers, the other for mobile devices) on the computer running LANrev Server.

Setting up automatic importing

To configure LANrev for automatic importing of data, create an import schema file as described in “Setting up an import file schema” on page 124 and put it into the AutomaticTextDataImport folder, which is located at:

- macOS: /Library/Application Support/LANrev Server/
- Windows Server 2003: C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server\
- Windows (other): C:\ProgramData\Pole Position Software\LANrev Server\

Performing an automated import

To perform an automated import:

1. Create a text file that conforms to the import file schema that you have defined.

   The file must contain all specified columns, in the order in which they are specified in the appropriate array (DesktopColumns or MDMColumns).

   If the import schema specifies processing the first row of the import file (using the DesktopSkipFirstLine and MDMSkipFirstLine elements), the import file must not contain column titles.

   Conversely, if the schema specified skipping the first row, that row must contain column titles (or some other non-payload content, but not a record that you wish to process).

2. Save the file in the desired format with the appropriate filename extension:

   - Tab-delimited text file with the extension “.txt”.
   - Comma-separated text file with the extension “.csv”.
   - Semicolon-separated text file with the extension “.semicolon.csv”.

3. Place the file in the appropriate subfolder of the AutomaticText-DataImport folder, DesktopImport or MDMImport.

LANrev Server automatically reads each of these files. Each found import record is assigned to the device record in the internal database that matches the record's key field, and the other fields of that device record are updated with the data from the import file.

If the import file contains both custom field data and enrollment user data, the custom field data is updated first.

If the import schema in the ImportLayout.plist file is invalid or if it specifies an information item that is not present in the LANrev database, the problem is noted in the log and the data file is moved into a subfolder of the AutomaticTextDataImport folder – DesktopImportFailedFiles or MDMImportFailedFiles, depending on the type of file.

If there no matching computer or mobile device in the LANrev database for an import record, the issue is noted in the log.

Setting up an import file schema

In order to automatically import information from text files on the server, as described in "Automatically importing information" on page 122, you must specify the column scheme of the import files.

This is done by creating a property list file (an XML file specifying preferences, indicated by the .plist extension) that is placed in the import folders. Although the file can be created with any text editor, we recommend that you use either Xcode, which has a built-in editor for property lists, or an XML editor.

Basic structure

The property list file has a dictionary as its root element that contains one or two arrays:

- DesktopColumns specifies the structure of import files for managed computers.
- MDMColumns specifies the structure of import files for managed mobile devices.

You can specify either one of the arrays or both of them, depending on what kinds of data you want to import.

In addition, you can specify whether the first line in either kind of import file is processed or not. By default, the lines are processed (that is, it is assumed that the files do not contain column titles but begin with the first payload record.) If you want the first line to be skipped, insert either or both of these Boolean elements in the root element and set their values to true:

- DesktopSkipFirstLine to skip processing the first row of import files for managed computers.
- MDMSkipFirstLine to skip processing the first row of import files for managed mobile devices.

The file must be saved UTF-8 encoded with the extension ".plist".

Structure of an array

Each array contains several dictionaries, one for each column in the import file.

These dictionaries can be named as desired, and they must occur in the order in which the columns occur in the file.

Exactly one of the columns in each array must be marked as the key column (see below), which is used to determine to which managed device each row in the import file belongs.

Structure of a column specification

Each dictionary that represents a column contains a string entry. The name of that entry is always "InfoItemName", and the content of the entry is the name of the information item to which the column corresponds.

The name of the information item must be specified exactly as it appears in the **Information Items** window; we recommend that you right-click the desired information item and copy and paste the name.

You can only specify information items with manually editable content:

- Device Ownership
- Enrollment Domain
- Enrollment User
- Any manual custom fields that you have defined (see "Custom information" on page 106 for details)

One of the column specifications in each array must be marked as the key column, by which the import record is matched with an existing device record in the LANrev database. This is done by adding a second entry, which must be a Boolean named IsKeyField which is set to true. Each array must have exactly one key field, and the value in the specified information item must be unique for each managed device. The choice of information items for the key field is not restricted to the above list; for example, Agent Serial Number can be used.

Example

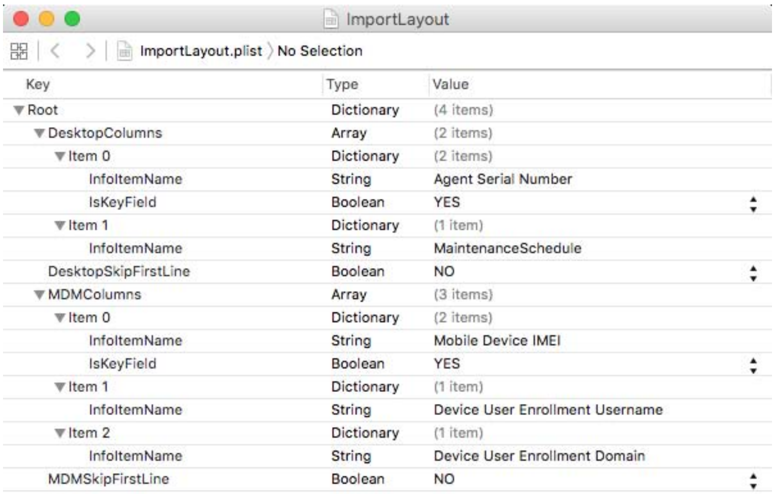
The following example specifies the import schema for both computers and mobile devices.

For computers, the import files contain the agent serial number and the (manual) custom information field MaintenanceSchedule.

For mobile devices, the import files contain the IMEI as the key field, the enrollment user, and the enrollment domain.

For both computer import files and mobile device import files, the first lines of the files are processed (not skipped).

As an Xcode document, this schema looks like this:



Key	Type	Value
▼Root	Dictionary	(4 items)
▼DesktopColumns	Array	(2 items)
▼Item 0	Dictionary	(2 items)
InfoItemName	String	Agent Serial Number
IsKeyField	Boolean	YES
▼Item 1	Dictionary	(1 item)
InfoItemName	String	MaintenanceSchedule
DesktopSkipFirstLine	Boolean	NO
▼MDMColumns	Array	(3 items)
▼Item 0	Dictionary	(2 items)
InfoItemName	String	Mobile Device IMEI
IsKeyField	Boolean	YES
▼Item 1	Dictionary	(1 item)
InfoItemName	String	Device User Enrollment Username
▼Item 2	Dictionary	(1 item)
InfoItemName	String	Device User Enrollment Domain
MDMSkipFirstLine	Boolean	NO

The equivalent XML file is:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>DesktopColumns</key>
  <array>
    <dict>
      <key>InfoItemName</key>
      <string>Agent Serial Number</string>
      <key>IsKeyField</key>
      <true/>
    </dict>
    <dict>
      <key>InfoItemName</key>
      <string>MaintenanceSchedule</string>
    </dict>
  </array>
  <key>DesktopSkipFirstLine</key>
  <false/>
  <key>MDMColumns</key>
  <array>
    <dict>
      <key>InfoItemName</key>
      <string>Mobile Device IMEI</string>
      <key>IsKeyField</key>
      <true/>
    </dict>
    <dict>
      <key>InfoItemName</key>
      <string>Device User Enrollment Username</string>
    </dict>
```

```
            <dict>
              <key>InfoItemName</key>
              <string>Device User Enrollment Domain</string>
            </dict>
          </array>
          <key>MDMSkipFirstLine</key>
          <false/>
        </dict>
        </plist>
```

Storing and exporting information

The information that LANrev gathers from the managed clients is automatically stored on LANrev Server without requiring any manual interaction or configuration. (There are, indeed, no configuration options for data storage.)

The gathered software can be made available to other tools by exporting it. There are three principal ways of doing so:

- Manual export to XML, HTML, or text files. This is described in "XML, HTML, and text export" on page 127.
- Periodic automatic export to an ODBC database, as described in "ODBC export" on page 128.
- Periodic automatic export to Microsoft System Center Configuration Manager (SCCM). This requires the LANrev SCCM Integration add-on module and is described in that module's documentation.

LANrev also offers backup and maintenance functions:

- Automated database backup and maintenance. This is described in "Configuring database backup and maintenance" on page 130.
- Deleting unneeded information from the server. This is described in "Deleting information from the server" on page 131.

XML, HTML, and text export

You can export information that is being displayed in an LANrev window to a range of common exchange formats:

- HTML
- Comma-separated text (CSV) in two variants
- Tab-delimited text
- XML (using a custom structure)

The process is the same in each case:

1. Make sure that the information you want to export is displayed in a window.

   This includes both the desired records (computer, files, etc.) and the desired columns.

2. From the **File** menu, choose **Export**.

   The operating system’s Save dialog opens.

3. From the dialog’s **File Format** pop-up menu, choose the desired format. Specify a name and location for the export file and click **Save**.

The data from the window is exported in the specified format to the specified location.

ODBC export

LANrev Server can automatically export data from its database at specified intervals over an ODBC connection, allowing the target database to be used for a range of applications such as logging, backup, or reporting.

Preparing for ODBC export

To be able to use LANrev’s ODBC export feature, you need:

- a database that can be accessed via ODBC
- a compatible ODBC driver
- an account in the database that can create tables and insert data

See the documentation of the database or the ODBC driver for details on installing and configuring this software.

NOTE While LANrev is expected to be compatible with a wide range of ODBC software, it has currently only been tested with MySQL and the MyODBC driver. We cannot guarantee compatibility with other databases and drivers.

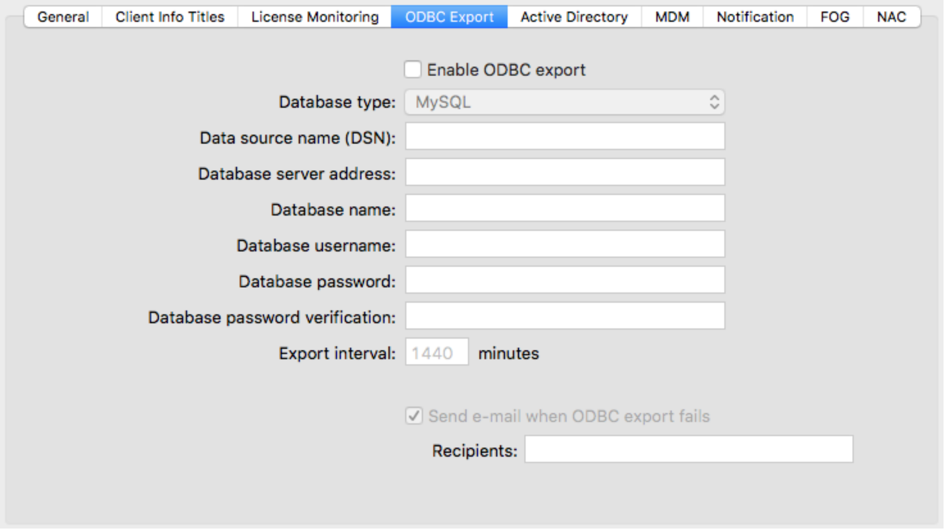
Setting up ODBC export

To set up LANrev for ODBC support, you configure the required access information and desired update interval on the LANrev server:

1. In the **Server Center** window, click the **Server** > **Server Settings** category.

   The **Server Settings** dialog is displayed.

2. Click the dialog’s **ODBC Export** tab.



☐ Enable ODBC export

Database type: MySQL

Data source name (DSN):

Database server address:

Database name:

Database username:

Database password:

Database password verification:

Export interval: 1440 minutes

☑ Send e-mail when ODBC export fails

Recipients:

3. Check **Enable ODBC support** and fill in the fields:

   - **Database type**: The kind of database management system connected via ODBC.
   - **Data source name (DSN)**: The name of the data source as defined in ODBC.
   - **Database server address**: The IP address or DNS name of the database server.
   - **Database name**: The name of the database on the server in which the information from LANrev is to be stored.
   - **Database username**: The database account that LANrev is to use to store the data.
   - **Database password**: The password for the database user account.
   - **Database password verification**: Repeat the password here to guard against typos.
   - **Export interval**: The desired interval in which LANrev export data to the database.
   - **Send e-mail when ODBC export fails**: Check this option and enter an e-mail address in the **Recepient** field to have LANrev send out automatic notifications when the ODBC export could not be completed. You can enter multiple addresses separated by commas. (Sending e-mail requires the SMTP information in the **Notification** tab to be filled in.)

   Note: Apart from the data source name, you can leave all fields empty if the corresponding information is specified in the data source.

4. Click **OK**.

The settings are stored on the server; the export is initiated immediately and in the specified interval from then on.

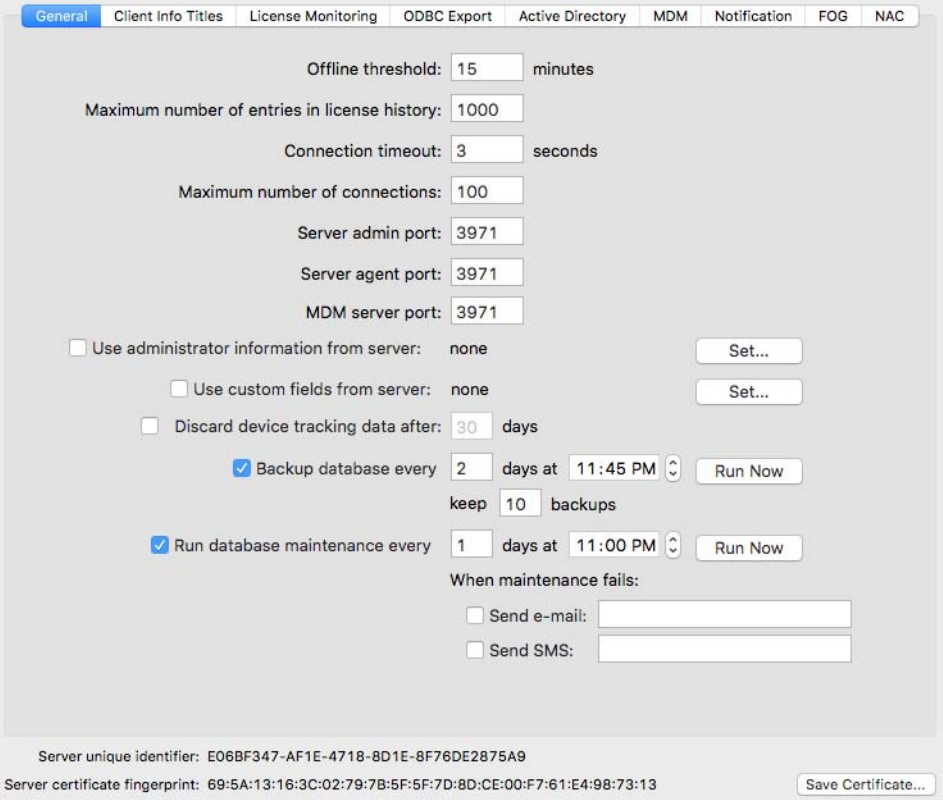
Configuring database backup and maintenance

LANrev lets you configure the database’s backup and maintenance options.

To configure the options:

1. In the **Server Center** window, click the **Server** > **Server Settings** category.

   The **Server Settings** dialog is displayed.



Offline threshold: 15 minutes
Maximum number of entries in license history: 1000
Connection timeout: 3 seconds
Maximum number of connections: 100
Server admin port: 3971
Server agent port: 3971
MDM server port: 3971
□ Use administrator information from server: none
□ Use custom fields from server: none
□ Discard device tracking data after: 30 days
☑ Backup database every 2 days at 11:45 PM
keep 10 backups
☑ Run database maintenance every 1 days at 11:00 PM
When maintenance fails:
□ Send e-mail:
□ Send SMS:

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9
Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13

2. If you want LANrev to automatically perform database maintenance, check the **Run database maintenance** option and specify the desired interval and time of day.

   Database maintenance involves eliminating empty blocks from the database file on disk and performing a full consistency check on the database.

3. If you want LANrev to perform automatic database backups, check the **Backup database** option and specify the desired interval, time of day, and number of backup generations to keep.

   The LANrev Server database is located in the **/Library/Application Support/LANrev Server** folder on macOS-based servers and in **C:\Documents and Settings\All Users\Application Data\Pole Position Software\LANrev Server** on Windows.

Backups are located in the same folders, in subfolders with the suffix **.dbbackup**, **.dbbackup1**, **.dbbackup2**, etc. for the successive backup generations.

4. If you want to immediately perform the database maintenance or create a database backup, click the appropriate **Run Now** button.

5. Choose **Save Server Settings** from the **Server** menu.

LANrev performs the specified operations on the server until the settings are edited again.

Deleting information from the server

Occasionally, you may have collected a significant amount of information that is no longer needed. To prevent this information from taking up space and processing power on the server, you can delete it manually.

Deleting entire records

To delete unneeded records from LANrev Server:

1. In any browser window, select the records that you want to remove from the server.

2. Right-click the records and choose **Remove from Server** from the context menu.

   A confirmation alert is displayed.

3. Click **OK**.

LANrev removes all selected records (along with any associated data, such as inventory information for computer records) from the server. This operation cannot be undone; however, you may recreate the records, for example, by performing a file search to recreate file records.

Deleting associated data for a record

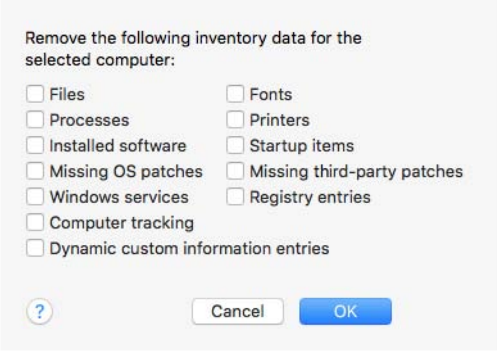
To delete unneeded information related to computer records:

1. In any browser window, select computers for which you want to remove related data.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. Right-click the records and choose **Remove Inventory Data** from the context menu.

The **Remove Inventory Data** dialog is displayed:



Remove the following inventory data for the selected computer:

□ Files
□ Processes
□ Installed software
□ Missing OS patches
□ Windows services
□ Computer tracking
□ Dynamic custom information entries

□ Fonts
□ Printers
□ Startup items
□ Missing third-party patches
□ Registry entries

3. Check all the types of information that you would like to remove and click OK.

LANrev removes the specified types of associated data for all selected records from the server. This operation cannot be undone; however, you can gather the deleted data anew using the **Gather Inventory Information** command.

Displaying information

When information on administered computers has been found by the LANrev agents and stored on LANrev Server, it can be displayed in the administrator application. This is done in browser windows.

Browser windows are, basically, tables in which each row represents a computer or other monitored object (file, font, process, etc.), and each column an information item, that is, a database table column.

They also let you search for, filter, and sort objects, and provide a way to display an overview of information on a single computer.

NOTE Details on the elements of browser windows are found in “Browser windows” on page 517.

Details on displaying information are available in:

- “Opening and configuring browser windows” on page 132
- “Displaying an overview of a single computer” on page 135
- “Controlling information display from a URL” on page 136
- “Searching, filtering, and sorting” on page 138

Opening and configuring browser windows

You can open browser windows from the **File** menu and configure both the categories in the sidebar as well as the columns displayed in the main area of the window. To keep configuration changes, you must save them.

Opening a new browser window

To create a new browser window, choose **New** from the **File** menu.

Configuring the sidebar

You can add categories, groups, and smart groups to the sidebar as well as rename and delete them:

- To add a category, choose **New Category** from the sidebar's context menu.
  To rename a category, select it and choose **Rename Category** from the sidebar's context menu.
  To delete a category, select it and choose **Remove Category** from the sidebar's context menu.
- Adding groups is described in "Creating groups" on page 139.
  Renaming groups is described in "Editing groups" on page 141.
  Removing groups is described in "Deleting groups" on page 142.

Configuring a browser window

You configure browser windows by adding, rearranging and removing information items:

- To add an information item, drag it from the **Information Items** window into the table area – this adds the column at the right-hand side of the table – or to the Columns drawer, where you can insert it at the desired location.
  You can also drag columns between Columns drawers of different browser windows or copy and paste them.
- To rearrange columns, drag their titles in the table area or in the Columns drawer to the desired location.
  To resize columns, drag the right-hand borders in the table title area.
- To remove a column, select its title in the Columns drawer and click the **Remove** button.

NOTE If the Columns drawer is not displayed, you can open it by choosing **Configure Columns** from the **View** menu.

No particular action is required from you to display data in the columns you have added; this is done automatically as long as the data is available on LANrev Server. Note, however, that some types of data are not collected automatically and must be requested manually, as described in "Gathering information" on page 95.

You can rearrange the groups in the sidebars of most browser windows by dragging them. You can also drag custom smart groups – but not built-in ones such as **Macs only** – between browser windows and the **Server Center** window.

Saving configured browser windows

When you have configured a browser window, you can save it for future reuse using the **Save As** command from the **File** menu. Doing so saves the structure of the window; it does not save the actual data, which are always dynamically loaded from LANrev Server.

Working with tabs

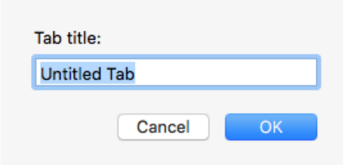
Each LANrev browser window can contain multiple tabs. LANrev tabs are analogous to Web browser tabs: The content of each of them is independent of the others'; the sizes of all tabs in one window are the same; all tabs in one window always move together on the screen.

Adding a tab to a window

To add a new tab to a browser window:

1. From the **File** menu, choose **New Tab**. If there are already tabs in the window, you can also click the New Tab icon ⊕.

   The **New Tab** dialog is displayed:



Tab title: Untitled Tab

2. Enter the desired name and click **OK**.

   The new tab appears in the window.

NOTE Tabs can only be added to browser windows, not to other types of windows.

Renaming a tab

To rename a tab:

1. From the **File** menu, choose **Rename Tab**.

   The **Rename Tab** dialog is displayed, which looks similar to the **New Tab** dialog shown above.

2. Edit the name as desired and click **OK**.

   The name of the tab is changed.

Rearranging tabs

You can rearrange tabs (changing their order in their window) by dragging them by their titles.

Closing tabs

To close a tab, either click its close icon ⊗ or make it active and choose **Close Tab** from the **File** menu.

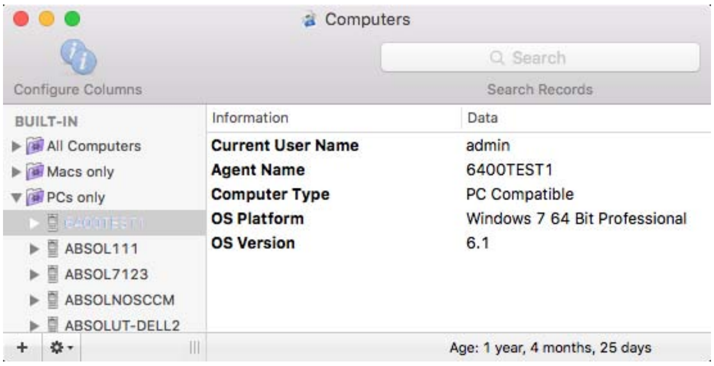
Displaying an overview of a single computer

While browser windows normally display a range of information items for a large number of computers, it can also display a complete overview of a single computer.

To display an overview:

1. In the **Groups & Computer**s sidebar of any browser window, open a group that contains the desired computer and click on the computer.

   A selection of important information items is displayed:



Information	Data
Current User Name	admin
Agent Name	6400TEST1
Computer Type	PC Compatible
OS Platform	Windows 7 64 Bit Professional
OS Version	6.1

Age: 1 year, 4 months, 25 days

2. To see more detailed information, open the computer in the sidebar to display a range of information item categories. Click the desired category to display the respective information.

3. To revert to the normal tabular display, click on any group in the sidebar.

NOTE If the “**Double-clicking a computer**” option in the Preferences dialog is set to “**Display detail view**”, you can also double-click a computer to view the details.

Configuring the individual computer display

You can configure all displays for individual computer information:

- Add information items to a particular display pane by dragging them there from the **Information Items** window.
- Rearrange information items by dragging them to the desired location in the list.
- Remove information items by selecting them and pressing the Backspace key.

Any configuration changes you make in these display panes affect all other computers with the same operating system platform (Windows or macOS).

Saving the browser window (as described in “Saving configured browser windows” on page 134) also saves these configuration changes.

Controlling information display from a URL

In addition to the standard selection of information to display via the graphical user interface, LANrev also lets you specify computers to display via a URL.

You can construct a URL to display information on a particular computer in LANrev using this syntax: lanrevadmin://showagent?<field>=<value>.

- <field> is the information item by which you want to find the desired computer. It can have any of these values (the value being the first word, with the full name of the information item added in parentheses):
  - agentip (**Agent Active IP**)
  - agentserial (**Agent Serial Number**)
  - computername (**Computer Name**)
  - agentname (**Agent Name**)
  - computerserial (**Computer Serial Number**)
  - primarymacaddress (**Primary MAC Address**)
  - adcomputername (**AD Computer Name**)
  - clientinfo1 (**Client Information 1 … 10**)
  - clientinfo2 (**Client Information 1 … 10**)
  - clientinfo3 (**Client Information 1 … 10**)
  - clientinfo4 (**Client Information 1 … 10**)
  - clientinfo5 (**Client Information 1 … 10**)
  - clientinfo6 (**Client Information 1 … 10**)
  - clientinfo7 (**Client Information 1 … 10**)
  - clientinfo8 (**Client Information 1 … 10**)
  - clientinfo9 (**Client Information 1 … 10**)
  - clientinfo10 (**Client Information 1 … 10**)
  - computerservicetag (**Computer Service Tag**)
  - currentuseraccount (**Current User Account**)
  - currentusername (**Current User Name**)
  - customagentname (**Custom Agent Name**)
  - mainboardassettag (**Mainboard Asset Tag**)
  - mainboardserial (**Mainboard Serial Number**)
  - osproductid (**OS Product ID**)
  - osserial (**OS Serial Number**)
  - securityid (**Security Identifier**)
  - systemenclosuretag (**System Enclosure Asset Tag**)
  - systemenclosureserial (**System Enclosure Serial Number**)
- <value> is the value to search for.

Calling the URL causes LANrev to search the specified field for the specified value and display a single-computer overview of the found computer.

For example, the URL lanrevadmin://showagent?computername=My%20Computer displays the computer with the name “My Computer” in the single-computer overview in LANrev Admin.

LANrev Admin must be installed on the computer on which the URL is called. If it is not running, it is started automatically.

NOTE With some of the available fields, there may be more than one matching computer. If this happens, LANrev displays the first computer matching the specified criteria.

Setting up Google Chrome to support lanrevadmin:// URLs

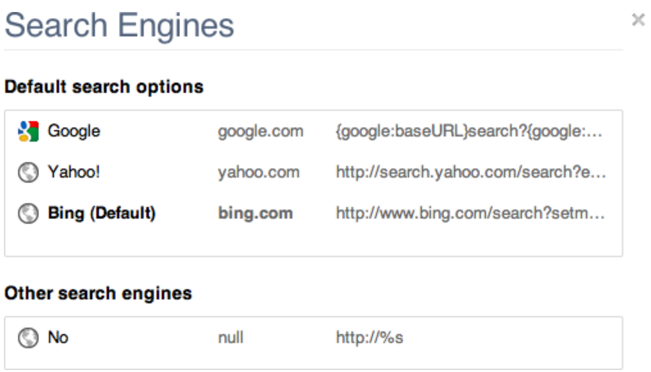
In its default setup, Google Chrome does not understand the lanrevadmin:// syntax. To make it compatible with this syntax:

1. In Google Chrome, right-click the address bar and choose **Edit Search Engines**.

   The **Search Engines** page is displayed.

2. In the **Other search engines** section, specify a new search engine with these values:

   - **Add a new search engine**: No
   - **Keyword**: null
   - **URL with %s in place of query**: http://%s



Search Engines

Default search options

Google	google.com	{google:baseURL}search?{google:...
Yahoo!	yahoo.com	http://search.yahoo.com/search?e...
Bing (Default)	**bing.com**	http://www.bing.com/search?setm...

Other search engines

No	null	http://%s

3. Press return and close the page.

4. Quit Chrome.

5. Open the “Local State” file with a text editor.

   This file is found in different locations, depending on the operating system:

   - macOS: /Library/Application Support/Google/Chrome/

- Windows Server 2003: C:\Documents and Settings\<username>\Local Settings\Application Data\Google\Chrome\User Data\
- Windows Vista and above, Windows Server 2008 and above: C:\Users\<username>\AppData\Local\Google\Chrome\User Data\

For information on where to find the “Local State” file on other platforms, see the Chrome help.

6. In the “protocol_handler” section, “excluded_schemes” subsection, add this line (including quotes and comma):

```
"lanrevadmin": false,
```

7. Save and close the file.

You can now use lanrevadmin:// URLs in Chrome like in other browsers.

Searching, filtering, and sorting

Various methods are available to focus on the currently interesting part of the information displayed in browser windows:

- You can search for specific text in a particular column or the entire browser window.
- You can filter computers by creating groups, either according to specified criteria or manually, and restricting the display to just one group.
- You can sort the browser window on any number of columns.

All these methods can be combined to present the information in the browser window.

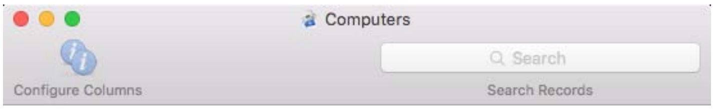
They are described below in:

- “Searching in browser windows” on page 138
- “Creating groups” on page 139
- “Sorting browser windows” on page 142

Searching in browser windows

To search for specific text in browser windows:

1. Enter the text in the **Search Records** field in the toolbar:



2. Press Return.

LANrev searches the currently displayed records, hiding all that do not contain the text in the information items in the browser window.

By default, all columns are searched. If you want to search just one particular column, choose that column from the pop-up menu before pressing Return.

Creating groups

Groups in browser windows are collections of administered computers. They allow you to easily work with a subset of all managed computers.

There are two kinds of groups:

- (Standard) groups are much like file folders: To include a computer in a group, you add it manually; to take it out again, you manually remove it.
- Smart groups are not so much collections of specific computers but descriptions of what kind of computers you want to include in a group.
  They are defined by selection criteria and at any time dynamically display those computers that meet the criteria in that instant. Inclusion and exclusion of computers is automatic. For example, you could define a smart group to include all computers with less than 512 MB of memory. When a computer’s RAM is updated to more than that amount, LANrev automatically removes it from that group.
  In standard browser windows, there are three predefined smart groups – for all computers, macOS computers, and Windows computers. In specialized browser windows, for example, the **Server Center** window, additional or different smart groups may be predefined.

You can use both kinds of groups as command targets by dragging them into the target area of the respective command window. When a command is saved for later execution, the target computers are the members of the groups at execution time, not the computers that were members of the groups when the command was saved.

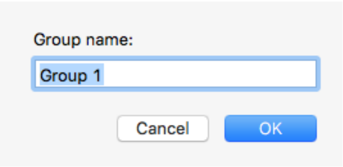
When smart groups are command targets for repeating commands, LANrev re-evaluates for each repetition which computers belong to the group. In other words, a computer that was a command target because it met the group criteria may not be a target in the next execution because it no longer meets the criteria, and vice versa.

Creating a (standard) group

To create a manually maintained group:

1. From the action menu in the browser window, choose **New Group**.

   The **New Group** dialog opens:



Group name: Group 1

2. Enter the name of the new group and click **OK**.

3. To add computers to the group, drag them from the table (not from other groups in the sidebar) into the group.

4. To remove computers from the group, display the group, right-click the computer, and choose **Remove from Group** from the context menu.

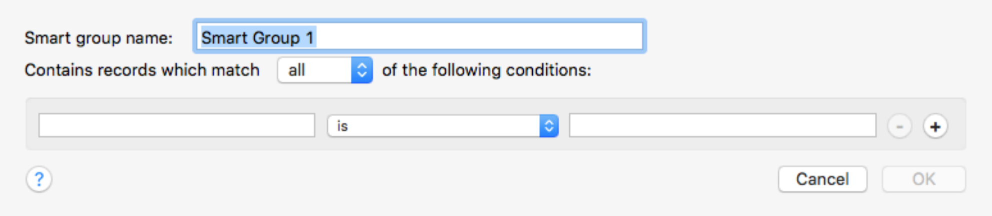
   Note: Computers cannot be individually removed from smart groups.

Creating a smart group

To create a smart group:

1. From the action menu in the browser window, choose **New Smart Group**.

   The **Smart Group** dialog opens:



Smart group name: Smart Group 1

Contains records which match all of the following conditions:

is

2. Enter the name for the new group and define the conditions that computers must meet to be included in the group.

   To define a condition, specify an information item in the left-hand text field – you can use any information item listed in the **Information Items** window – choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

   When the text insertion mark is in a field, you can drag a column from the Columns drawer into the field.

   With the **+** and **–** buttons, you can add and remove conditions.

3. If you have specified more than one condition, specify through the upper pop-up menu whether computers must meet one or all of the conditions.

4. Click **OK**.

Creating smart groups, alternate technique

You can also create smart groups by example. To do so:

1. In any browser window, select records showing the criteria that you want to use for the smart group.

   For example, to create a group with all computers with dual-core processors, add the relevant information item – **Cores per Processor** – to a browser window, if it is not already present. Then, select a computer with the desired value in this column, that is, 2.

2. Right-click the column in the browser window that you want to use for specifying the smart group and choose **New Smart Group from "<information item>"** from the context menu (where **<information item>** is replaced with the title of the column in which you clicked).

   For example, for the smart group for all dual-core processor based computers, click in the **Cores per Processor** column.

3. The **Smart Group** dialog opens with conditions based on your selections already predefined. Proceed as described in the procedure above.

   In particular, you can edit the predefined selection conditions, add new ones, or delete them.

Duplicating groups

You can duplicate groups that you have created in LANrev (but not predefined groups). To do so:

1. Select the group that you want to duplicate in the sidebar of any window in which it is displayed.

2. Choose **Edit** > **Copy**.

3. Choose **Edit** > **Paste**.

LANrev creates an identical duplicate of the group.

Editing groups

To rename a group, select it and choose **Rename Group** from the action menu.

To edit the definition of a smart group, select it and choose **Edit Smart Group** from the action menu.

Adding computers to a standard group and removing them is described above in "Creating a (standard) group" on page 139.

Deleting groups

To delete a group, select it and choose **Remove Group** from the action menu.

Saving group definitions

Groups defined in a browser window are automatically saved when the window is saved. Saving browser windows is described in “Saving configured browser windows” on page 134.

Transferring groups

Groups can be exported and imported by means of the **Export Groups** and **Groups** commands.

Export Groups stores all groups and smart groups (but not special categories such as **License Specifications** from the **Server Center** window) from the frontmost window in one file.

Groups inserts all groups from the selected file into the frontmost window. Existing groups remain unaffected.

You can directly transfer groups between windows by dragging and dropping them.

Exporting groups

To export selected groups and smart groups from the frontmost window:

1. From the **File** menu, choose **Export Groups**.

   A standard Save dialog is displayed.

2. Give the file a name, choose a storage location, and click **Save**.

The definitions of the selected groups and smart groups (but not special categories such as **License Specifications** from the **Server Center** window) from the frontmost window are saved in the file.

Using an alternative method:

- Select the groups you want to export and drag them to the desktop.

Sorting browser windows

Browser windows can be sorted on as many columns as desired.

Sorting by a column

To sort the window by a column, double-click the column’s title. The column is made an additional sorting column:

- If this is the first sorting column, the records are sorted by this column.
- If there already are sorting columns, the double-clicked column is added as the next-lower sorting column. This means that all records that sort the same according to the existing columns are sorted by the newly added column.
  For example, when sorting only by the first column results in:
  1 3 4
  1 2 4
  1 3 1
  2 1 3
  additionally sorting by the second column creates:
  1 2 4
  1 3 4
  1 3 1
  2 1 3

A sorting column is indicated by a small triangle in its title. The order of the sorting columns is indicated by the shading of the triangles:

▲ Primary sorting column

▲ Second column

▲ Third column

△ Subsequent columns (these are not visually differentiated any more)

Reversing the sort order

To reverse the sort order for a column, double-click the column’s title again. (The column must already be a sorting column.)

The triangular indicators show the current sort order: If the triangle points upwards, smaller values come first, if it points downwards, larger values come first.

Removing sorting

If you want to stop sorting the table by a particular column, double-click its title with the Command key held down.

Chapter 5 Controlling computers

You can use LANrev to control administered computers in several ways.

This is discussed in detail in:

Sending messages

You can send messages to administered computers, for example, to advise employees of upcoming administrative actions.

While there is no dedicated facility for letting users answer to your messages, you can add a **Cancel** button to message dialogs. Because the agents report which button a user has pressed to dismiss the dialog and this information is noted in the command history, you can use this function to ask simple yes/no questions.

Sending messages to iOS devices requires a different process, which is described in "Sending a message to mobile devices" on page 236.

In addition to sending messages manually, as described below, messages can also be sent automatically by adding an action to a computer group. See "Working with actions" on page 178 for details.

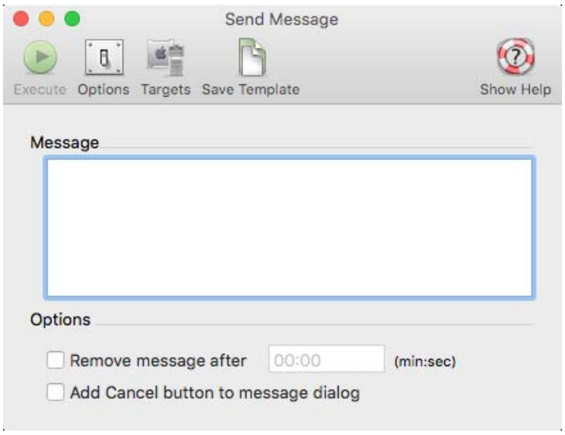
To send a message to administered computers:

1. In any browser window, select the computers to which you want to send the message.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Send Message**.

The **Send Message** dialog opens:



□ Remove message after 00:00 (min:sec)
□ Add Cancel button to message dialog

3. Enter the desired message.

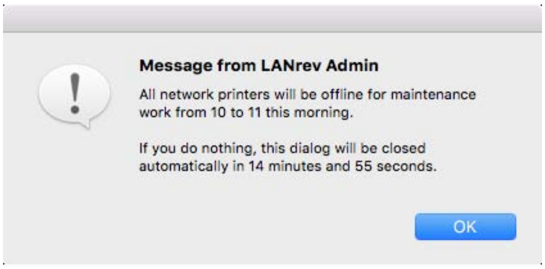
   Note: To insert a line break, press Option-Return.

4. Set the message options:

   - When you want to make sure that the dialog does not remain on screen indefinitely when there is no user present, specify an interval after which the message is closed automatically.
     The dialog is closed as if the user had clicked **OK**. (The timeout is, however, noted in the log.)
   - When you want the users to be able to express non-acceptance, add a **Cancel** button. (There is always an **OK** button.)

5. Click **Execute**.

The message is displayed on the target computers:



Message from LANrev Admin

All network printers will be offline for maintenance work from 10 to 11 this morning.

If you do nothing, this dialog will be closed automatically in 14 minutes and 55 seconds.

If a user dismisses the dialog by clicking on the **Cancel** button (if any), you can see this in the **Command Error Info** column in the **Commands** window.

Restarting, shutting down, and sleep

LANrev can control the operating state of administered computers, that is, it can restart them, shut them down, put them to sleep, or wake them up.

The process for these commands is very similar; only waking computers up differs slightly.

Using the **Power Management Settings** command, you can also schedule these events, either for a fixed time or for after a certain period of inactivity. This is described in "Scheduling power management events" on page 148.

Restarting, shutting down, and putting to sleep

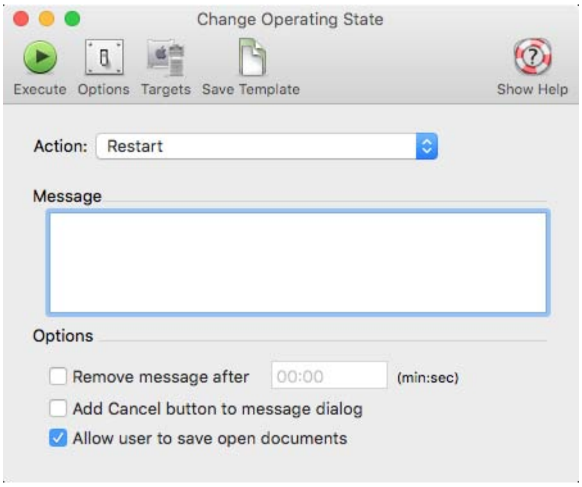
To restart administered computers, shut them down, or put them to sleep:

1. In any browser window, select the computers that you want to control.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Change Operating State**.

   The **Change Operating State** dialog opens:



Change Operating State

Action: Restart

Message

Options

□ Remove message after 00:00 (min:sec)

□ Add Cancel button to message dialog

☑ Allow user to save open documents

3. Choose the desired action from the pop-up menu.

   The **Force restart (FileVault authenticated)** option is a forced restart that applies only to computers meeting all of these criteria:

   - macOS 10.8.2 and above.
   - MacBook Pro mid 2009 or newer, MacBook or iMac late 2009 or newer, Mac mini mid 2010 or newer, MacBook Air late 2010 or newer, Mac Pro late 2013 or newer.

- The currently valid FileVault key has been stored in LANrev. (See “macOS profiles” on page 668 for more information.)

Other computers will be simply force-restarted.

Choosing this option lets you start the administered computer once without requiring the presence of the local user to enter the FileVault password.

Note: This option leaves the target computers running and unlocked. Depending on the circumstances, this may present a security risk.

Note: When you try to put to sleep a Windows computer, LANrev first tries to hibernate it. If that is not supported, it tries to put it into stand-by mode. If the computer does not support this mode either, the command fails with an error log entry.

4. If you want the user to be able to save any changes to open documents, check **Allow user to save open documents**.

   If this option is unchecked, restarts and shutdowns are ‘hard’, that is, any running processes are killed immediately.

5. If desired, enter a message that warns the users. The relevant options are described in “Sending messages” on page 144.

6. Click **Execute**.

Waking up computers

Administered computers can be woken up only if ‘Wake on LAN’ is enabled on them. How this function is enabled differs between systems. Depending on your system, you will find the required information in the documentation of the operating system, of the computer or motherboard, or of the LAN card.

NOTE Usually, you find the required setting in the **Energy Saver** control panel on macOS computers or the network adapter’s hardware properties on Windows systems.

Waking up computers is possible across subnets as long as an LANrev server or agent is running (active) in the target subnet.

To wake up administered computers:

1. In any browser window, select the computers that you want to control.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Wake Up**.

The **Wake Up** dialog opens. It contains no command-specific options.

3. Click **Execute**.

Scheduling power management events

You can set schedules for all power management events. Events can be scheduled to occur at specific times or after a certain period of inactivity.

A report on the effects of the power management is available, as described in “Displaying a power usage report” on page 150.

Setting up a new schedule

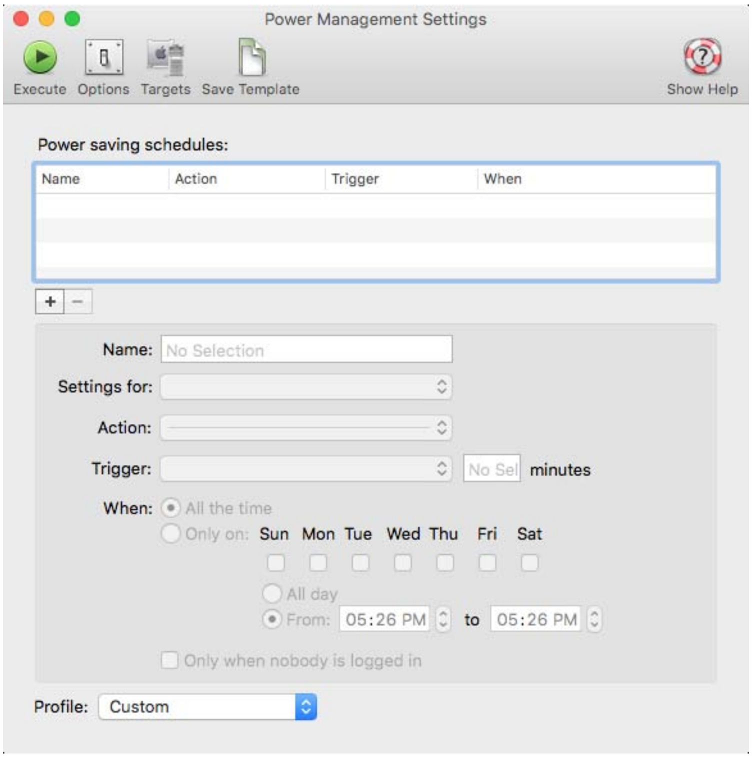
To assign a new schedule to administered computers:

1. In any browser window, select the computers on which you want to set up the schedule.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Power Management Settings**.

   The **Power Management Settings** dialog opens.



Power Management Settings

Power saving schedules:

Name	Action	Trigger	When

Name: No Selection

Settings for:

Action:

Trigger: No Sel minutes

When: ● All the time

○ Only on: Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □

○ All day

● From: 05:26 PM to 05:26 PM

□ Only when nobody is logged in

Profile: Custom

3. Click the **+** button to create a new schedule.

4. Enter a name for the new schedule in the **Name** field.

5. From the **Settings for** pop-up menu, choose the power modes to which the schedule applies.

6. From the **Action** pop-up menu, choose the event that is to occur when the schedule's trigger fires.

   For details on the available options, see "Power Management Settings" on page 412.

7. From the **Trigger** pop-up menu, choose the trigger that initiates the chosen action.

   You can choose between a specific time or a certain period of inactivity.

   When you have chosen **After Inactivity Of**, specify the interval in minutes.

8. Use the **When** checkboxes and radio buttons to specify the time of the day and days of the week when the schedule is active.

   The specified action can occur only on the chosen dates and hours of the day.

9. If desired, add more schedules as described in step 3 through step 8 or delete schedules as described below.

10. Click **Execute**.

All schedules listed in the command dialog are applied to all specified target computers. If any schedules were active on the computers before, they are removed.

Assigning existing schedules

Perform the procedure described in **Setting up a new schedule**, above, but skip step 3 through step 8.

Alternately, you can choose from the **Profile** pop-up menu a profile containing the desired schedules, optionally modify them, and execute the command.

Deleting a schedule

To delete an existing schedule, select it in the **Power saving schedules** list and click the **–** button.

To remove all schedules from a computer, empty the list and execute the **Power Management Settings** command.

Saving schedules

You can save schedules as profiles that can be easily recalled to be applied to target computers.

To save all schedules currently listed in the **Power saving schedules** list as a profile, choose **Save As** from the **Profile** pop-up menu and enter a name for the profile. The new profile is added to the **Profile** pop-up menu.

To rename a profile, choose it from the **Profile** pop-up menu. Then choose **Rename** from the **Profile** pop-up menu and enter the new name.

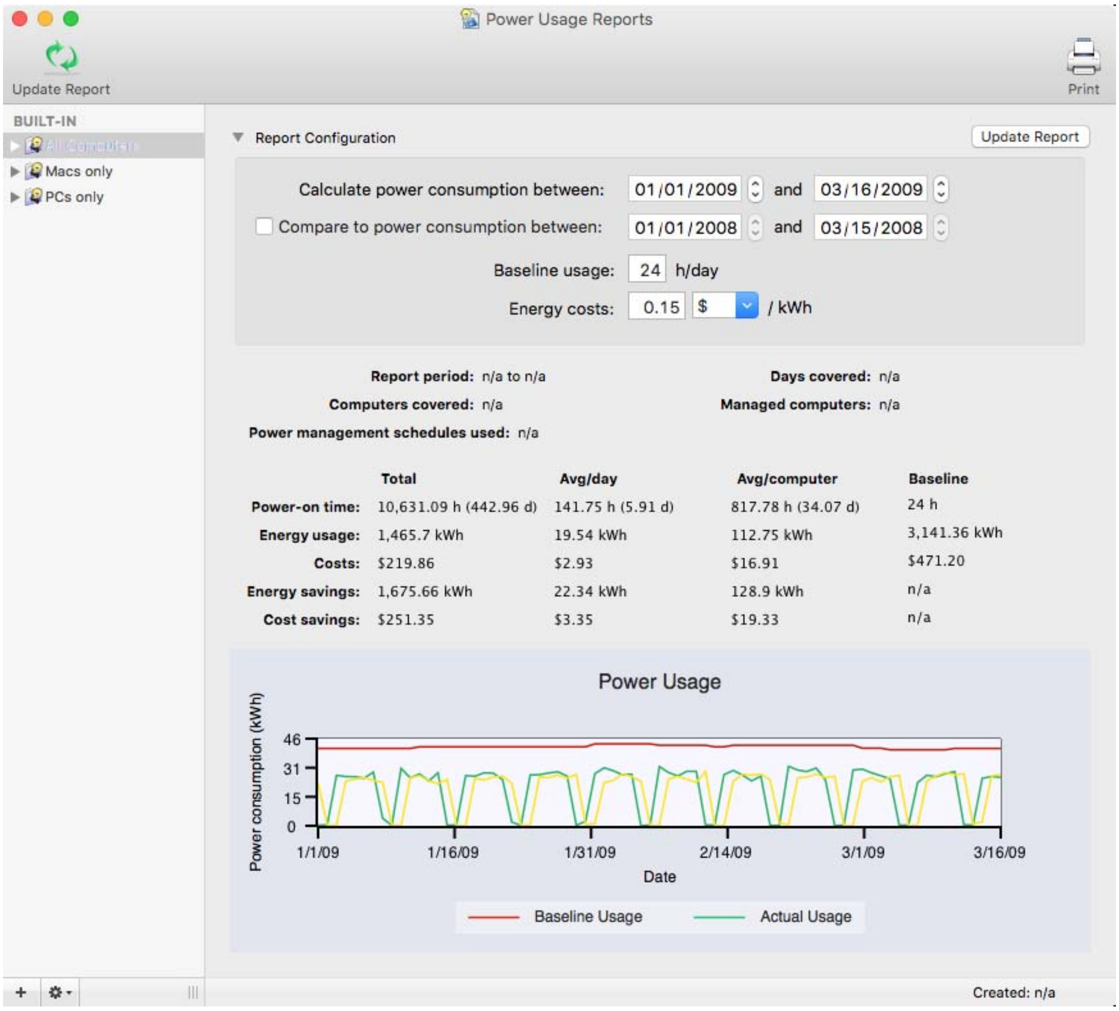
To delete a profile, choose it from the **Profile** pop-up menu. Then choose **Delete** from the **Profile** pop-up menu.

Displaying a power usage report

LANrev can create reports on the savings of power and money that have been achieved by using the power management schedules. To display a report:

1. From the **Window** menu, choose **Power Usage Reports**.

   The **Power Usage Reports** window opens:



Calculate power consumption between: 01/01/2009 and 03/16/2009

□ Compare to power consumption between: 01/01/2008 and 03/15/2008

Baseline usage: 24 h/day

Energy costs: 0.15 $ / kWh

Report period: n/a to n/a

Days covered: n/a

Computers covered: n/a

Managed computers: n/a

Power management schedules used: n/a

	Total	Avg/day	Avg/computer	Baseline
Power-on time:	10,631.09 h (442.96 d)	141.75 h (5.91 d)	817.78 h (34.07 d)	24 h
Energy usage:	1,465.7 kWh	19.54 kWh	112.75 kWh	3,141.36 kWh
Costs:	$219.86	$2.93	$16.91	$471.20
Energy savings:	1,675.66 kWh	22.34 kWh	128.9 kWh	n/a
Cost savings:	$251.35	$3.35	$19.33	n/a

2. In the window’s sidebar, select the computer group on which you want to create a report.

3. Enter the desired report period in the **Calculate power consumption between** fields.

4. Enter the time the computers would have been running without power management schedules in the **Baseline usage** field.

   This is the average number of hours that you think a managed computer would have been running during the report period.

5. Enter the amount of money you pay for power in the **Energy costs** field.

6. Click the **Update Report** button.

The actual and baseline values and savings are displayed in the report window and visualized as a graph. Details regarding the displayed information is available in “Power Usage Reports” on page 505.

NOTE The power consumption of the various devices is set in the **Power Consumption** preference pane.

Remotely controlling computers

LANrev lets you view and control the screens of a client computer using a wide variety of screen sharing software. All that is required to use this feature is that a controlling application is installed on your computer and a compatible client is available on the target computer.

For similar functions related to mobile devices, see “Remotely controlling mobile devices” on page 244.

Supported applications

LANrev supports these screen sharing applications:

- Apple Remote Desktop 3 (guest and host: macOS only)
- DameWare (guest and host: Windows only)
- macOS Screen Sharing (guest: any macOS or Windows computer with a VNC client; host: macOS 10.5 and later only)
- MS Remote Assistance (guest and host: Windows only)
- PC Anywhere (guest and host: Windows only)
- Remote Desktop:
  - CoRD (guest: macOS only; host: Windows only)
  - MS Remote Desktop (guest: macOS or Windows; host: Windows only)
- SSH (guest and host: macOS only)
- Timbuktu (guest and host: macOS or Windows)
- Timbuktu secure (guest and host: macOS only)
- VNC:

- LANrev Remote (guest and host: macOS or Windows)
- Chicken of the VNC (guest: macOS only; host: macOS or Windows)
- JollysFastVNC (guest: macOS only; host: macOS or Windows)
- Real VNC (guest: Windows only; host: macOS or Windows)
- Tight VNC (guest: Windows only; host: macOS or Windows)
- Ultra VNC (guest: Windows only; host: macOS or Windows)

Note: VNC is cross-platform; you can combine any of the above VNC implementations as guest and host applications.

NOTE "Guest" in the above list refers to the platforms on which the software runs as an observer, "host" indicates the platforms that can be observed. For example, using MS Remote Desktop, you can observe or control a Windows computer from a macOS or Windows computer.

Setting up remote control

To set up initiating remote control from within LANrev:

1. If you want to use an application other than LANrev Remote, install the desired screen sharing software on your administrator workstation.

   LANrev Remote is installed automatically as part of LANrev Admin. You can install multiple supported applications.

2. Install compatible client software on all intended target computers if necessary.

   You can use LANrev for doing so; see "Installing software" on page 293 for options.

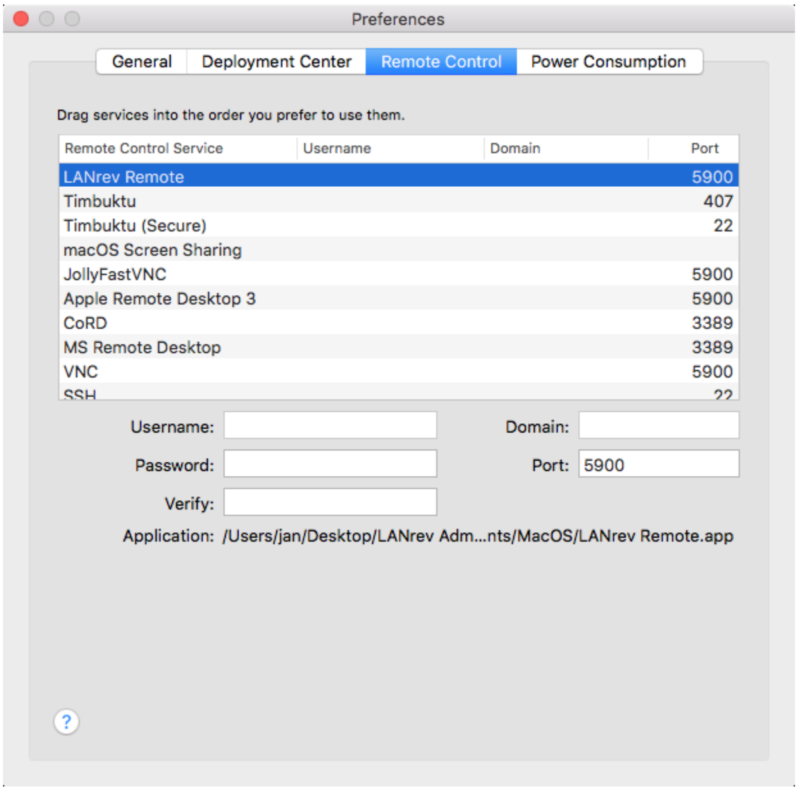
   In some cases, client software is already part of the operating system. For example, macOS includes a VNC client.

   Using LANrev Remote for viewing a client computer requires the function to be enabled on the client. This is done by checking the **Enable screen sharing** option in the **General** pane of the **Agent Settings** dialog.

   You also need to make sure that the port LANrev is using is not already claimed by a different app. For example, macOS Screen Sharing is using port 5900, which is the default port that LANrev Remote is using. If you want to use LANrev Remote to view a computer on which Screen Sharing is enabled, you need to change the port. This can also be done in **Agent Settings**.

   Different client software can be installed on different computers. For example, you can use MS Remote Desktop on some and VNC on others. LANrev automatically selects the correct client, as explained below.

3. To set your preferences, choose **Preferences** from the **LANrev Admin** menu and click the **Remote Control** pane:



Drag services into the order you prefer to use them.

Remote Control Service	Username	Domain	Port
LANrev Remote			5900
Timbuktu			407
Timbuktu (Secure)			22
macOS Screen Sharing			
JollyFastVNC			5900
Apple Remote Desktop 3			5900
CoRD			3389
MS Remote Desktop			3389
VNC			5900
SSH			22

Username:		Domain:	
Password:		Port:	5900
Verify:			

Application: /Users/jan/Desktop/LANrev Adm...nts/MacOS/LANrev Remote.app

4. Arrange the various supported applications in the list in the order in which you would like to prefer to use them by dragging them.

   Note: If a remote control connection to a given client is possible with more than one protocol, LANrev uses the one that is highest in the list. For example, if your list looks like the one in the screenshot above and one client could be controlled through both LANrev Remote and MS Remote Desktop, LANrev uses LANrev Remote.

5. For each protocol that you intend to use, select it in the list and enter the default username, password, domain, and port.

   Some of this information cannot be specified for all protocols.

6. Close the window.

Initiating remote control

To remotely control a client computer:

1. In any browser window, select the computer whose screen you want to share.

2. Right-click the selected computer and choose **Remote Control**.

   LANrev compiles a list of all suitable protocols (that is, all supported protocols for which there is a control application on your computer and client software on the target) and chooses the one that is highest in the list of protocols in the **Preferences** dialog's **Remote Control** pane.

   If LANrev is unable to find suitable client software on the target computer, it displays a dialog (similar to the one described above) in which you can manually specify a protocol and settings to use to connect to the client in question.

3. When a suitable connection setup has been found – either automatically or manually – LANrev prompts the applicable control application on your computer to open a remote control connection to the target. You can then use the applications full capabilities to control the target computer.

   Note: For details on the applications' capabilities, see their respective documentations.

   Note: Some remote control applications do not accept passwords from other software. When using one of these applications, you need to re-enter the password in the application, even when you have already provided it in LANrev.

Launching a remote control session from a URL

In addition to launching a remote control session via the graphical user interface, LANrev also lets you do so via a URL.

This works just like displaying information for a computer via a URL, as described in "Controlling information display from a URL" on page 136, except that the command is "remotecontrolagent" instead of "showagent".

For example, the URL lanrevadmin://remotecontrolagent?computername=My%20Computer launches a remote control session with the computer named "My Computer" as the host.

Note that remote control sessions for mobile devices cannot be launched via a URL.

Locking and wiping computers

LANrev enables you to prevent any access to managed computers and to delete all content from them. Both functions require MDM-managed computers running macOS 10.10 or above and are typically used to protect computers that were stolen or otherwise removed from their proper ownerships.

Locking computers prevents any access to them unless a special password set by you is entered. The password must be entered locally on the computer; it is not possible to remotely unlock locked computers. The lock cannot be circumvented by booting from an external disk or the recovery partition, nor by reinstalling the operating system.

NOTE If you lose the unlock password, accessing the locked computers requires you to contact Apple for assistance.

Wiping computers removes all data from all writable internal and external drives (but not mounted server volumes), including the operating system, applications, and user data. The computer is also locked as described above.

IMPORTANT Wiping a computer irretrievably deletes all information from it (although it might be possible to restore some of the data with specialized forensic tools). If your company is not the owner of that information, such as might be the case with BYOD computers, doing so without the owners consent may expose you to civil or criminal liability.

Locking or wiping a computer

To lock or erase an MDM-managed computer running macOS 10.10 or above:

1. Select the computer in any browser window listing computers,

2. Depending on what you want to achieve, choose one of the commands:

    - To prevent all access to the computer while keeping the information on it intact, choose **Commands** > **Lock macOS Computer**.
    - To remove all content from the computer and prevent any access to it, choose **Commands** > **Erase macOS Computer**.

    Please note that using these commands has serious and – in the case of wiping a computer – irreversible consequences, as described above. Make sure that you understand these consequences before proceeding.

3. Enter a password for unlocking the computer in the **Password** field and repeat it in the **Verification** field.

    We recommend that you note this password in a secure location, because without it the locked computers can only be accessed with the help of Apple’s service department.

4. Click the Execute Command button.

The computer is locked against any access until the password you specified is entered. If you have chosen the wiping command, all data on it is irretrievably deleted. (Although it might be possible to recover some of the data with specialized tools.)

Working with configuration profiles

LANrev lets you centrally manage and deploy configuration profiles for computers running macOS 10.7 or later as well as Workgroup Manager settings (MCX) for computers running Mac OS X 10.5 or 10.6.

You can import existing profiles, edit them and create new profiles. (Workgroup Manager settings can only be imported, not edited or newly created.)

Once a profile has been stored in LANrev, you can install it manually or automatically through software distribution groups.

For details, see:

- “Creating or importing configuration profiles” on page 156
- “Using variables in configuration profiles” on page 159
- “Overview of installing configuration profiles on computers” on page 160
- “Manually installing a configuration profile” on page 160
- “Manually removing a configuration profile” on page 161
- “Installing a configuration profile via a computer group” on page 161
- “Removing a configuration profile via a computer group” on page 162
- “Conflicting installation settings for configuration profiles” on page 162

NOTE Only administrators with the **Modify Configuration Profiles** right can work with configuration profiles and MCX settings. See “New Administrator” on page 758 for details.

Creating or importing configuration profiles

You can both create new configuration profiles and import existing profiles into LANrev (optionally editing them while doing so).

LANrev supports importing and creating profiles for configuring computers running macOS 10.7 or later as well as importing Workgroup Manager settings (MCX) for computers running Mac OS X 10.5 or 10.6. See “Configuration profile editor” on page 666 for details.

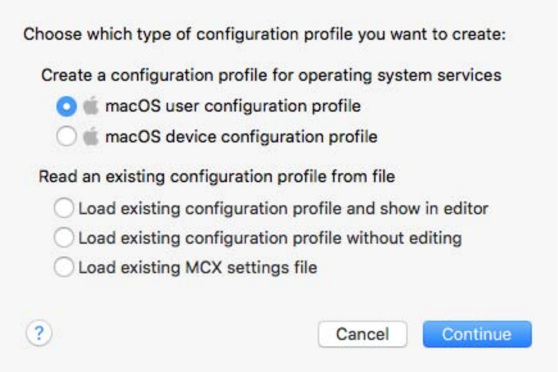
You can use information variables in these configuration profiles, as described in “Using variables in configuration profiles” on page 159.

Creating a new configuration profile

To create a new configuration profile:

1. In the **Server Center** window, right-click in the sidebar and choose **Software Distribution** > **New Configuration Profile** from the context menu.

   The **Configuration Profile Type** dialog opens:



Choose which type of configuration profile you want to create:

Create a configuration profile for operating system services

● macOS user configuration profile

○ macOS device configuration profile

Read an existing configuration profile from file

○ Load existing configuration profile and show in editor

○ Load existing configuration profile without editing

○ Load existing MCX settings file

2. Depending on what kind of profile you want to create, choose **macOS user configuration profile** or **macOS device configuration profile**.

3. Click **OK**.

   The configuration profile editor is opened and displays the available settings for the chosen type of profile.

4. Edit the settings as desired.

   See “Configuration profile editor” on page 666 for more information on the options available in the editor.

5. Click **OK**.

The new profile is created in LANrev and is available for manual or automatic installation on managed computers.

Importing and editing an existing configuration profile

To open an existing profile from disk and import an edited version into LANrev, proceed as described in “Creating a new configuration profile”, above, but choose **Load existing file and show in editor** in step 2.

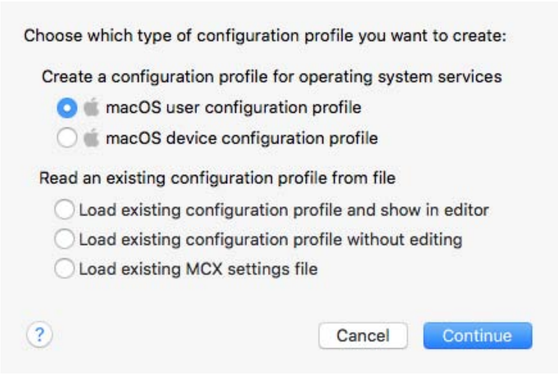
The changed profile is imported into LANrev and is available for manual or automatic installation on managed computers. The configuration profile file on disk is not modified.

Importing a configuration profile or MCX settings file unchanged

To import an existing profile or MCX settings file from disk without editing it:

1. In the **Server Center** window, right-click in the sidebar and choose **Software Distribution** > **New Configuration Profile** from the context menu.

   The **Configuration Profile Type** dialog opens:



Choose which type of configuration profile you want to create:

Create a configuration profile for operating system services

● macOS user configuration profile

○ macOS device configuration profile

Read an existing configuration profile from file

○ Load existing configuration profile and show in editor

○ Load existing configuration profile without editing

○ Load existing MCX settings file

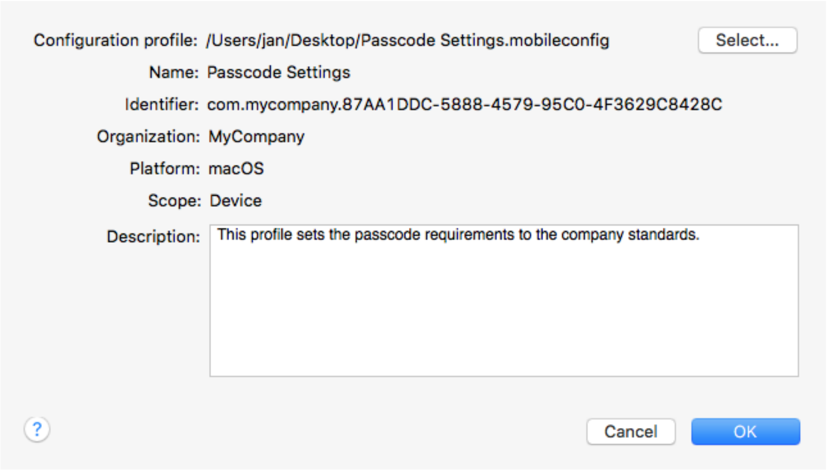
2. Choose the desired option:

   - To load a profile, choose **Load existing configuration profile without editing** and click **OK**.
   - To load an MCX settings file, choose **Load existing MCX settings file** and click **OK**.

   A standard file selection dialog opens.

3. Select the desired file and click **Open**.

   For a configuration profile, the **Configuration Profile** dialog opens:



Configuration profile: /Users/jan/Desktop/Passcode Settings.mobileconfig

Name: Passcode Settings

Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C

Organization: MyCompany

Platform: macOS

Scope: Device

Description: This profile sets the passcode requirements to the company standards.

For an MCX settings file, the **MCX Settings File** dialog opens, which is similar to the Configuration Profile dialog shown above.

See “Configuration Profile dialog for MCX settings files” on page 724 for details.

4. When you import an MCX settings file, edit the **Scope**, **Name**, **Identifier**, **Organization**, and **Description** settings as desired.

5. Click **OK**.

The profile or settings file is imported into LANrev and available for manual or automatic installation on administered computers.

Editing or exporting a configuration profile

You can edit an existing configuration profile or export it as a file to disk:

1. In the sidebar of the **Server Center** window, select the desired profile.

   The details of the profile are displayed in the main part of the **Server Center** window.

   You cannot edit or export MCX settings.

2. In the main part of the window, click the **Edit Profile Settings** button.

3. The Configuration Profile Editor opens and displays the contents of the profile.

4. To edit the profile, change the settings as desired.

5. To export the profile, click the **Save to Disk** button at the lower left of the editor window.

   Note that you can export the profile only if the profile was made exportable by checking the **Allow save to disk** option (see “Common settings” on page 667 for more information) or if you have superadministrator privileges.

Using variables in configuration profiles

LANrev supports the use of variables in configuration profiles for macOS computers. The variables are replaced by LANrev before the configuration profile is installed on the managed device.

The general handling of these variables is described in “Information variables” on page 175. The available variables are listed in “Variables for computers” on page 401. (Note that you cannot use any of the variables that Apple defines for use with Apple Configurator.)

When LANrev applies a configuration profile to a computer, it automatically replaces the variable placeholder in the profile with the current value of the variable for that device. This results in two limitations:

- Configuration profiles containing variables must be applied with LANrev; other tools do not support the variables.

- Any changes to the content or definition of a variable after the configuration profile has been applied have no effect on the computer. For such changes to affect the device, the profile has to be reapplied after the change has been made.

Overview of installing configuration profiles on computers

You can install a configuration profile either manually or via a computer group (software distribution group).

Details of installing configuration profiles are described in:

- **Manually installing a configuration profile** (page 160)
- **Manually removing a configuration profile** (page 161)
- **Installing a configuration profile via a computer group** (page 161)
- **Removing a configuration profile via a computer group** (page 162)
- **Conflicting installation settings for configuration profiles** (page 162)

Manually installing a configuration profile

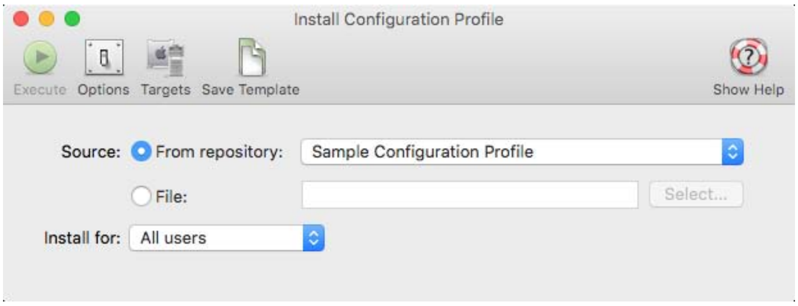
To install a configuration profile on computers:

1. In a browser window, select the computers on which you want to install the configuration profile.

   Make sure to select only computers with a common operating system; all profiles are specific to a particular operating system and cannot be installed on other operating systems.

2. Right-click the computers and choose **Install Configuration Profile** from the context menu.

   The **Install Configuration Profile** dialog opens:



Source: ● From repository: Sample Configuration Profile

○ File:

Install for: All users

3. Specify the profile to install:

   - If you want to install a profile that has already been stored in LANrev (as described in “Creating or importing configuration profiles” on page 156), activate **From repository** and choose the desired profile from the pop-up menu.
   - If you want to install a profile that is available as a file on disk, active **File** and drag the file into the field beside the option or click **Select** to choose the file.

4. If the selected profile is a user profile, choose the user for which it is going to installed from the **Install for** pop-up menu.

   This menu is not available for device profiles.

5. Click **Execute**.

The profile is installed on each selected computer, where it is added to the existing profiles (if any) on the computer. User profiles (as opposed to device profiles) for users not currently logged in will be installed once the user logs in to the computer the next time.

Manually removing a configuration profile

To remove a configuration profile from a computer:

1. In the sidebar of a browser window, expand the computer from which you want to remove the configuration profile.

2. Click the **Installed Profiles** subgroup of the device.

   The configuration profiles that are present on the computer are listed in the main part of the window.

3. Select the profile you want to remove and press the Backspace key.

The profile is removed from the computer. User profiles (as opposed to device profiles) for users not currently logged in will be removed once the user logs in to the computer the next time.

Installing a configuration profile via a computer group

To install a configuration profile on computers automatically:

1. In the **Server Center** window, drag the profile from the **Software Distribution** > **Configuration Profiles** group to one of the subcategories of the computer group (in the **Computer Groups** section) via which you want to distribute it:

   - **Auto-install Configuration Profiles**: The profile is pushed to the computers in the group. It remains on a computer even after the computer is removed from the policy. (After this point, users can remove the profiles manually, however.)
   - **Auto-install, auto-remove Configuration Profiles**: The profile is pushed to the computers. It is automatically deleted from a computer that is removed from the computer group.

   Note that the actual effect may be different for computers that also belong to other policies where the same configuration profile has a different role. See “Conflicting installation settings for configuration profiles” on page 162 for details.

The profile is sent to all computers that belong to the computer group. User profiles (as opposed to device profiles) for users not currently logged in will be installed once the user logs in to the computer the next time.

If computers are later added to the group, the profile is installed on them as well. (This may not be the case for computers also belonging to another policy in which the configuration profile is forbidden. See "Conflicting installation settings for configuration profiles" on page 162 for details.)

Removing a configuration profile via a computer group

To remove a configuration profile from computers automatically:

1. In the **Server Center** window, drag the profile from the **Software Distribution** > **Configuration Profiles** group to the **Forbidden Configuration Profiles** folder of the computer group (in the **Computer Groups** section) via which you want to remove it.

The profile is removed from all computers belonging to the computer group. (This may not be the case for computers also belonging to a different group with conflicting settings. See "Conflicting installation settings for configuration profiles" on page 162 for details.) User profiles (as opposed to device profiles) for users not currently logged in will be removed once the user logs in to the computer the next time.

If computers are later added to the computer group, the profile is removed from them as well (unless they also belong to a different group which prevents this).

NOTE Profiles in the "Auto-install, Auto-remove Configuration Profiles" subcategory of a computer group are automatically removed from any computer that is removed from the group.

You can also remove configuration through computer groups by adding an action to the group. See "Working with actions" on page 178 for details.

Conflicting installation settings for configuration profiles

It is possible to assign a configuration profile to multiple computer groups in different roles. For example, it could be auto-installed in one policy and forbidden in another.

This can become an issue if one computer is a member of multiple groups and these groups contain the same configuration profile in different categories.

For example, a computer could belong to one computer group in which the profile is automatically installed and another in which it is forbidden. Clearly, there is no way to satisfy both groups' requirements at the same time.

In cases like this, LANrev uses this hierarchy for the different categories of profiles:

- Forbidden
- Auto-install
- Auto-remove

Higher entries have precedence over lower entries. For example, if a configuration profile is auto-installed in one group to which a computer belongs and forbidden in another, the profile is not available on the computer because the “forbidden” category has a higher priority than “auto-install”.

This means that, in some instances, an auto-installed and auto-removed profile remains on a device even when the computer is removed from the computer group in question. This is the case when the computer also belongs to another group in which the profile auto-installed (and the device does not belong to a policy in which the profile is forbidden).

Controlling Time Machine

Using LANrev, you can control the Time Machine feature of client computers running macOS 10.5 or later. You can:

- Initiate a backup
- Stop a backup
- Activate automatic Time Machine backups
- Deactivate automatic Time Machine backups

To control the operation of Time Machine:

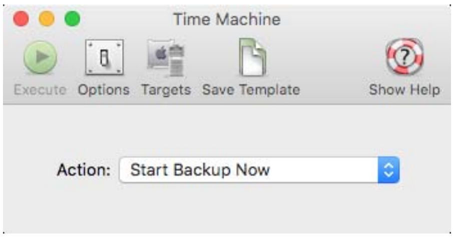
1. In any browser window, select the computers on which you want to control Time Machine.

   Only target computers running macOS 10.5 or later will be affected by this procedure.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Time Machine**.

   The **Time Machine** dialog opens:



Action: Start Backup Now

3. Choose the desired action from the pop-up menu.

4. Click **Execute**.

Tracking computers

You can use LANrev to track the current locations of mobile computers.

This capability – called TheftTrack – is largely automatic; it requires minimal configuration and is thereafter available whenever needed.

For information on tracking the locations of mobile devices, see “Geotracking mobile devices” on page 259.

NOTE LANrev’s computer tracking is not a comprehensive theft prevention or retrieval solution and should not be considered as such. (For example, thieves could circumvent it by reformatting the computer’s hard disk.) This feature can, however, be an important part of a larger comprehensive system that you set up.

NOTE Computer tracking can be set and altered only by administrators with the **Change Computer Tracking** right. See “New Administrator” on page 758 for details.

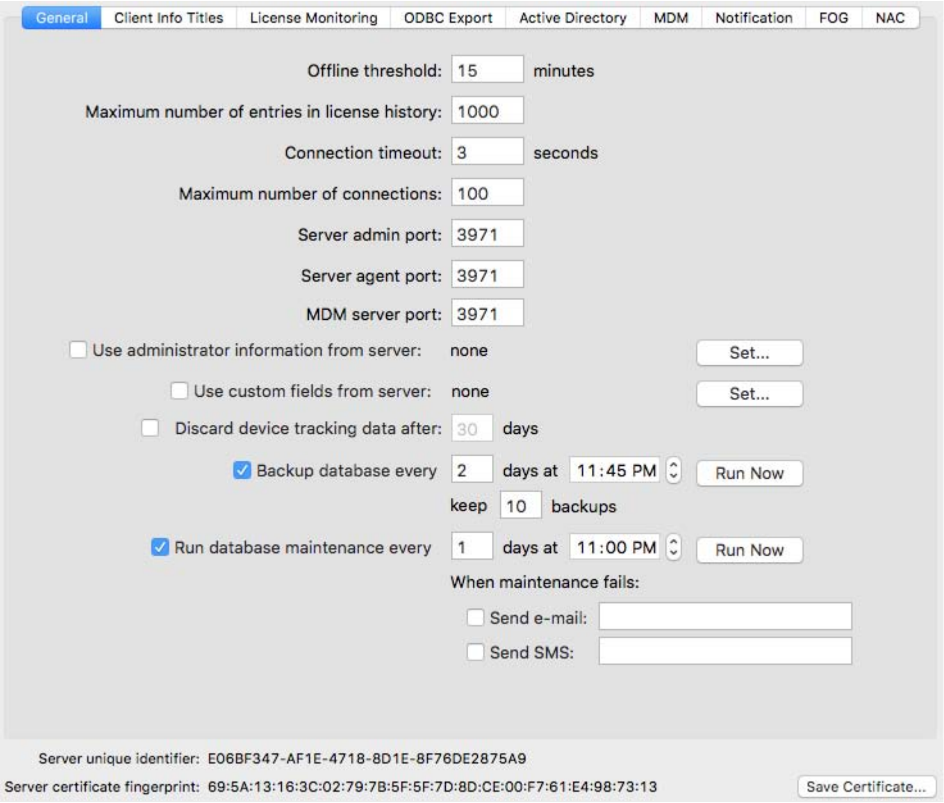
Setting up computer tracking

To set up computer tracking, you must make sure that at least one of your LANrev servers can be reached from the Internet. As most servers are usually secured behind a firewall, you will often have to take special steps to make this possible.

To set up a server for access from the Internet:

1. In the **Server Center** window, click the **Server** > **Server Settings** category.

The server settings are displayed in the main part of the window.



Offline threshold: 15 minutes

Maximum number of entries in license history: 1000

Connection timeout: 3 seconds

Maximum number of connections: 100

Server admin port: 3971

Server agent port: 3971

MDM server port: 3971

□ Use administrator information from server: none

□ Use custom fields from server: none

□ Discard device tracking data after: 30 days

☑ Backup database every 2 days at 11:45 PM

keep 10 backups

☑ Run database maintenance every 1 days at 11:00 PM

When maintenance fails:

□ Send e-mail:

□ Send SMS:

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9

Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13

Note: The Server Setting command is available only to administrators with the **Change Server Settings** *right. See "New Administrator" on page 758 for details.*

2. In the dialog's **General** tab, set the agent port to a different number than the admin port.

   This separation of the ports is necessary so that the admin port can remain inaccessible from the Internet.

3. If you want to keep the data generated while tracking computers for only a limited time, check the **Discard computer tracking data after** option and enter the desired number of days after which LANrev is to delete data.

4. Click **OK** to save the new server settings.

5. In your firewall, open the port that you have specified as LANrev Server's agent port.

You have now set up LANrev Server so that it can receive information from agents even if they are located outside of your organization’s network, as long as they are connected to the Internet.

NOTE The LANrev Server will not accept administrative requests over the agent port. Only agent communication is possible over that port. (This does not apply if both ports are identical.)

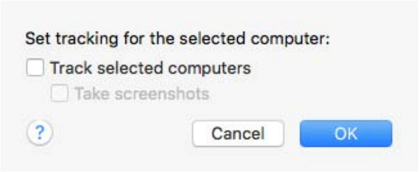
Starting to track a computer

LANrev does not automatically track all administered computers; rather, you specifically tell it which ones you want to monitor.

To specify that a computer be tracked:

1. In any browser window, select the computer that you want to track.
2. Right-click the computer and choose **Computer Tracking** from the context menu.

   The **Computer Tracking** dialog opens:



Set tracking for the selected computer:

□ Track selected computers

□ Take screenshots

3. To track the computer, check **Track selected computers**. If you want the computer to transmit screenshots, check that option as well.
4. Click **OK**.

LANrev immediately starts tracking the computer and continues to do so until you disable tracking.

NOTE Tracking can be enabled when the computer is already outside your network but requires one contact between the agent and LANrev Server to actually begin.

Stopping the tracking of a computer

To stop tracking a computer, open the **Computer Tracking** dialog as described above and uncheck the **Track selected computers** option.

Getting information on tracked computers

You can get information on tracked computers in three ways:

- In a browser window table

To get information on all tracked computers in a table, open a new browser window and add the information items of the **Computer Tracking** category, as described in “Opening and configuring browser windows” on page 132.
Note: The information items are explained in “Computer Tracking” on page 870.

- In the detailed computer view
  To get information on an individual computer, open that computer’s detail view as described in “Displaying an overview of a single computer” on page 135 and click the **Computer Tracking** category.
  If you have set the tracked computer to take screenshots, they are displayed here as well. The context menu of the screenshot lets you view it in a separate window or Preview or copy it to the clipboard.
- In an exported HTML or XML file
  To get information on all tracked computers in an exported file, list all computers which you want to include in the file in a browser window and choose **Export** from the **File** menu. Choose either of the two **TheftTrack Report** options from the **File Format** menu in the Save dialog.

You can use the information displayed by LANrev for taking appropriate steps to physically locate and retrieve the computers.

You can also send commands to the tracked computer (for example, to execute shell scripts), even if is located behind a firewall. Commands that you send are queued and executed when the tracked computer sends the next ‘heartbeat’ signal.

Executing files from your computer

LANrev can execute files from an administrator’s computer on administered computers. Because these files can be scripts or application programs, a wide range of tasks can be performed with this feature.

The main limitation is the unavailability of remote input – you cannot enter any parameters while a script or application is running. This means that you need to rely on the cooperation of the local users, use a screen-sharing utility such as VNC, or make sure that no input is required.

To execute a file from your computer on administered computers:

1. In any browser window, select the computers on which you want to execute the file.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose the desired command:

- **Execute Script** to execute a Unix shell script or AppleScript (only on macOS client computers) or a DOS batch file, Visual Basic script, or Powershell script (only on Windows client computers)
  Note that you can also execute scripts automatically by adding an action to a computer group. See "Working with actions" on page 178 for details.
- **Execute macOS File** to execute a macOS application (only on macOS client computers)
- **Execute Windows File** to execute a Windows application (only on Windows client computers)

The command dialog opens. The individual dialogs are described below.

3. Set the desired options, as described below.

4. Click **Execute**.

The file is copied to the target computers, executed there, and removed when the execution has been completed.

Script

Enter a script text in the **Text** field or select a text file containing a script file.

- If you enter a script text or choose an uncompiled text file, you must make sure that the text conforms to the respective syntax. In the case of AppleScript text entered directly, the **Check Syntax** button can help you.
  *Note: When you specify scripts that are intended for computer platforms different from the one you are using, LANrev automatically converts the scripts' line endings to the convention required by the target platform. This does not apply to auxiliary files uploaded by means of the "***Transfer all files in folder containing executable***" option described below.*
- If desired, specify command line options for the script. LANrev provides these options to the script on the target computers according to the respective script architecture's conventions. You can include shell variables in the options, as described in "Environment variables" on page 176.
- By default, any results the scripts return can be viewed in the command history. To have the results be displayed in their own windows upon script completion, check the **Automatically view results** option.
  To view the results from all target computers together in a single window, also check **All results in one window**.
- If the script must be executed with the privileges of an (operating system) administrator, check the **Executable requires administrative privileges** option.
  Note: Checking this option does not change the user account in which the script is executed, it merely gives the script more privileges. This is similar to authorizing installer applications by supplying an administrator password.

- Except for AppleScript scripts, choose the user context in which the script is to be executed – either in the account of whatever user is currently logged in, with a system account, or in a specified account. In the latter case, the specified account must exist on all target computers.
- Note that scripts that access other applications need these applications to be present on the target computers and have the same names there. If applications are missing or have different names, script execution will fail.
- If the script relies on additional files that must be transferred to the target computers, put them in the same folder and check the **Transfer all files in folder containing executable** option.

Details on the elements of the command dialog are available in "Execute Script" on page 429.

macOS application

Select the desired application using the **Select** button.

Choose the installation volume. Specify the user account, as described above in "Script".

Specify the execution method – whether to copy the file from your computer or from a server, and in the latter case using which method. If the application is to be copied from a server, provide the necessary access details.

If desired, you can give command line options and a working directory.

Specify a message, if desired. The details are described in "Sending messages" on page 144.

NOTE If a message has been specified, this is indicated by a diamond in the dialog's **Message** tab.

Details on the elements of the command dialog are available in "Execute macOS File" on page 431.

Windows application

Select the desired application using the **Select** button.

Specify the user account in which the application is to be executed. You can choose either the current user, the local system administrator account, or a specific user account. In the latter case, you must specify the password. Also, the account must be available on every target computer – either locally or via the domain – and have the same password everywhere. When you specify a domain username, you must prefix the domain.

If desired, you can give command line options and a working directory.

NOTE When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, LANrev adds the `/qn` option (`/quiet /norestart` for MSU files) to run the installer silently. When you add your own options or when another type of installer is selected, you have to provide the command line parameters for a silent installation yourself.

Specify the execution method – whether to copy the file from your computer or from a server, and in the latter case using which method. If the application is to be copied from a server, provide the necessary access details.

Specify a message, if desired. The details are described in “Sending messages” on page 144.

NOTE If a message has been specified, this is indicated by a diamond in the dialog’s **Message** tab.

Details on the elements of the command dialog are available in “Execute Windows File” on page 434.

Executing local files

LANrev can execute files that are already present on the target computers. This requires the same file to be present on every target computer at the same location.

NOTE Information on copying files to target computers is available in “Transferring files to administered computers” on page 290.

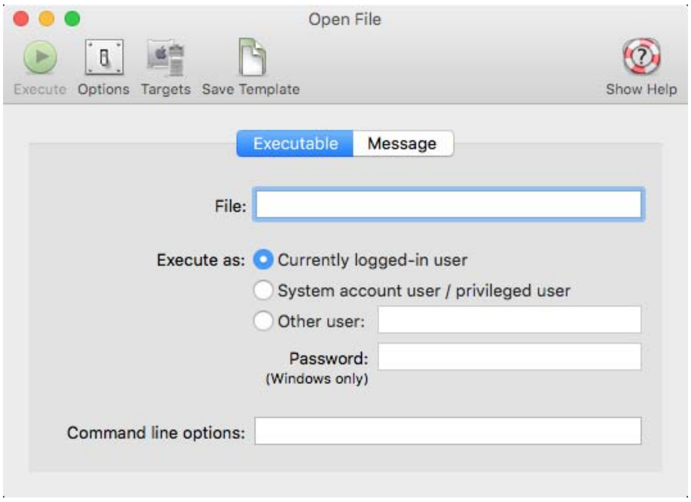
To execute a file that is already on the target computers:

1. In any browser window, select the computers on which you want to execute the file.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Open File**.

The **Open File** dialog opens:



File:

Execute as: ● Currently logged-in user
○ System account user / privileged user
○ Other user:
Password:
(Windows only)

Command line options:

3. Enter the path of the file that you want to execute.

   Note: If you select a file in step 1 (instead of computers), the path of that file is pre-entered in the dialog.

4. Specify the user account in which the file is to be executed.

   You can specify, the currently active user account, a user with system administrator privileges, or a specific account. In the latter case, you must provide the password for Windows target computers (but not macOS targets).

5. If desired, you can specify command line options, provided the target application supports them

   You can include shell variables in the options, as described in "Environment variables" on page 176.

6. Click **Execute**.

Terminating processes

LANrev lets you terminate processes on administered computers.

In addition to terminating processes manually, as described below, processes can also be terminated automatically by adding an action to a computer group. See "Working with actions" on page 178 for details.

There are two variants for killing processes: 'soft', allowing users to save any changes, and 'hard', instantly killing the processes.

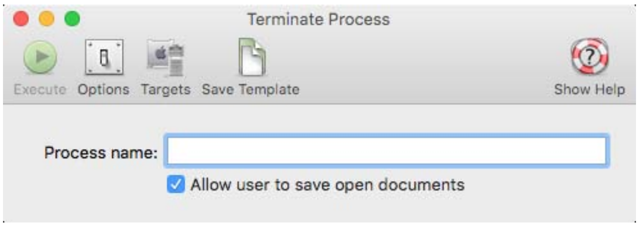
To terminate a process on administered computers:

1. In any browser window, select the computers on which you want to terminate the process.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Terminate Process**.

   The **Terminate Process** dialog opens:



Process name:
☑ Allow user to save open documents

3. Enter the name of the process that you want to terminate. The process must have the same name on all target computers.

   Note: If you select a process in step 1 (instead of computers), the name of that process is pre-entered in the dialog.

4. Choose a 'soft' or 'hard' termination.

   For a 'soft' termination, check **Allow user to save open documents**. In this case, the process is sent a 'terminate' event. The effect is similar to choosing **Quit** in an application. If the process is still operative, users have an opportunity to save any unsaved changes. If the process hangs, it cannot be terminated in this way; you must choose the 'hard' termination.

   For a 'hard' termination, uncheck the option. This is equivalent to forcefully killing a process.

5. Click **Execute**.

Working with services

You can use LANrev to start and stop services on administered Windows computers as well as specify their startup status.

Stopping a service

To stop a service on an administered Windows computer:

1. In any browser window, select the computers on which you want to terminate the services.

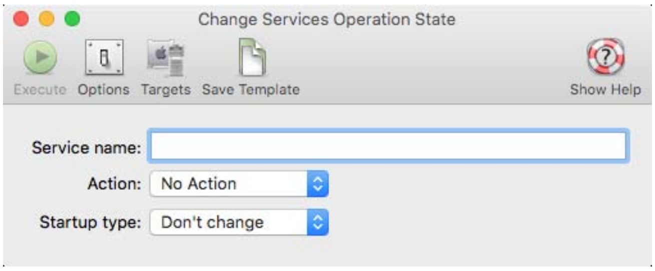
   Note: If the desired service is contained in the server database (the information having been collected with the **Gather Inventory**

Information *command), you can also select the service in a browser window in which it is displayed. To display services, add information items from the* **Windows Services** *information items group.*

Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Change Services Operation State**.

   The **Change Services Operating State** dialog opens:



Service name:

Action: No Action

Startup type: Don't change

3. Enter the name of the service that you want to stop (as displayed in the **Service Name** information item. The service must have the same name on all target computers.

   Note: If you select a service in step 1 (instead of computers), the name of that service is pre-entered in the dialog.

4. Choose **Stop** from the **Action** pop-up menu.

5. Click **Execute**.

Starting or restarting a service

To start or restart a service, proceed as described in **Stopping a service**, above, but choose **Start** or **Restart**, respectively, from the **Action** pop-up menu.

Setting a service's startup status

To set a services' startup status, proceed as described in **Stopping a service**, above, but make no choice from the **Action** pop-up menu.

Instead, choose an option from the **Startup type** pop-up menu, depending on the desired effect:

- **Automatic**: The service is automatically started whenever the operating system boots.
- **Manual**: The service is not automatically started but may be started by users or other applications.
- **Disabled**: The service cannot be started at all.

Editing the registry

LANrev lets you create, edit, and delete keys and values in the registries of Windows client computers.

In addition to editing registry entries manually, as described below, the registry can also be modified automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

NOTE It is easier to work with registry entries that are listed in the Registry Entries table of the LANrev database. Searching for entries to include them in the database is described in “Gathering information on registry entries” on page 103.

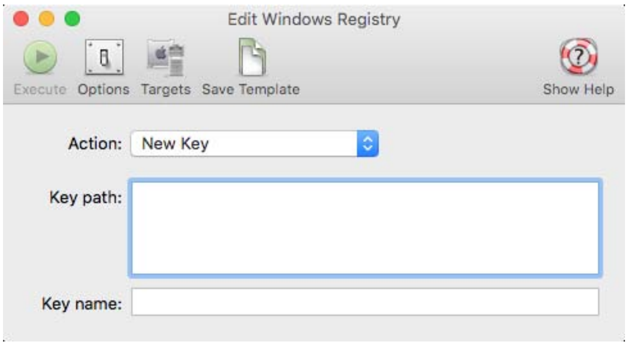
To edit the registry:

1. In any browser window, select the computers on which you want to edit the registry. Or select a registry entry that you want to edit in the **Registry Entries** window or any other browser window displaying registry entries.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Edit Windows Registry**.

   The **Edit Windows Registry** dialog opens:



Action: New Key

Key path:

Key name:

   Note: Which fields are displayed in the dialog depends on the chosen action. If you have selected a registry entry before choosing the command, values from that entry are pre-entered into the dialog.

3. Choose the desired action from the **Action** pop-up menu.

   LANrev displays the fields appropriate to the action in the dialog.

4. Fill in the fields that are visible:

   - **Key path**: Enter the path of the key in which you want to create a new key or value.

- **Key name**: Enter the new key’s name.
- **Value path**: Enter the path of the value that you want to change.
- **Value type**: Specify the new data type of the value.
- **Value**: Enter the data that is to be stored in the specified value.
- **Path**: Specify the path of the key or value that you want to rename or delete.
- **New name**: Enter the new name of the specified key or value.

When you specify a path, you can include environment variables, as described in “Environment variables” on page 176.

5. Click **Execute**.

Variables

You can use variables to customize actions and texts for individual targets.

LANrev provides two kinds of variables:

- Information variables: These variables give you access to the contents of information fields in text that is sent to or displayed on client devices by commands or actions and in configuration profiles. See “Environment variables” on page 176 for details.
- Environment variables: These are variables available in the operating system that you can, in particular, use in scripts. See “Environment variables” on page 176 for details.

Information variables

Information variables give you access to the values of certain information items for a target device, allowing you to customize messages and settings without needing individual commands for each target.

You can use information variables in commands and similar circumstances when specifying text that is sent to or displayed on the device (such as the body of an e-mail):

- In command dialogs
- In action definitions
- In configuration profiles

LANrev replaces a variable at execution time with the actual information for the target device.

Defining a variable

A wide range of variables is predefined; you can immediately use these variables.

In addition, you can define your own variables by specifying custom information fields, giving them the manual style (meaning that the information in them is not automatically calculated by LANrev), and specifying a variable name for the field, as described in “Defining custom information fields” on page 108.

Using an information variable

To use a variable in a text field, enclose it in curly brackets and prefix a dollar sign, for example, `${MDU_Company}`.

You can use all these predefined variables:

- “Variables for computers” on page 401
- “Variables for mobile devices” on page 458

In addition, you can use any custom information fields that you have given a variable name. (See “Defining custom information fields” on page 108 for more information on this.)

Environment variables

Several commands let you use shell or environment variables. LANrev can use the standard variables of the target system and defines several variables of its own.

Using shell variables

The conventions for using shell variables in command options depend on the target OS platform (that is, the OS running on the clients you are targeting):

- For macOS targets, enclose the variable in curly braces and prefix it with a dollar sign. For example: "${HOME}".
- For Windows target, enclose the variable in percent signs. For example: "%USERPROFILE%"

In either case, the entire string must be enclosed in quotes.

File-related variables defined by LANrev

LANrev includes some special environment variables related to file and folder locations:

- LANREV_EXECUTABLE_DIRECTORY: the local folder into which payloads are downloaded during installations
- ProgramFilesx64: On 64-bit Windows systems, the folder in which 64-bit applications are stored (usually C:\Program Files). On other systems, this variable is undefined.
- ProgramFilesx32: On 64-bit Windows systems, the folder in which 32-bit applications are stored (usually C:\Program Files (x86)). On 32-bit Windows systems, the folder in which applications are stored (usually C:\Program Files). On other systems, this variable is undefined.
- ProgramFilesSystemNative: On Windows systems, the folder in which system-native applications – that is, 32-bit applications

on 32-bit systems and 64-bit applications on 64-bit systems – are stored (usually C:\Program Files). On other systems, this variable is undefined.

- CommonProgramFilesx64: On 64-bit Windows systems, the folder in which common files used 64-bit applications are stored (usually C:\Program Files\Common Files). On other systems, this variable is undefined.
- CommonProgramFilesSystemNative: On Windows systems, the folder in which the common files used by system-native applications – that is, 32-bit applications on 32-bit systems and 64-bit applications on 64-bit systems – are stored (usually C:\Program Files\Common Files). On other systems, this variable is undefined.
- SysDirx32: On Windows systems, the system folder for 32-bit applications. On other systems, this variable is undefined.
- SysDirx64: On 64-bit Windows systems, the system folder for 64-bit applications. On other systems, this variable is undefined.
- SysDirxSystemNative: On Windows systems, the system folder for system-native applications. (For 32-bit system, this is the same as SysDirx32. For 64-bit systems, this is the same as SysDirx64.) On other systems, this variable is undefined.

These variables do not apply to AppleScript scripts. Most of them are not available outside of LANrev, although LANREV_EXECUTABLE_DIRECTORY is available as a command line option for scripts and applications launched by LANrev.

Registry-related variables defined by LANrev

LANrev includes some special environment variables related to registry locations:

- HKLM_Softwarex32 and HKEY_LOCAL_MACHINE_Softwarex32: The registry software hive for 32-bit applications.
  On 32-bit systems, this is HKEY_LOCAL_MACHINE\Software; on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software\Wow6432Node.
- HKLM_Softwarex64 and HKEY_LOCAL_MACHINE_Softwarex64: The registry software hive for 64-bit applications.
  On 32-bit systems, this is undefined; on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software.
- HKLM_SoftwareSystemNative and HKEY_LOCAL_MACHINE_SoftwareSystemNative: The registry software hive for the native applications on the system.
  On 32-bit systems, this is HKEY_LOCAL_MACHINE\Software; on 64-bit systems, this is HKEY_LOCAL_MACHINE\Software.

These variables cannot be used with the **Execute Script** command. They are, however, available for license specifications and software installations.

Working with actions

Actions let you specify what LANrev is to do when a computer is added to a smart computer group.

Available actions include:

- Sending a message, e-mail, or text (SMS) to the device
- Sending an e-mail or text (SMS) to an administrator
- Changing the Agent name of the device
- Setting the values of custom information fields for the device
- Updating the information about the device stored on the inventory server
- Adding the device’s user to the VPP program or removing them
- Sending an invitation to register for the VPP program
- Execute a script
- Terminate a process
- Edit the Windows registry
- Removing MDM or configuration profiles

Actions are defined centrally and stored in the **Actions** group in the **Server Center** window, from where they can be assigned to any desired smart computer groups.

Details of working with actions are described below.

Creating a new action

To create a new action:

1. In the sidebar of the **Server Center** window, choose the appropriate command from the **Actions** submenu of the context menu:

   - **New Send Message Action** to create an action that sends a message to the computer that has joined the computer group.
   - **New Send E-Mail Action** to create an action that sends an e-mail to one or more specified addresses (usually those of administrators).
     Note that LANrev can send e-mails only when the SMTP information in the **Notification** tab of the **Server Settings** is filled in.
   - **New Send SMS (Text Message) Action** to create an action that sends a text message (SMS) to one or more specified phones (usually those of administrators).
     Note that LANrev can send texts only when the SMS information in the **Notification** tab of the **Server Settings** is filled in.
   - **New Set Agent Name Action** to create an action that changes the name that the Agent reports for the device.

- **New Set Custom Field Value Action** to create an action that sets the value of a manual custom information field for the computer.
- **New Gather Inventory Action** to update the information stored on the inventory server for the computer. (As if **Gather Inventory Information** has been chosen for the computer.)
- **New Register User in VPP Action** to create an action that adds the computer's user to the VPP program.
- **New Send VPP Invitation Action** to create an action that sends an invitation to register in the VPP program to a user.
- **New Retire User from VPP Action** to create an action that removes the device's user from an VPP account.
- **New Remove Configuration Profile Action** to create an action that removes a configuration profile from the computer.
- **New Execute Script Action** to create an action that executes a script on the computer.
- **New Terminate Process Action** to create an action that terminates a process runing on the computer.
- **New Edit Windows Registry Action** to create an action that modifies the registry on the computer.
- **New Remove from MDM Management Action** to create an action that removes the MDM profile from the computer. (The computer is still administered through LANrev.)

A dialog specific to the action is displayed.

2. Fill in the dialog's fields as desired.

   For an explanation of the available fields, see the dialog descriptions in:

   - "New Send Message Action" on page 743
   - "New Send E-Mail Action" on page 744
   - "New Send SMS (Text Message) Action" on page 745
   - "New Set Agent Name Action" on page 746
   - "New Set Custom Field Value Action" on page 747
   - "New Gather Inventory Action" on page 747
   - "New Register User in VPP Action" on page 749
   - "New Send VPP Invitation Action" on page 750
   - "New Retire User from VPP Action" on page 752
   - "New Remove Configuration Profile Action" on page 753
   - "New Execute Script Action" on page 754
   - "New Terminate Process Action" on page 755
   - "New Edit Windows Registry Action" on page 756
   - "New Remove from MDM Management Action" on page 757

3. Click **OK** to save the action.

The new action appears in the **Actions** group of the sidebar and can be assigned to smart computer groups, as described in "Specifying actions in computer groups" on page 329.

Re-executing actions

You can re-execute actions on computers in various ways:

- A single action on a single computer: Display the computer in the sidebar of the **Server Center** window; expand it and click its **Performed Actions** subcategory; right-click the desired action and choose **Re-execute This Action for This Device** from the context menu.
- A single action on all applicable computers: Expand the **Actions** category in the sidebar of the **Server Center** window; right-click the desired action in the main table of the window and choose **Re-execute This Action for All Devices** from the context menu.
- A single action on all devices of a computer group: Expand the computer group in the sidebar of the **Server Center** window and click its **Actions** subcategory; right-click the desired action and choose **Re-execute This Action for This Policy** from the context menu.
- All actions on a single computer: Display the computer in the sidebar of the **Server Center** window; expand it and click its **Performed Actions** subcategory; right-click anywhere in the window’s table area and choose **Re-execute All Actions for This Device** from the context menu.

In each case, an alert is displayed in which you can choose between re-executing the actions when a target device next checks in and immediately re-executing them. Choosing immediate execution sends push notifications to the devices to check in with the MDM server.

Any delays and repetitions you have specified for an action also apply when it is re-executed.

Reviewing actions

All actions that have been applied to a computer are listed in the **Performed Actions** subgroup of the device when it is expanded in the sidebar of the **Server Center** window.

Deleting actions

To delete an action from LANrev, right-click it in the sidebar of the **Server Center** window and choose **Remove Action** from the context menu.

This deletes the action, including removing it from all computer groups to which it is assigned.

For removing actions from individual policies, see “Specifying actions in computer groups” on page 329.

Chapter 6 *Working with mobile devices*

Mobile devices running iOS or Android are administered from LANrev through an MDM (mobile device management) server.

See “Installing MDM support” on page 26 for information on installing the server and “Enrolling mobile devices” on page 50 for information on activating the MDM for a particular mobile device.

Details are described in these sections:

Working with configuration profiles

LANrev lets you centrally manage and deploy configuration profiles for mobile devices.

You can import existing profiles, edit them and create new profiles. Information variables can be used in these profiles that let you include certain device-specific values, for example, in descriptions.

Once a profile has been imported into LANrev, you can install it manually, automatically through policies, or let the users decide whether to install a particular profile.

For details, see:

- “Creating or importing configuration profiles” on page 182
- “Using variables in configuration profiles” on page 185

- “Overview of installing configuration profiles on mobile devices” on page 186
- “Manually installing a configuration profile” on page 186
- “Manually removing a configuration profile” on page 189
- “Installing a configuration profile via a policy” on page 189
- “Making a configuration profile available for optional installation” on page 190
- “Removing a configuration profile via a policy” on page 191
- “Conflicting policy settings for configuration profiles” on page 192

Creating or importing configuration profiles

You can both create new configuration profiles and import existing profiles into LANrev (optionally editing them while doing so).

LANrev supports creating profiles for configuring basic iOS, Android, or Windows Phone settings, profiles for proprietary extensions from several Android vendors, and profiles for a number of mobile applications. See “Configuration profile editor” on page 666 for details.

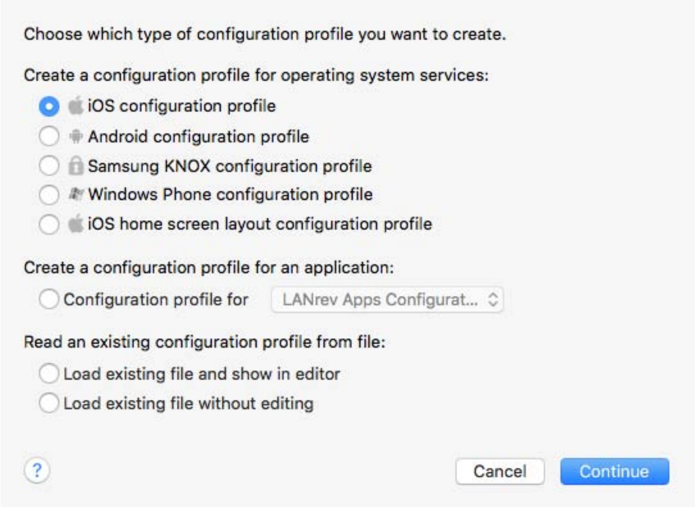
You can use variables in these configuration profiles, as described in “Using variables in configuration profiles” on page 185.

Creating a new configuration profile

To create a new configuration profile:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Configuration Profiles and Certificates** > **New Configuration Profile** from the context menu.

   The **Configuration Profile Type** dialog opens:



Choose which type of configuration profile you want to create.

Create a configuration profile for operating system services:

● iOS configuration profile
○ Android configuration profile
○ Samsung KNOX configuration profile
○ Windows Phone configuration profile
○ iOS home screen layout configuration profile

Create a configuration profile for an application:

○ Configuration profile for LANrev Apps Configurat...

Read an existing configuration profile from file:

○ Load existing file and show in editor
○ Load existing file without editing

2. Depending on what you want to do, choose the appropriate option in this dialog:

   - To create a new device configuration profile, choose one of the options in the first group (depending on the intended target platform).
   - To create a configuration profile for a mobile app, click **Configuration profile for** and choose the desired app from the pop-up menu.
     Support for creating app configuration profiles must be provided from the app's developer in the form of an add-on module that you copy into the ~/Library/Application Support/LANrev Admin/Profile Editor Modules folder.

3. Click **Continue**.

   The configuration profile editor is opened and displays the available settings for the chosen type of profile.

   If you have chosen **iOS home screen layout configuration profile**, the home screen editor is opened instead. Working with this editor is described in "Configuring home screen layouts" on page 254.

4. Edit the settings as desired.

   See "Configuration profile editor" on page 666 for more information on the options available in the editor.

5. Click **OK**.

The new profile is created in LANrev and is available for manual or profile-based installation on managed mobile devices.

Importing and editing an existing configuration profile

To open an existing profile from disk and import an edited version into LANrev, proceed as described in "Creating a new configuration profile", above, but choose **Load existing file and show in editor** in step 2.

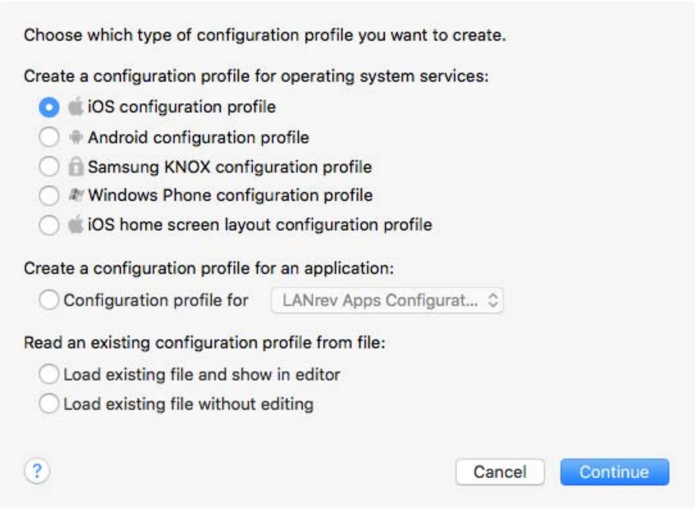
The changed profile is imported into LANrev and is available for manual or profile-based installation on managed mobile devices. The configuration profile file on disk is not modified.

Importing a configuration profile unchanged

To import an existing profile from disk without editing it:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Configuration Profiles and Certificates** > **New Configuration Profile** from the context menu.

The **Configuration Profile Type** dialog opens:



Choose which type of configuration profile you want to create.

Create a configuration profile for operating system services:

● iOS configuration profile
○ Android configuration profile
○ Samsung KNOX configuration profile
○ Windows Phone configuration profile
○ iOS home screen layout configuration profile

Create a configuration profile for an application:

○ Configuration profile for LANrev Apps Configurat...

Read an existing configuration profile from file:

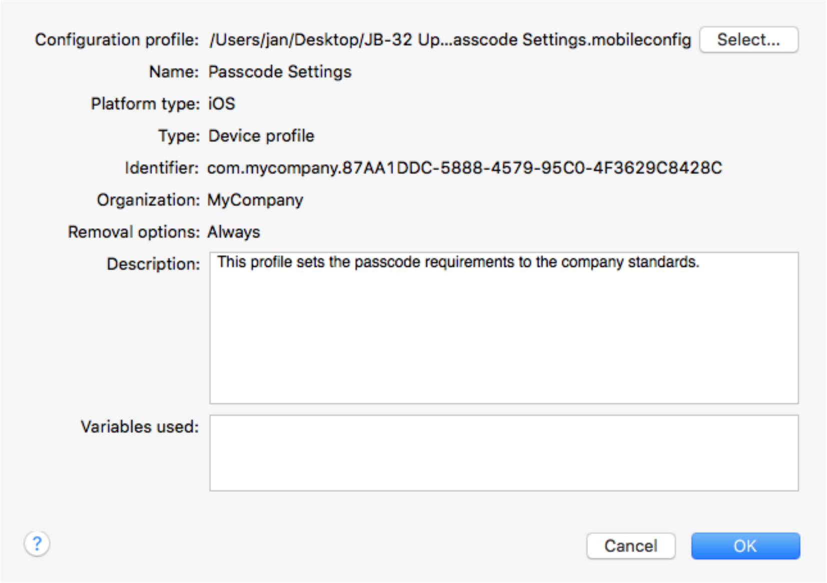
○ Load existing file and show in editor
○ Load existing file without editing

2. Choose **Load existing file without editing** and click **OK**.

   A standard file selection dialog opens.

3. Select the desired file and click **Open**.

   The **Configuration Profile** dialog opens:



Configuration profile: /Users/jan/Desktop/JB-32 Up...asscode Settings.mobileconfig
Name: Passcode Settings
Platform type: iOS
Type: Device profile
Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C
Organization: MyCompany
Removal options: Always
Description: This profile sets the passcode requirements to the company standards.
Variables used:

4. Click **OK**.

The profile is imported into LANrev and available for manual or profile-based installation on administered mobile devices.

Editing or exporting a configuration profile

You can edit an existing configuration profile or export it as a file to disk:

1. In the sidebar of the **Mobile Devices** window, select the desired profile.

   The details of the profile are displayed in the main part of the **Mobile Devices** window.

2. In the main part of the window, click the **Edit Profile Settings** button.

3. The Configuration Profile Editor opens and displays the contents of the profile.

4. To edit the profile, change the settings as desired.

5. To export the profile, click the **Save to Disk** button at the lower left of the editor window.

   Note that you can export the profile only if the profile was made exportable by checking the **Allow save to disk** option (see “Common settings” on page 667 for more information) or if you have superadministrator privileges.

Using variables in configuration profiles

LANrev supports the use of variables in configuration profiles for mobile devices. The variables are replaced by LANrev before the configuration profile is installed on the managed device.

The general handling of these variables is described in “Information variables” on page 175. The available variables are listed in “Variables for mobile devices” on page 458. (Note that you cannot use any of the variables that Apple defines for use with Apple Configurator.)

When LANrev applies a configuration profile to a mobile device, it automatically replaces the variable placeholder in the profile with the current value of the variable for that device. This results in two limitations:

- Configuration profiles containing variables must be applied with LANrev; other tools do not support the variables.
- Any changes to the content or definition of a variable after the configuration profile has been applied have no effect on the mobile device. For such changes to affect the device, the profile has to be reapplied after the change has been made.

Overview of installing configuration profiles on mobile devices

You can install a configuration profile either manually or via a policy. Using a policy also allows you to make configuration profiles available to managed mobile devices, but leave it up to the local user of the mobile device whether to install them. (This latter option is not supported for Windows Phone.)

LANrev works with both configuration profiles for devices (including the operating system) and for specific applications that support configuration through profiles.

NOTE Before you can install a profile, it must have been imported into or created in LANrev, as described in “Creating or importing configuration profiles” on page 182.

Details of installing configuration profiles are described in:

- **Manually installing a configuration profile** (page 186)
- **Manually removing a configuration profile** (page 189)
- **Installing a configuration profile via a policy** (page 189)
- **Making a configuration profile available for optional installation** (page 190)
- **Removing a configuration profile via a policy** (page 191)
- **Conflicting policy settings for configuration profiles** (page 192)

Manually installing a configuration profile

Manually installing configuration profiles is different for device configuration profiles and app-specific profiles.

In cases where an installation fails, you can retry it.

Device configuration profiles

To install a device configuration profile on mobile devices:

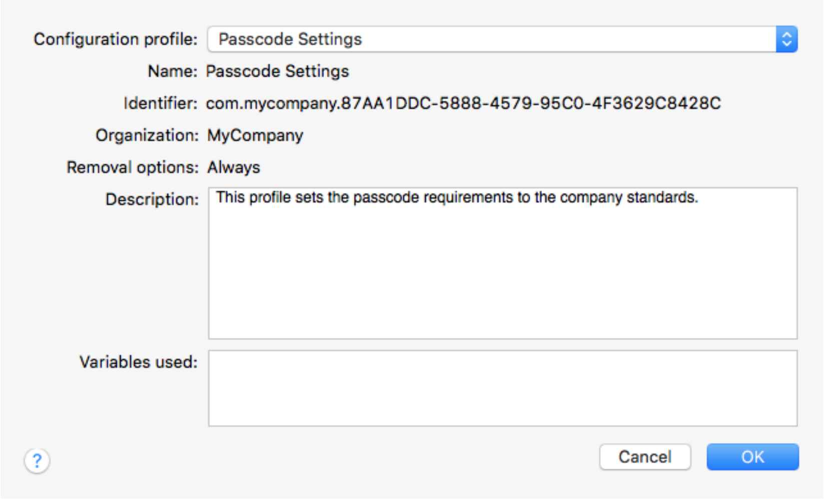
1. In the **Mobile Devices** window, select the devices on which you want to install the configuration profile.

   Make sure to select only devices with a common operating system; all profiles are specific to a particular operating system and cannot be installed on other operating systems.

2. Right-click the devices and choose **Install Configuration Profile** from the context menu.

   If you have selected shared devices, you can optionally press the Option key while choosing the command to install the profile only for the currently logged-in user of the device.

The **Install Configuration Profile** dialog opens:



Configuration profile: Passcode Settings

Name: Passcode Settings

Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C

Organization: MyCompany

Removal options: Always

Description: This profile sets the passcode requirements to the company standards.

Variables used:

3. From the **Configuration profile** pop-up menu, choose the desired profile.

   The menu contains all profiles that have been installed in LANrev, as described in “Creating or importing configuration profiles” on page 182. You can also use the **Other** command from the menu to open a configuration profile file from a volume on your computer.

4. Edit the description if desired.

5. Click **OK**.

The profile is sent to all selected mobile devices. It is installed on each selected device the next time it contacts the mobile OS vendor’s notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The results vary slightly depending on the type of device:

- iOS and Android devices: The profile is added to the profiles that are installed on the devices.
  All configuration profiles that are installed on an iOS or Android device are listed in the **Configuration Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.
- Windows Phone devices: The profile replaces the current profiles of the mailboxes with which the selected devices are synchronized.
  Because of the way Exchange ActiveSync works, this applies the profile also to all other devices that are synchronized to the same Exchange mailboxes. (If such other devices are iOS devices, the profile does not replace their current profiles but the profile’s settings may override those of any configuration profiles installed on the devices.)

The configuration profile that is currently in effect for a Windows Phone device is listed in the **ActiveSync Policy** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

App-specific configuration profiles

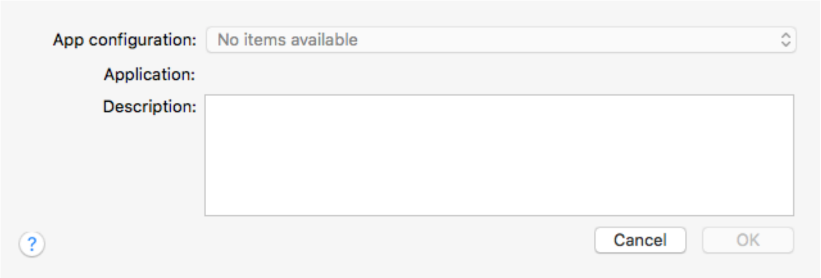
To install an app-specific device configuration profile on mobile devices:

1. In the **Mobile Devices** window, select the devices on which you want to install the configuration profile.

   App-specific configuration profiles can only be installed on devices running iOS 7.0 and up.

2. Choose **Commands** > **Change Application Configuration**.

   The **Change Application Configuration** dialog is displayed:



App configuration: No items available

Application:

Description:

3. Choose the desired profile from the pop-up menu.

   The application to which the selected profile applies and a description are displayed in the dialog.

4. Click **OK**.

The configuration profile is applied to all copies on the selected devices of the app to which it belongs. If a profile is already assigned to any of these apps, it is replaced by the selected profile.

Failed installations

If a configuration profile could not be installed on a device, for example, because it is not compatible with the device, an error message is generated.

In that case, you can fix all profiles with issues and then reapply them in one step using the **Retry All Failed Profiles** context menu command for the device.

Manually removing a configuration profile

To remove a configuration profile from a mobile device:

1. In the sidebar of the **Mobile Devices** window, expand the device from which you want to remove the configuration profile.

2. For iOS and Android devices, click the **Configuration Profiles** subgroup of the device; for Windows Phone devices, click the **ActiveSync Policy** subgroup.

   The configuration profiles that are present on the device are listed in the main part of the window.

3. Select the profile you want to remove and press the Backspace key.

   You can also right-click the profile and choose **Delete Profile** from the context menu.

The profile is removed from the device the next time it contacts the mobile OS vendors notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

For Windows Phone devices only, the removed profile is replaced with the settings of the default EAS policy specified on the Exchange server.

Installing a configuration profile via a policy

To install a configuration profile on mobile devices automatically:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items** > **Configuration Profiles** group to one of these subcategories of the **Configuration Profiles** category of the policy via which you want to distribute it:

   - **Auto-install**: The profiles are pushed to the device. They remain on a device even after it is removed from the policy. (After this point, users can remove the profiles manually, however.)
   - **Auto-install, auto-remove**: The profiles are pushed to the device. They are automatically removed from the device when it is removed from the policy.

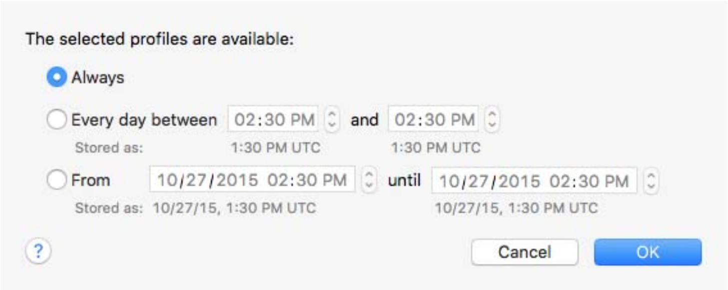
   Note that the actual effect may be different for devices that belong to other policies where the same configuration profile has a different role. See “Conflicting policy settings for configuration profiles” on page 192 for details.

2. If you do not want to restrict the time during which the profile is available, you are done. Only if you want to restrict it, continue.

3. Click the group into which you have put the profile inside the policy in the sidebar so that the configuration profiles contained in it are being displayed in the main part of the window.

4. Right-click the profile and choose **Set Availability Time** from the context menu.

   The **Set Availability Time** dialog is displayed:



The selected profiles are available:

● Always

○ Every day between 02:30 PM and 02:30 PM
Stored as: 1:30 PM UTC 1:30 PM UTC

○ From 10/27/2015 02:30 PM until 10/27/2015 02:30 PM
Stored as: 10/27/15, 1:30 PM UTC 10/27/15, 1:30 PM UTC

5. Specify when the profile should be available:

   - To make it available for a particular time each day, choose **Every day between** and enter the desired start and end times.
   - To make it available for a one-time period, choose **From** and specify the desired start and end times.

   For further information, see the description of this dialog in “Set Availability Time” on page 642.

The profile is sent to all devices that belong to the policy the next time each device contacts the mobile OS vendor’s notification server and is unlocked. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If devices are later added to the policy, they are treated the same way. (This may not be the case for devices also belonging to another policy in which the configuration profile is forbidden. See “Conflicting policy settings for configuration profiles” on page 192 for details.)

Profiles are installed on Windows Phone devices automatically, as described above, only if there are no other conflicting automatic profile assignment. If more than one auto-install profile is specified for a Windows Phone device (whether from one policy or from multiple policies), no profile is automatically installed.

Making a configuration profile available for optional installation

To make a profile available on an iOS or Android device but let the user decide whether to install it:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items** > **Configuration Profiles** group one of these subcategories of the **Configuration Profiles** category of the policy via which you want to distribute it:

  - **On-demand**: The profiles are made available for manual download in LANrev Apps at the users discretion. They remain on a device even after it is removed from the policy. Users can remove the profiles manually at any time.
  - **On-demand, auto-remove**: The profiles are made available for manual download in LANrev Apps at the users discretion. They are automatically removed from the device when it is removed from the policy.

2. If you do not want to restrict the time during which the profile is available, you are done. If you want to restrict it, specify the desired time as described beginning in step 3 of "Installing a configuration profile via a policy", above.

The profile is sent to all mobile devices that belong to the policy and is listed there in the **Profiles** section of LANrev Apps. (This may not be the case for devices also belonging to a different policy with conflicting settings. See "Conflicting policy settings for configuration profiles" on page 192 for details.) If LANrev Apps is not available on the device, nothing happens. (See "Preparing iOS devices for software installation" on page 195 for information on installing LANrev Apps.)

The profile is transferred to each device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If devices are later added to the policy, the profile is made available on them as well.

All configuration profiles that are installed on a device are listed in the subsections of the **Configuration Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Optional installation of profiles is not supported for Windows Phone devices.

Removing a configuration profile via a policy

To remove a configuration profile from mobile devices automatically:

1. In the **Mobile Devices** window, drag the profile from the **Assignable Items** > **Configuration Profiles** group to the **Forbidden Configuration Profiles** folder of the policy via which you want to remove it.

2. If you do not want to restrict the time during which the profile is forbidden, you are done. If you want to forbid it only during a certain time, specify the desired time as described beginning in step 3 of "Installing a configuration profile via a policy", above.

The next time a device that belongs to the policy contacts the mobile OS vendor's notification server and is unlocked, the profile is removed from that device. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

This may not be the case for devices also belonging to a different policy with conflicting settings. See "Conflicting policy settings for configuration profiles" on page 192 for details.

If devices are later added to the policy, the profile is removed from them as well (unless they also belong to a different policy which prevents this).

NOTE Profiles in the "Auto-install, auto-remove" or "On-demand, auto-remove" subcategories of the Configuration Profiles category of a policy are automatically removed from any device that is removed from the policy.

Conflicting policy settings for configuration profiles

It is possible to assign a configuration profile to multiple policies in different roles. For example, it could be auto-installed in one policy and forbidden in another, or on-demand in one policy and auto-installed and auto-removed in another.

This can become an issue if one device is a member of multiple policies and these policies contain the same configuration profile in different categories.

For example, a device could belong to one policy in which the profile is automatically installed and another in which it is forbidden. Clearly, there is no way to satisfy both policies' requirements at the same time.

In cases like this, LANrev uses this hierarchy for the different categories of profiles:

- Forbidden
- Auto-install
- On-demand
- Auto-remove

Higher entries have precedence over lower entries. For example, if a configuration profile is auto-installed in one policy to which a device belongs and forbidden in another, the profile is not available on the device because the "forbidden" category has a higher priority than "auto-install".

This means that, in some instances, an auto-installed and auto-removed profile remains on a device even when the device is removed from the policy in question. This is the case when the device also belongs to another policy in which the profile may be installed on-demand (and the device does not belong to a policy in which the profile is forbidden).

Windows Phone and multiple profiles

Because only one configuration profile (EAS policy) can be active on a Windows Phone device at any time, LANrev does not install a profile on any Windows Phone devices when the (LANrev) policy or policies to which it belongs specify more than one profile as automatically installed.

Installing provisioning profiles on iOS devices

You can install a provisioning profile manually on an iOS device. While provisioning profiles are normally automatically installed as part of an application, manually installing them may be necessary in special situations.

This is described in:

- **Manually installing a provisioning profile** (page 193)
- **Manually removing a provisioning profile** (page 194)

NOTE Android does not support provisioning profiles.

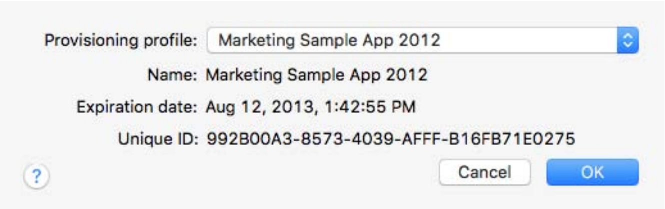
Manually installing a provisioning profile

To install a provisioning profile on iOS devices:

1. In the **Mobile Devices** window, select the devices on which you want to install the configuration profile.

2. Right-click the devices and choose **Install Provisioning Profile** from the context menu.

   The **Install Provisioning Profile** dialog opens:



Provisioning profile: Marketing Sample App 2012
Name: Marketing Sample App 2012
Expiration date: Aug 12, 2013, 1:42:55 PM
Unique ID: 992B00A3-8573-4039-AFFF-B16FB71E0275

3. From the **Provisioning profile** pop-up menu, choose the desired profile.

   The menu contains all profiles that are part of an application package.

   If the profile you want to install is not part of an application package, choose **Other** and select the provisioning profile file on your computer.

4. Click **OK**.

The profile is sent to all selected mobile devices. It is installed on each device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

All provisioning profiles that are installed on a device are listed in the **Provisioning Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Failed installations

If a configuration profile could not be installed on a device, for example, because it is not compatible with the device, an error message is generated.

In that case, you can fix all profiles with issues and then reapply them in one step using the **Retry All Failed Profiles** context menu command for the device.

Manually removing a provisioning profile

To remove a provisioning profile from an iOS device:

1. In the sidebar of the **Mobile Devices** window, expand the device from which you want to remove the provisioning profile.

2. Click the **Provisioning Profiles** subgroup of the device.

   The provisioning profiles that are present on the device are listed in the main part of the window.

3. Select the profile you want to remove and press the Backspace key.

   You can also right-click the profile and choose **Delete Profile** from the context menu.

The profile is removed from the mobile device the next time it contacts the mobile OS vendor's notification server and is unlocked. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Any applications that rely on this profile for authorization can no longer be used on the device after the next time the device (not the app) is restarted.

All provisioning profiles that are installed on a device are listed in the **Provisioning Profiles** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Preparing iOS devices for software installation

Due to the access restrictions for non-Apple software on iOS devices, installing software on such devices through a management system is both limited and requires preparation.

There are two fundamental requirements:

- Any enterprise software to be distributed through LANrev must be properly signed with a provisioning profile.
- Software distribution requires the LANrev Apps app to be installed on iOS 4.x devices, but not iOS 5 and later. However, LANrev Apps is required for many other functions of LANrev, so we strongly recommend that you always install it.

There are three basic ways to install LANrev Apps, either as a download from Apple's App Store or as signed enterprise software:

- Distributing LANrev Apps as an enterprise app is more work to set up but lets you distribute the app as an MDM-managed app, simplifying future updates. In addition, it does not put any requirements on your users.
  This process requires preparing and distributing LANrev Apps. Contact HEAT Professional Services for details.
- Installing LANrev Apps as an App Store download is easier but requires each user of a managed iOS device to have a valid Apple ID. Also, future updates need to be manually installed by the users, or they need to enable automatic updates in their device's settings.
  For details, see "Downloading LANrev Apps from the App Store", below.
- Users can download the apps directly from the App Store. This requires them to manually enter their credentials, as described in "Installing mobile apps" on page 56, and we do not recommend this approach.

NOTE For devices running iOS 4.x or 5.x, LANrev Apps 1.3 is required, which is available from the Resource Center.

NOTE The preparation described in this section is not required for Android or Windows Phone devices.

Downloading LANrev Apps from the App Store

1. Make sure that every user with a device on which you want to deploy LANrev Apps has an account with Apple's App Store.

   For devices running iOS 9 and up, an App Store account is not required if LANrev Apps is assigned to the devices (instead of the users of the devices).

2. Enroll all iOS devices to which you want to distribute the app in LANrev.

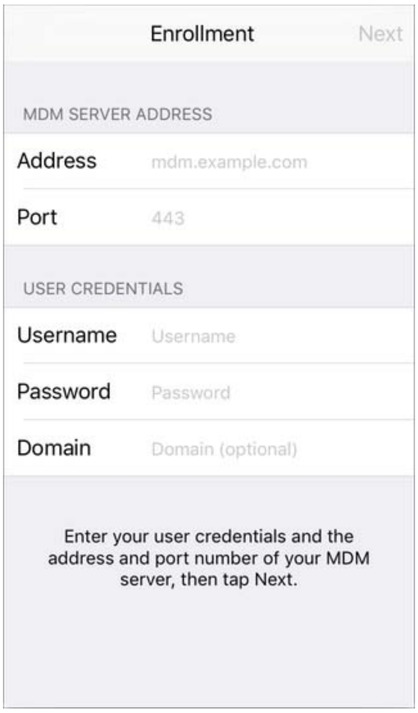
   This is described in "Enrolling mobile devices" on page 50.

3. Have all users download and install LANrev Apps from the App Store.

   This can be done either on the mobile device itself or on the computer from which the device is managed through iTunes. In the latter case, the device must be synced with iTunes so that LANrev Apps is transferred to the device.

4. Configure LANrev Apps with the internet address and port of your MDM server. There are three ways to do this:

   - When LANrev Apps is first launched, it presents a dialog in which the users can enter this information.



Enrollment

MDM SERVER ADDRESS

Address: mdm.example.com

Port: 443

USER CREDENTIALS

Username: Username

Password: Password

Domain: Domain (optional)

Enter your user credentials and the address and port number of your MDM server, then tap Next.

     When the user has entered the server address and port in this screen, LANrev Apps is configured. Skip the remaining steps of this procedure.
   - You can configure LANrev Apps via an app configuration profile. This is documented in the separate guide "Creating App Configuration Profiles".
   - You can provide this information via a configuration profile, as described below.

5. The **Mobile Devices** window's **Assignable Items** > **Configuration Profiles** section contains a profile named "Configure LANrev Apps". Install this profile on all iOS devices which have donwloaded LANrev Apps, as described in "Overview of installing configuration profiles on mobile devices" on page 186.

   You can install the profile either manually or via a policy. If you install it via a policy, it is removed automatically once LANrev Apps has been configured, ensuring that users do not continue to find the icon on their home screens although they already have configured the app.

   The installed configuration profile appears as an icon on the home screens of the iOS devices, like an app. Tapping this profile automatically configures LANrev Apps, even if the server settings screen is being displayed.

6. Communicate to the users (for example, by e-mail) that they should tap the configuration profile to configure LANrev Apps.

   Also communicate to the users that they must enable push notifications on their devices for LANrev Apps to work properly.

   If the users are running iOS 6, they must manually enter their Active Directory or Open Directory credentials and pick their device from a list during this process.

When users have performed these steps (installing and configuring the app and enabling push notifications), they have access to all apps you make available to their devices through LANrev. They can also receive messages you send to them from LANrev.

Installing software on mobile devices

You can distribute enterprise applications to managed iOS and Android devices. Depending on the operating system running on the mobile device, in most cases you can also distribute application files from an app store.

(The special case of installing OS updates is not described here; see "Updating mobile device operating systems" on page 205 for details.)

Distributing applications involves two steps:

1. Import the application file into LANrev as a mobile application package.

2. Then you can distribute that package to mobile users.

   You can either push-install apps to individual devices or make apps available for user-initiated installation in the LANrev Apps mobile application, which looks and works similar to Apple's App Store app.

All steps are described below in these sections:

- **Importing an application into LANrev** (page 198)
- **Making applications available on mobile devices** (page 200)
- **Uninstalling applications from mobile devices** (page 203)

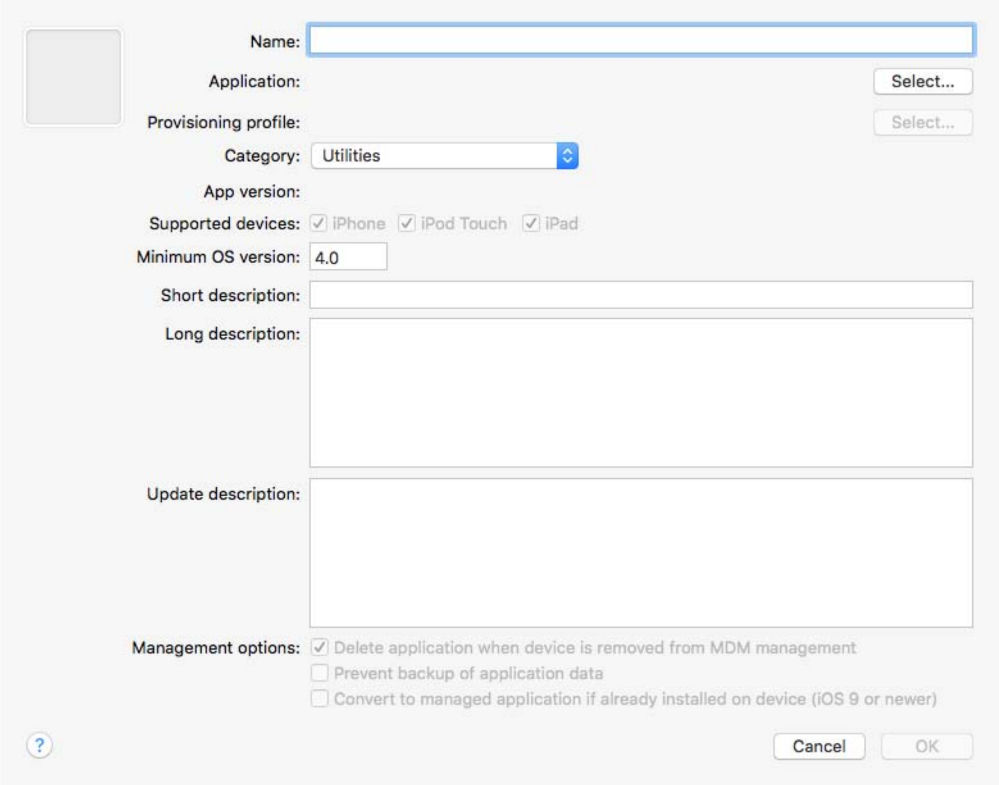
Importing an application into LANrev

Before you can distribute a mobile application through LANrev, you must import it.

To import a mobile application into LANrev:

1. In the **Mobile Devices** window, right-click the sidebar and choose **Mobile Applications** > **New Enterprise Application Package** from the context menu.

   The **Mobile Application** dialog opens:



Name:

Application:

Provisioning profile:

Category: Utilities

App version:

Supported devices: ☑ iPhone ☑ iPod Touch ☑ iPad

Minimum OS version: 4.0

Short description:

Long description:

Update description:

Management options: ☑ Delete application when device is removed from MDM management
□ Prevent backup of application data
□ Convert to managed application if already installed on device (iOS 9 or newer)

   The dialog is described in “New Enterprise Application Package” on page 553.

2. Click the upper **Select** button and choose the application file.

   This file must have the .ipa extension (for iOS apps) or .apk extension (for Android files), respectively.

   Note: Importing Android apps requires a Java runtime environment (JRE) to be installed on your computer.

3. If desired, edit the name for the application package.

This is the name under which the application package is listed in LANrev. It is automatically taken from the application file you have chosen, but you can modify it before saving the package.

4. If desired, add an icon to the application package or change the existing icon.

   You can paste any graphic into the field in the upper left. It will automatically be scaled to the required sizes.

5. You may need to specify an provisioning profile:

   - If you are importing an Android app or if you are importing an iOS app with an embedded provisioning profile – which is indicated by a disabled lower **Select** button – you do not need to specify a profile. Skip to the next step.
   - If you are importing an iOS app that does not include a provisioning profile, you must specify a profile.
     Click the lower **Select** button and choose the provisioning profile.

   The provisioning profile is required for the application to run. It must either be an ad-hoc profile that authorizes the application for a set of specific devices or an enterprise provisioning profile that authorizes the application for all iOS devices.

   The provisioning profile must be provided by the application's developer. It is often embedded in the app.

6. Choose the software category to which the application belongs from the **Category** list.

7. Fill in the short, long, and update descriptions as desired.

8. Set management options:

   - If you want the app to remain on managed devices only as long as those devices are under MDM management, check the **Delete application when device is removed from MDM management** option.
     If the option is unchecked, this app remains on devices on which it is installed, even when MDM management of the devices ends.
     This option is available only for iOS apps.
   - If you want the data of the application not to be copied in an iTunes or iCloud backup of the device, check the **Prevent backup of application data** option.
     If the option is unchecked, the data of the app is backed up normally.
     This option is available only for iOS apps.
   - If you want to start manage copies of this applications that are already installed on devices, check **Convert to managed application if already installed on device**.
     If this option is checked, any copy of this application that already exists on a managed device is converted to a

managed application whenever this application package is installed on the device.
This option affects only devices running iOS 9 and up.

9. Click **OK** to save the package.

The application package is saved in LANrev and can now be made available in the LANrev Apps mobile app as described in “Making applications available on mobile devices”, below.

NOTE Because making the app package available for installation on the server requires a significant amount of background processing over network connections, it may take a few minutes before the app is fully available, even if it is already displayed in the **Mobile Devices** window. Trying to install it before it is fully ready may result in error messages, for example, about missing checksums.

Making applications available on mobile devices

There are two ways to make apps available on managed iOS or Android devices, via policies or via direct installation. Both are described below.

Making apps available via policies

Once you have created an application package as described above, you can use it to make the application available on devices:

1. Drag the new application package from the **Assignable Items** > **Enterprise Applications** group to one of the subgroups (except **Forbidden**) of the **Enterprise Applications** group inside any mobile policy that contains the mobile devices on which you want to make the application available.

   The subgroups differ in how the application is installed and removed:

   - Auto-install: The app is installed when the device enters the policy. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
   - On-demand: The app can be installed manually by the user. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
   - Auto-install, Auto-remove: The app is installed when the device enters the policy and removed when it leaves.
   - On-demand, Auto-remove: The app can be installed manually by the user. It is removed from the device when it leaves the policy.

   Note: For information about on-demand installation on iOS devices, contact HEAT Support.

   On some mobile operating systems, the user may need to confirm the installation or the removal of apps.

   Silent installation (no user confirmation required) is supported on:

- Lenovo devices with Persistence
- Some Samsung Galaxy devices

Silent removal is supported on:

- iOS 5.0 or newer (only for apps installed via MDM)
- Lenovo devices with Persistence
- Some Samsung Galaxy devices

When you drag the application to the policy, a dialog opens in which you can set management options.

2. Set the desired options. (Depending on the type of application, not all options may be displayed.)

   - **App configuration**: The configuration profile you want to apply to the app you install. The pop-up menu lists all profiles that are available for the app (if any).
     This option is available only for iOS devices.
   - **Per-app VPN**: The VPN configuration profile that you want to assign to the app you install. The pop-up menu lists all per-app VPN configuration profiles that are available in LANrev (if any). Per-app VPN configuration profiles can be created with the configuration profile editor by choosing to create an iOS profile.
     This option is available only for iOS devices.
   - **Delete application when device is removed from MDM management**: If this option is checked, the application is removed from the device when the device is no longer under MDM management.
     This option is available only for iOS devices.
   - **Prevent backup of application data**: If this option is checked, the local data of the application on the device cannot be backed up to iTunes or iCloud.
     This option is available only for iOS devices.
   - **Convert to managed application if already installed on device**: If this option is checked, any unmanaged copy of the application that is already present on the device is converted into a managed application.
     This option is available only for devices running iOS 9 and up.
   - **Allow Automatic updates when installed as managed application**: Check this option if you want LANrev to automatically update the app when it is assigned to devices.
     This option only has an effect if (and while) auto-updating is enabled in the record for the app in LANrev. (For details, see “Application Info tab” on page 555.)
     The option applies only when the app is put into the “Auto-install” or “Auto-install, Auto-remove” group.
   - **Assign these volume licenses to**: You can choose whether to assign licenses from Apple’s volume licensing program to the devices in the policy or the users of the devices. If you choose to install to the device, you must

also choose the VPP account from which the license is to be taken.
This option is available only for devices running iOS 9 and up. It affects only applications that support the assignment of licenses to devices; licenses for all other applications are assigned to user regardless of your choice for this option.

- **Standard installation**: The application is installed in the usual location on the device.
  This option is available only for Android devices.
- **KNOX installation**: The application is installed in the KNOX workspace on the device.
  This option is available only for Android devices on which there is a KNOX workspace. The app will not be installed on devices that don't have a KNOX workspace.

The application is displayed in the list of applications inside LANrev Apps on (for apps installed on demand) or downloaded to (for automatically installed apps) any mobile device belonging to the policy as soon as the device next contacts the mobile OS vendor's push notification server. If it is online via WiFi or a mobile network, this happens quickly, usually within a minute, but if it is not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

You can send messages (see "Sending a message to mobile devices" on page 236) or e-mails to the users of the devices to notify them of the availability of the new application.

Making apps available via direct installation

For a more ad-hoc approach, you can distribute apps directly:

1. In the **Mobile Devices** window, select the mobile devices on which you want to install the app.

2. Choose **Commands** > **Install Application** from the context menu.

   The **Install Application** dialog is displayed.

3. From the **Application** pop-up menu, choose the app you want to install.

   You can choose apps that you have imported, enterprise apps as well as apps from the App Store or Google Play. For information on importing app store apps, see "Distributing App Store or Google Play apps to mobile users" on page 206.

4. If desired, assign an app-specific configuration profile.

   You can choose any profile that applies to the app and has previously been generated using the configuration profile generator. For more information, see "Working with configuration profiles" on page 181.

5. If desired, assign an app-specific VPN configuration to iOS apps.

   You can choose any profile that applies to the app and has previously been generated as an iOS configuration profile with the configuration profile generator. For more information, see “Creating a new configuration profile” on page 182.

6. Set the desired management options.

   You can choose a variety of settings related to MDM management. For more information, see “Install Application” on page 461.

7. If desired, edit the long description of the app.

8. Click **OK**.

The application is transferred to each selected device and the users are prompted to install it the next time the device contacts the mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

On iOS 4.x devices, the user is prompted to install the application only when LANrev Apps comes to the front the next time.

If a user declines the installation, the app is not installed on that device.

Note that you cannot install an application on an iOS device that already contains an unmanaged version of the application. (Unmanaged applications are all applications that have been installed by means other than through the MDM system.)

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window. Managed applications available for download are listed in the **Assignable Items** section.

Uninstalling applications from mobile devices

You can directly uninstall applications from devices, with the details varying according to the mobile operating system:

- On iOS 4 devices, direct uninstallation is not available. Instead, you have to remove the provisioning profile, as described below in “Uninstalling applications from iOS 4 devices”
- On iOS 5 and up, only managed applications can be removed, that is, applications that have been installed through the LANrev MDM system.
- On Android devices, any application can be removed, but the local user must confirm it. If the device supports persistence, no user confirmation is required.

To uninstall applications (other than from iOS 4 devices):

1. In the **Mobile Devices** window, display a list of installed applications.

   For example, display the **Applications** category of a managed device or the built-in **All installed applications** smart group.

2. Select the applications that you want to uninstall.

3. Right-click the selected applications and choose **Delete Application** from the context menu.

The next time a device on which one of the selected application is installed contacts the mobile OS vendor’s notification server and is unlocked, any selected application is removed from that device. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If the app has been running with a VPP device license, LANrev automatically removes that license from the device. (User licenses are not automatically removed, because the same user may use that app on other devices with the same license.)

On Android devices, a confirmation alert is displayed before the application is actually removed. If the user does not allow the removal, the application remains on the device.

Uninstalling applications from iOS 4 devices

It is not possible to remotely uninstall applications from devices running iOS 4.x. However, you can prevent an application from running on the device by deleting the provisioning profile.

Note, however, that due to the way iOS handles provisioning profiles, deleting a profile becomes effective only when the device (not the app!) is restarted. In other words, even when you delete the provisioning profile, that app continues to be fully functional until the next device restart.

To disable an application:

1. In the **Mobile Devices** window, drag the application that you want to disable from the **Assignable Items** > **Enterprise Applications** group to the **Enterprise Applications** > **Forbidden** group inside the iOS policy to which the iOS device belongs.

   If no such policy exists, you need to create one first, as described in “Working with policies”, below.

The next time a device that belongs to the policy contacts the mobile OS vendor’s notification server, the provisioning profile is removed from that device. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

After the next restart of the device, the application can no longer be used on that device.

Also, the application cannot be installed on any device belonging to the policy.

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Updating mobile device operating systems

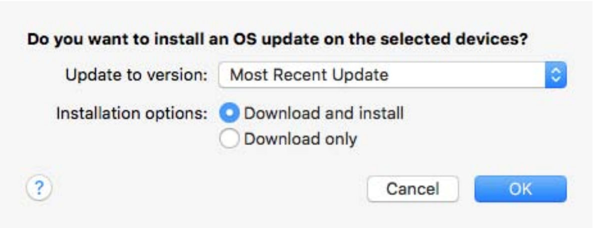
On devices that run iOS 9 and up, have been enrolled through Apple's device enrollment program, and also are supervised, you can remotely trigger operating system updates.

LANrev receives the list of available updates directly from Apple's servers; there is no need for you to specify the updates, nor can you configure their attributes. You can preview the updates that are available for a device and their properties using the information items from the **Available OS Updates** category.

To install an update:

1. Select the desired devices in any window listing mobile devices and choose **Commands** > **Install iOS Update**.

   The **Install iOS Update** dialog is displayed:



Do you want to install an OS update on the selected devices?

Update to version: Most Recent Update

Installation options: ● Download and install ○ Download only

2. From the pop-up menu, choose to update to the most recent version of iOS or to a specific older version. Set the desired installation options:

   - To have the device download and immediately install the update, choose **Download and install**.
     Note that some updaters give the user the option to postpone the update, but some do not. Also, some updaters require a device restart.
     If the updater is already on the device, it is installed immediately.

- To download the updater for installation at some later date, choose **Download only**.
  When the updater is on the device, either the user can install it manually through the Settings app, or you can install it remotely using this command and choosing the option **Download and install**.

Clicking **OK** sends the command to the devices, which download and, depending on the settings, install the updater.

Distributing App Store or Google Play apps to mobile users

You can push-install commercial apps to mobile users in a similar way to enterprise applications or make them available to users of managed devices to install on demand.

Push-installation works the same way as for enterprise applications, as described in “Making apps available via direct installation” on page 202.

For iOS apps only, if you have set up a volume purchasing agreement (VPP), you can let mobile users easily purchase apps through this program or assign managed licenses to them. See “Managing VPP app codes and licenses” on page 209 for details.

Creating app packages for app store apps

You can create app packages for App Store or Google Play apps that can then be distributed to mobile devices.

These app packages contain references to the apps, not the actual apps themselves, and appear in the App Store (for iOS apps) or Google Play (for Android apps) sections of LANrev Apps. Users can install these apps just like any other commercial app.

NOTE For VPP-licensed iOS apps, you can make LANrev automatically create app packages for any apps you license, by checking the **Automatically create packages for licensed apps** option in the VPP account settings. If you do so, you do not need to manually create those packages as described below.

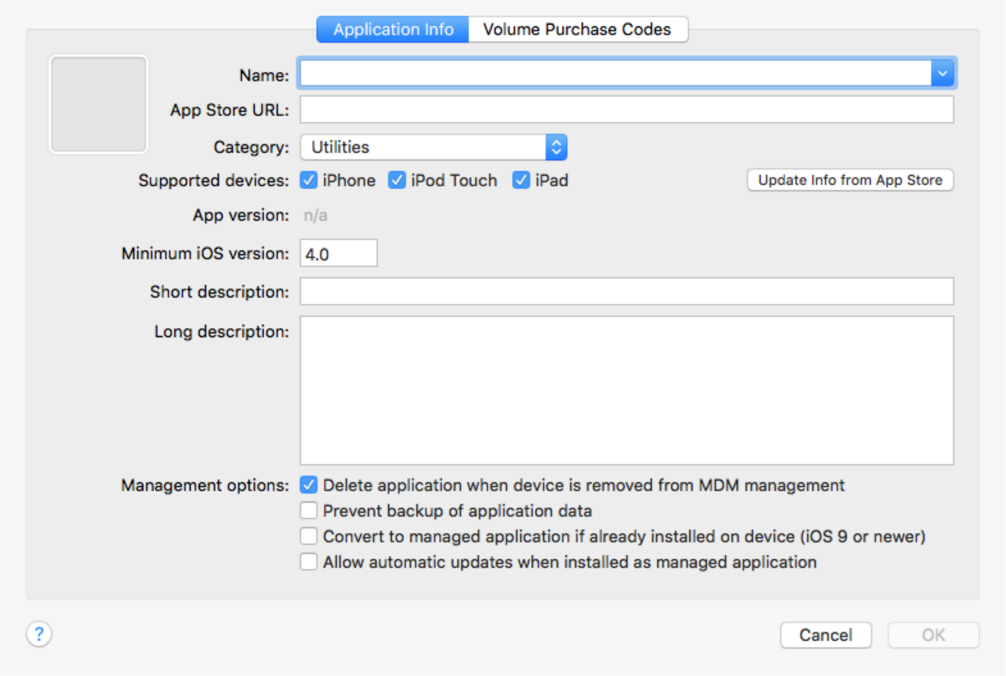
LANrev Apps must be installed on all mobile devices to which you want to distribute these app packages. See “Preparing iOS devices for software installation” on page 195 for information on distributing LANrev Apps to iOS devices and “Enrolling mobile devices” on page 50 for information on distributing it to Android devices.

To create and distribute recommended app packages:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Mobile Applications** > **New iOS App Store Application**

Package or **Mobile Applications** > **New Google Play Application Package**, depending on the target platform.

Depending on the command chosen, the **iOS App Store Application** dialog (shown below) or the **Google Play Application** dialog opens:



Name:

App Store URL:

Category: Utilities

Supported devices: ☑ iPhone ☑ iPod Touch ☑ iPad

App version: n/a

Minimum iOS version: 4.0

Short description:

Long description:

Management options:
☑ Delete application when device is removed from MDM management
□ Prevent backup of application data
□ Convert to managed application if already installed on device (iOS 9 or newer)
□ Allow automatic updates when installed as managed application

2. Specify the app you want to import. There are different ways to do this depending on the app store:

   - For Apple’s app store, you can start typing the name. After the first few characters, a list of matches will be displayed in a drop-down list. You can either continue typing or select the desired app in the list.
     Instead of using the name, you can also paste the URL of the app into the **Apple App Store URL** field and press the Tab key or click in another field.
   - For Google Play, paste the URL of the app into the **Google Play URL** field and press the Tab key or click in another field.

   You can obtain the URL by right-clicking the app’s icon anywhere in the respective online stores and choosing **Copy Link** from the context menu.

3. If you have volume purchase redemption codes for the app (iOS only), enter them as described in “Making volume purchase codes available” on page 209.

4. Fill in the short, long, and update descriptions as desired.

5. Set management options:

- If you want the app to remain on managed devices only as long as those devices are under MDM management, check the **Delete application when device is removed from MDM management** option.
  If the option is unchecked, this app remains on devices on which it is installed, even when MDM management of the devices ends.
  This option is available only for iOS apps.
- If you want the data of the application not to be copied in an iTunes or iCloud backup of the device, check the **Prevent backup of application data** option.
  If the option is unchecked, the data of the app is backed up normally.
  This option is available only for iOS apps.
- If you want to start manage copies of this applications that are already installed on devices, check **Convert to managed application if already installed on device**.
  If this option is checked, any copy of this application that already exists on a managed device is converted to a managed application whenever this application package is installed on the device.
  This option applies only to devices running iOS 9 and up.
- If you want the app to be automatically updated on the device, check **Allow Automatic updates when installed as managed application**.
  This option has an effect only for managed applications on devices running iOS 7 and up that are put in the policy's "Auto-install" or "Auto-install, Auto-remove" category. Also, automatic updates must be enabled in the app's record in LANrev. (For details, see "Application Info tab" on page 555.)

6. Click **OK** to close the dialog and save the new app package.

7. The new app package appears in the **Assignable Items** > **App Store Applications** group in the **Mobile Devices** window.

8. Drag the app package to the **App Store Applications** > **On-demand** group of a policy containing the devices to which you want to recommend the app.

   Policies are described in "Working with policies" on page 245.

The next time a device that belongs to that policy contacts the mobile OS vendor's notification server, the app package information is sent to that device. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The package appears on the device in the **App Store** section or **Google Play** section, respectively, of LANrev Apps.

Users can install the app by clicking the **Install** button; if they do so, the app is downloaded from the App Store or Google Play normally. If you have a VPP account with available licenses for the app and the user is assigned to that account, the VPP license is used.

All applications that are installed on a device are listed in the **Applications** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window. Recommended applications are listed in the **Assignable Items** section.

Managing VPP app codes and licenses

Apple’s App Store volume purchase program (VPP) lets you purchase (depending on the version of the program) either codes that can be redeemed by users or blocks of licenses that enable users to download the corresponding iOS apps.

The two VPP types, one using redemption codes and one using licenses, are managed in different ways. This is described in:

- **Making volume purchase codes available** (page 209)
- **Setting up VPP license management** (page 211)
- **Assigning and revoking VPP app licenses** (page 217)
- **VPP license statistics** (page 220)

Making volume purchase codes available

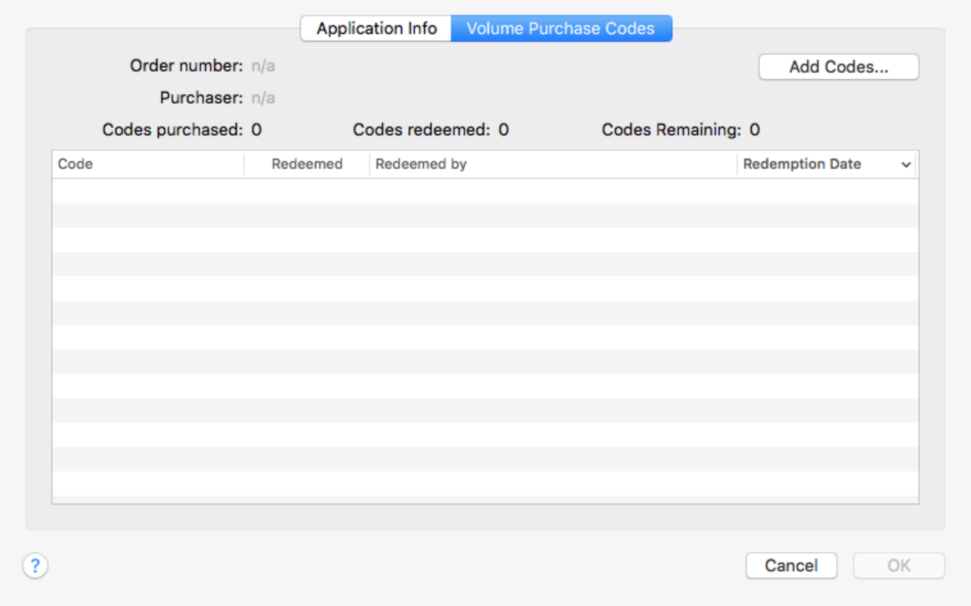
Apple’s App Store offers a volume purchasing program for apps. If you purchase a block of apps through this program, you receive a list of redemption codes and links.

You can import such code lists into LANrev and allow users of mobile devices to purchase apps through the volume purchasing program without needing to assign them codes individually.

To make volume-purchased apps available to users:

1. Create an app package for the App Store app, as described in “Distributing App Store or Google Play apps to mobile users”, above, until you reach step 3.

2. Click the **Volume Purchase Codes** tab to display the corresponding pane:



Order number: n/a

Purchaser: n/a

Codes purchased: 0 Codes redeemed: 0 Codes Remaining: 0

Code	Redeemed	Redeemed by	Redemption Date

3. Import the codes in one of these ways:

   - Copy and paste:
     - Open the Excel file with the codes that you have received from Apple.
     - Copy the entire contents or just the rows containing the codes and redemption links.
     - Switch to LANrev Admin and click inside the table area.
     - Paste the copied codes.
   - Exported text file:
     - Open the Excel file with the codes that you have received from Apple.
     - Save the file as a tab-delimited text file.
     - Switch to LANrev Admin and click the **Import Codes** button.
       A standard system Open dialog is displayed.
     - Select the exported text file and click **Open**.

   - Manually created text file:
     - Create a text file in which each line contains a redemption code, a tab character, and the corresponding redemption link.
     - Save the file as a tab-delimited text file.
     - Switch to LANrev Admin and click the **Import Codes** button.
       A standard system Open dialog is displayed.
     - Select the text file and click **Open**.

The codes are added to the table in the dialog.

4. Continue the procedure described in “Distributing App Store or Google Play apps to mobile users” with step 6.

All mobile devices to which the package is made available (via the policies to which you assign it) can now purchase the app using the redemption codes.

To redeem a code, the user simply clicks **Install** in LANrev Apps. LANrev automatically and transparently transmits an unused redemption code and the corresponding link to the App Store. The user of the mobile device does not notice any of this. The used code is automatically marked as redeemed and will not be assigned to another device.

Deleting codes

You can delete redeemed codes – in particular codes that have been redeemed outside of LANrev and thus are still considered available there:

1. In the **Mobile Devices** window, double-click the App Store app package into which the codes have been imported.

2. Click the **Volume Purchase Codes** tab.

3. In the table, select the codes that you want to delete.

4. Press the Backspace key.

5. Click **OK** to save the changes and close the dialog.

The codes are removed from the package and are no longer available for redemption inside LANrev.

Setting up VPP license management

To set up MDM support for Apple’s VPP, you must enter your VPP account credentials in LANrev and register all users that you want to be able to use licenses from the program:

- **Entering VPP account information** (page 212)
- **Registering users** (page 214)

This setup procedure applies only to managed licenses. For information on handling redemption codes purchased through the VPP, see “Making volume purchase codes available” on page 209.

A particular VPP account can be set up in any number of MDM tools. For example, the account could be configured on different independent copies of LANrev Server or in other tools capable of VPP management.

An account can be managed by only one tool at a time, which “owns” the account. If you perform VPP-related operations in LANrev and the affected account is currently managed by a different tool, LANrev will inform you of the fact and offer to take over the account.

If you decide to take over an account, your choices are:

- Simply take over the unmodified account. This is quick but may leave any licenses inaccessible that were assigned to devices in other tools (because LANrev does not know about these assignments).
- Reset the account before taking over. This revokes all assigned licenses, ensuring that they are available after the takeover. This is the safer way but can take several hours for large accounts. Also, you will need to reassign all licenses to the managed devices.

Note that although the function to take over a VPP account from another tool exists, we recommend that you configure your VPP management to avoid the necessity of such takeovers as much as possible.

Entering VPP account information

You can enter information on one or more VPP accounts. If you have multiple accounts, users will only be able to access accounts for which you have explicitly registered them.

To enter VPP account information:

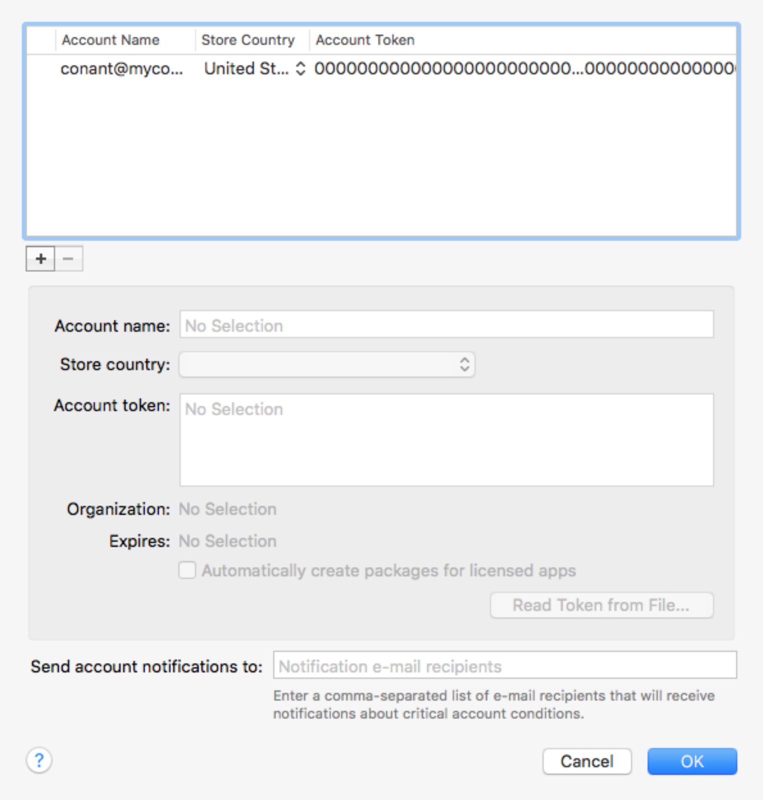
1. In the **Server Center** window, click **Server** > **Server Settings** to display the server configuration dialog.

2. Click the **MDM** tab.

   The MDM settings are displayed.

3. Click the **Configure** button in the **Apple VPP licensing account** section in the lower right.

The **Apple VPP Licensing Accounts** dialog opens:



Account Name	Store Country	Account Token
conant@myco...	United St... ◇	000000000000000000000000...0000000000000

Account name: No Selection

Store country:

Account token: No Selection

Organization: No Selection

Expires: No Selection

□ Automatically create packages for licensed apps

Send account notifications to: Notification e-mail recipients

Enter a comma-separated list of e-mail recipients that will receive notifications about critical account conditions.

Note that this button is available only to administrators with the **Modify VPP License Management** privilege.

4. To add an account, click the **+** button and enter the account information in the lower part of the window.

   You can read a token file from disk by clicking the **Read Token from File** button.

   Repeat this step until you have added all desired accounts. You can add additional accounts at any time.

5. To edit the details of an account, select it in the list and edit the fields in the lower half of the window.

6. To delete an account, select it in the list and click the **–** button.

   If an account is deleted, any licenses from the account that are assigned to users stay assigned, but no new assignments of account licenses through the MDM system can be made.

   You cannot undo the deletion of an account, but you can create a new account using the same token after the deletion is completed.

7. If you want to notify persons when there are issues with the VPP accounts, enter their e-mail addresses, separated by commas, in the **Send account notifications to** field.

8. When you have set up all accounts as desired, click **OK**.

You can now register MDM users with any of the accounts you have set up, as described below.

Registering users

Users can install an app store app with a VPP license when you register them for an account that contains a suitable license. Users can be registered manually, as described below, or automatically using an action, as described in "Working with actions" on page 232.

To register a user manually:

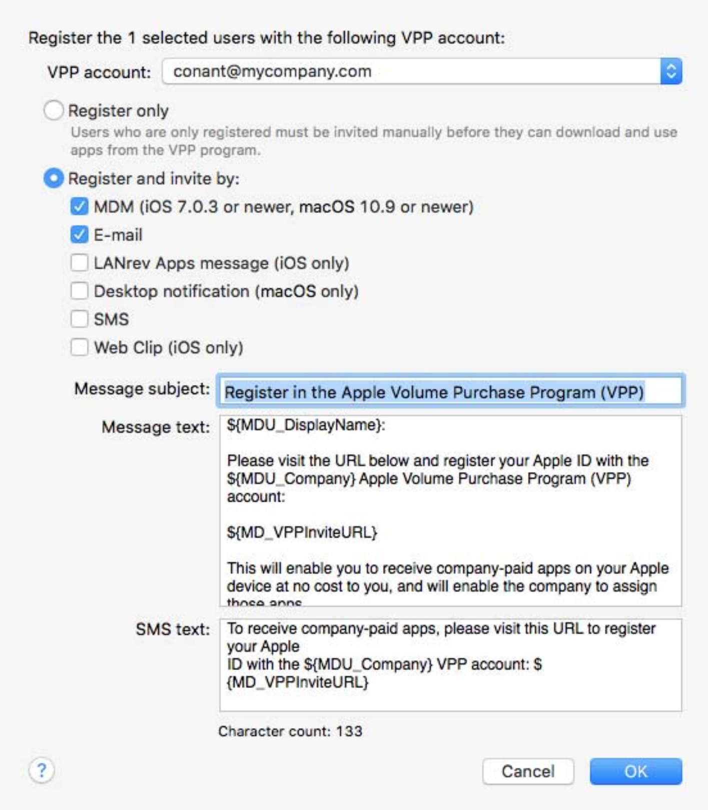
1. Make sure that all users you want to register have a personal Apple ID. The Apple IDs are required to complete the registration process.

2. In the **Mobile Devices** window, click any group of users in the sidebar that contains the desired user accounts.

   The users from that group are listed in the main part of the window.

3. Select all users that you want to assign to the same VPP account, right-click, and choose **Register Device User in VPP** from the context menu.

The **Register Users in VPP** dialog opens:



Register the 1 selected users with the following VPP account:

VPP account: conant@mycompany.com

○ Register only

Users who are only registered must be invited manually before they can download and use apps from the VPP program.

● Register and invite by:

☑ MDM (iOS 7.0.3 or newer, macOS 10.9 or newer)

☑ E-mail

□ LANrev Apps message (iOS only)

□ Desktop notification (macOS only)

□ SMS

□ Web Clip (iOS only)

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text: ${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

${MD_VPPInviteURL}

This will enable you to receive company-paid apps on your Apple device at no cost to you, and will enable the company to assign those apps

SMS text: To receive company-paid apps, please visit this URL to register your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}

Character count: 133

4. From the **VPP account** list, choose the account for which you want to register the users.

   To complete the process, the users need to access a URL on Apple’s servers to link their Apple ID with the VPP account. This URL is sent to them via an invitation.

   You can send the invitation as part of the registration or later as a separate step. Sending the invitation separately eases the load on Apple’s back-end servers and may improve performance for the registration process.

5. If you want to send the invitation separately later, choose **Register only** and click **OK**. You are now done with this procedure; at a later time, perform the steps described in “Sending an invitation to users”, below.

   If you want to send the invitation now, choose **Register and invite by** and continue below.

6. Specify the ways invitations are sent to the users by checking the appropriate options.

   If you want to invite users via a web clip, the predefined configuration profile “VPP Invite Web Clip” is sent to them. You can change the label and icon of this web clip by editing the profile. Note that you must not change the URL of the clip.

7. If desired, edit the message text.

   You can use a number of variables in the text, as described in "Register Device User in VPP" on page 618. Note that the users will need to visit an Apple web page to complete the process, so you should always include the `${MD_VPPInviteURL}` variable that resolves to this page's URL.

8. Click **OK** to close the dialog and send the registration messages.

9. If you want to register users for additional VPP accounts, repeat this procedure.

Once users have visited Apple's registration page and entered their Apple ID their, you can assign licenses to them from any account for which you have registered them.

Sending an invitation to users

You can register users and send invitations to them in one step or in two separate steps. Using two separate steps eases the load on Apple's back-end servers and may improve performance.

To invite users that you have already registered:

1. Make sure that all users you want to invite have already been registered as described in "Registering users", above.

2. In the **Mobile Devices** window, click any group of users in the sidebar that contains the desired user accounts.

   The users from that group are listed in the main part of the window.

3. Select all users that you want to assign to the same VPP account, right-click, and choose **Send VPP Invitation** from the context menu.

4. From the **VPP account** list, choose the account for which you want to register the users.

5. Specify the ways invitations are sent to the users by checking the appropriate options.

   If you want to invite users via a web clip, the predefined configuration profile "VPP Invite Web Clip" is sent to them. You can change the label and icon of this web clip by editing the profile. Note that you must not change the URL of the clip.

6. If desired, edit the message text.

   You can use a number of variables in the text, as described in "Send VPP Invitation" on page 619. Note that the users will need to visit an Apple web page to complete the process, so you should always include the `${MD_VPPInviteURL}` variable that resolves to this page's URL.

7. Click **OK** to close the dialog and send the invitation messages.

8. If you want to invite users to additional VPP accounts, repeat this procedure.

Once users have visited Apple's registration page and entered their Apple ID their, you can assign licenses to them from any account for which you have registered them.

Assigning and revoking VPP app licenses

Licenses for apps can be assigned to users or devices and removed again when users, devices, or apps are listed in the **Mobile Devices** window.

Any assignment requires that the VPP is properly set up, as described in "Setting up VPP license management" on page 211. In particular, the users in question must have been registered with the program and they must have specified their Apple ID.

Assigning VPP app licenses

You can assign app licenses when selecting users, devices, or apps.

Assigning a license when users or devices are selected:

1. In the main part of the **Mobile Devices** window, right-click one or more users or devices and choose **VPP Licensing** > **Assign Application Licenses to Device Users** or **Assign Application Licenses to Devices**.

   These commands let you assign the license to the user account or the device, respectively. Not all VPP-licensed applications support assigning to devices. Licenses can only be assigned to devices running iOS 9 and up.

   The **Assign Application Licenses to Users** or the **Assign Application Licenses to Devices** dialog opens.

2. In the **Assign Application Licenses to Devices** dialog, choose the desired VPP account from the pop-up menu. (In the **Assign Application Licenses to Users** dialog, skip this step.)

3. Check all listed apps that you want to assign to the selected users or users of the selected devices, or to the selected devices, respectively.

   To filter the list, you can enter part of the name of the desired app in the search field at the upper right of the dialog.

4. Click **OK**.

Licenses for the marked apps are assigned to the users or devices. If an app is assigned to users, it is added to the users' lists of purchased items in the iTunes store.

Any devices of these users that have been set up in their local settings to automatically download apps purchased on other devices will download the assigned apps. On other devices, users will have to download the apps manually.

Assigning a license when apps are selected:

1. Make sure that you have created app packages for all apps that you want to assign.

   Creating packages is described in "Distributing App Store or Google Play apps to mobile users" on page 206. When setting up a package, make sure to use the same app store URL as you have used when purchasing the license.

2. In the main part of the **Mobile Devices** window, right-click one or more app store apps and choose **VPP Licensing** > **Assign Application Licenses to Users** or **Assign Application Licenses to Devices**.

   The **Assign VPP Licenses** or the **Assign Application Licenses to Devices** dialog opens, with the selected apps listed in the upper half.

3. In the lower half of the dialog, check all users or devices to whom you want to assign the listed apps.

   To filter the list, you can enter part of the name of the user or device you are looking for in the search field at the right of the dialog.

4. Click **OK**.

Licenses for the selected apps are assigned to the marked users. The apps are added to the users' lists of purchased items in the iTunes store.

Any devices of these users that have been set up in their local settings to automatically download apps purchased on other devices will download the assigned apps. On other devices, users will have to download the apps manually.

Reassigning licenses from users to their devices

Some applications allow their licenses to be assigned to users or devices. If such licenses are assigned to users, you can reassign them to the users' devices instead:

1. In the **Mobile Devices** window, select the users whose licenses you want to reassign, right-click, and choose **Convert Application Licenses from Users to Devices** from the context menu.

You can also select devices and choose **VPP Licensing** > **Convert Application Licenses from Users to Devices** from the context menu.

In both cases, the license conversion assistant opens.

2. Follow the instructions in the assistant to select the licenses, users, and devices for the conversion.

   The elements of the assistant are described in **Convert Application Licenses from Users to Devices**.

Revoking VPP app licenses

As with assigning licenses, you can revoke app licenses when selecting users, devices, or apps. (Note that LANrev automatically removes device-assigned licenses are automatically removed when the app is deleted from the device through LANrev Admin, as described in "Uninstalling applications from mobile devices" on page 203.)

The licenses for some apps may be declared irrevocable by Apple. Such licenses cannot be revoked (whether in LANrev or otherwise) once they have been assigned; the procedures below do not apply to these licenses.

Revoking a license when users or devices are selected:

1. In the main part of the **Mobile Devices** window, right-click one or more users or devices and choose **VPP Licensing** > **Revoke Application Licenses**.

   The **Revoke Application Licenses** dialog opens. It lists all apps with licenses that are assigned to at least one of the selected users.

2. At the top of the dialog, choose from the pop-up menu whether you want to revoke licenses assigned to users, licenses assigned to devices, or both.

   If you choose to revoke only user-assigned licenses or only device-assigned licenses, the other kind of license remains unaffected by this command.

3. Check all listed apps for which you want to revoke the license from the selected users or devices.

   To filter the list, you can enter part of the name of the desired app in the search field at the upper right of the dialog.

4. Click **OK**.

Licenses for the marked apps are revoked from the selected users or devices. The apps remain on the user's device but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

Revoking a license when apps are selected:

1. In the main part of the **Mobile Devices** window, right-click one or more app store apps and choose **VPP Licensing** > **Revoke Application Licenses**.

   The **Revoke Application Licenses** dialog opens.

2. At the top of the dialog, choose from the pop-up menu whether you want to revoke licenses assigned to users, licenses assigned to devices, or both.

   If you choose to revoke only user-assigned licenses or only device-assigned licenses, the other kind of license remains unaffected by this command.

3. Check all users or devices from which you want to revoke the licenses for the listed apps.

   To filter the list, you can enter part of the name of the user or device you are looking for in the search field at the right of the dialog.

4. Click **OK**.

Licenses for the selected apps are revoked from the marked users. The apps remain on the users' devices but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

VPP license statistics

LANrev offers to way to monitor the number of VPP licenses available for an app or a book.

Individual apps and books

To view the licenses for an individual app or book:

1. Click the desired app or book in the sidebar of the **Mobile Devices** window.

   The detail view for the item is displayed.

2. Click the **Volume Licenses** tab.

   The number of purchased, assigned, and available licenses is displayed in the upper part of the tab.

   Note that the **Volume Licenses** tab is not available for Android apps, as these cannot be part of the VPP.

Monitoring licenses in tables

To view the licenses for multiple apps or books in a table:

1. Display a table containing mobile App Store apps or iBooks Store books.

   This can either be an appropriate section of the **Mobile Devices** window or a browser window displaying the desired kind of information.

2. Add one or more of the relevant information items to the table, depending on what you want to monitor.

   - For apps:
     - App Store VPP Licenses Purchased
     - App Store VPP Licenses Assigned
     - App Store VPP Licenses Remaining
   - For books:
     - Book VPP Licenses Purchased
     - Book VPP Licenses Assigned
     - Book VPP Licenses Remaining

Distributing media to mobile devices

You can import media files into LANrev and make them available to managed iOS and Android devices through the LANrev Safe app.

NOTE LANrev Safe can also provide access to media files stored on SharePoint servers. See “Providing access to media stored on SharePoint servers” on page 228 for details.

Media files are distributed through profiles, allowing you fine-grained control over who will and will not have access to a particular file. Furthermore, you can optionally prevent media files from being taken out of LANrev Safe.

The files are stored in encrypted form on the device and are not part of any backups of the mobile device to PC (for example, in iTunes).

To distribute media files, you first import them into LANrev and then assign them to any policies through which you want to distribute them. The details of this are described in:

- **Importing a media file** (page 223)
- **Distributing a media file** (page 225)
- **Manually installing media files** (page 227)
- **Providing access to media stored on SharePoint servers** (page 228)

Distributing media files to Windows Phone devices is not supported.

Supported media types

You can distribute all kinds of media (that is, any file from your computer) to managed mobile devices. LANrev Safe provides support for viewing a number of popular document, image, video and sound formats right within the app; other media types can be opened in other apps, provided they are available on the mobile device and that you have allowed the media file to leave LANrev Safe (see "Importing a media file", below).

These types of media can be displayed within LANrev Safe:

- Web formats
  - HTML (.htm, .html)
  - XML (.xml)
  - XSL (.xsl)
  - Safari web archive (.webarchive); iOS only
- PDF (.pdf)
- Text
  - Pages (.pages); iOS only
  - RTF (.rtf)
  - RTF directory (.rtfd); iOS only
  - Unformatted text (.txt)
  - Word (.doc, .docx)*; iOS only
- Presentations
  - Keynote (.key); iOS only
  - PowerPoint (.ppt, .pptx)*; iOS only
- Spreadsheets
  - Excel (.xls, .xslx)*; iOS only
  - Numbers (.numbers); iOS only
- Images
  - BMP (.bmp)
  - GIF (.gif)
  - JPEG (.jpg, .jpeg)
  - PNG (.png)
  - TIFF (.tif, .tiff); iOS only
  - WebP (.webp); Android only
- Audio**
  - AAC audio (.m4a, .3gp)
  - AAC audio books (.m4b, .m4p); iOS only
  - AIFF (.aiff, .aif, .aifc, .cdda); iOS only
  - AMR (.amr, .3gp)
  - FLAC (.flac); Android only
  - MIDI (.imy, .mid, .xmf, .mxmf, .ota, .rtttl, .rtx); Android only
  - MP3 (.mp3, .swa)
  - MPEG audio (.mpeg, .mpg, .mp3, .swa)
  - Vorbis (.ogg, .mkv); Android only
  - WAVE (.wav, .bwf)
- Video and multimedia**
  - 3GP (.3gp, .3gpp)
  - 3GP2 (.3g2, .3gp2)
  - AVI (.avi)
  - MPEG-4 (.mp4, .m4v)
  - QuickTime (.mov, .qt, .mqv); iOS only
  - VP8 (.webm, .mkv); Android only

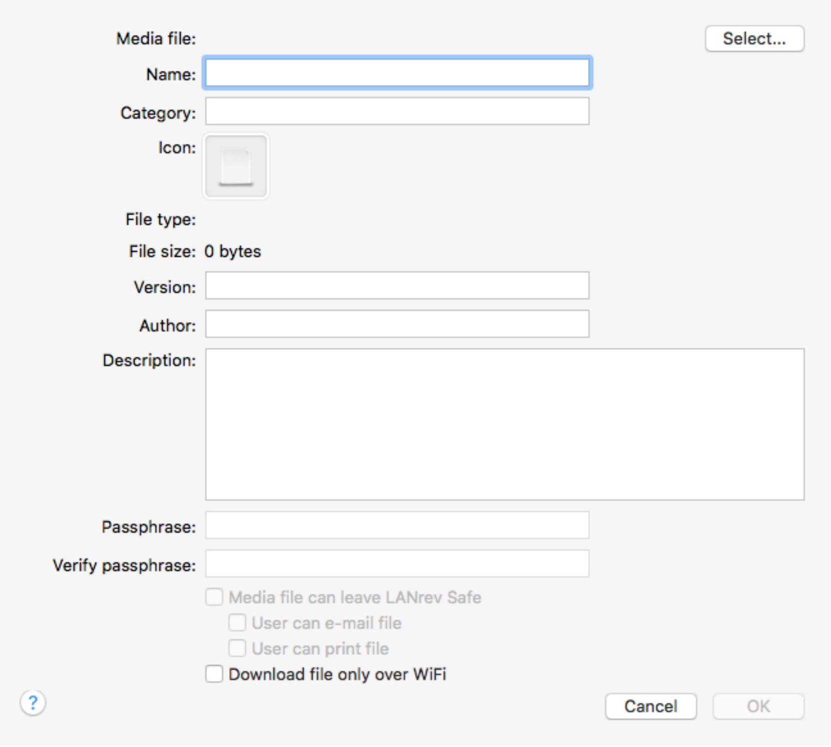
* Microsoft Office files in Office 95 or older formats are not supported.
** The support for audio and video formats depends on the container and codec formats of the device on which LANrev Safe is installed. Some files may therefore not be playable within LANrev Safe, even though the container and codec are in principle supported and listed as such above. On some devices, LANrev Safe may be able to play additional formats not listed above.

Importing a media file

To be able to assign a media file to a policy and thereby distribute it to managed mobile devices, you first import it into LANrev:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Media** > **New Media File**.

   The **Mobile Media File** dialog is displayed.



Media file:
Name:
Category:
Icon:
File type:
File size: 0 bytes
Version:
Author:
Description:
Passphrase:
Verify passphrase:
□ Media file can leave LANrev Safe
□ User can e-mail file
□ User can print file
□ Download file only over WiFi

2. Click **Select** and choose the desired file or drag the file from the desktop into the **Media file** area.

   The **Name**, **Category**, and **Icon** fields are automatically filled based on the file you selected.

   You can also select entire folders of media files to batch-import them. If you do, some special considerations apply, as described in “Importing folders of media files”, below.

3. Edit the **Name** and **Category** fields if desired. You can also paste a graphic into the **Icon** field that is displayed as the media file’s icon on the mobile devices.

4. Enter a description in the **Description** field.

   This description will be displayed to mobile users and should give them some indication of the relevance of the file.

5. If desired, set a password for the media file by entering it in the **Passphrase** and **Verify passphrase** fields.

   The passphrase must be entered every time the file is displayed in LANrev Safe.

   If you set a passphrase, you cannot allow the media file to leave LANrev Safe. Therefore, you can set a passphrase only for file types that are supported by LANrev Safe. (See "Supported media types" on page 222 for a list of supported file types.)

   You cannot set a passphrase when **Media file can leave LANrev Safe** is enabled.

6. If you want the mobile users to be able to view or edit the media file in apps other than LANrev Safe, check **Media file can leave LANrev Safe**.

   This allows users, for example, to view the file in a PDF reader, edit in a text editor, or forward it to others by e-mail.

   If desired, you can also check **User can e-mail file** and/or **User can print file** to provide buttons with LANrev Safe for these two tasks.

   You cannot check **Media file can leave LANrev Safe** if you have set a password for the file, as described in step 5.

   Note: While unchecking this option reliably prevents the file from leaving LANrev Safe, the same is not necessarily true for the information contained in the file. For example, a mobile user still could take screenshots of the file and send those to other persons.

7. If the file is large, you may want to check **Download file only over WiFi** so that the user does not have to suffer long downloads or high data charges because the file was downloaded over a mobile data connection, such as 3G (UMTS) or LTE.

   This setting requires LANrev Safe 1.1 or newer. Earlier versions of LANrev Safe ignore it.

8. Click **OK**.

The new media file is added to the **Assignable Items** > **Media** section of the sidebar and can now be assigned to policies.

Importing folders of media files

Instead of importing individual files, you can import entire folders in one step. The process is the same as described above, with a few changes:

- The names under which the media files are stored in LANrev (the content of the **Name** field) cannot be set individually. Instead LANrev uses the file names, without the file name extensions.
- You can specify a category. If you do, it applies to all files contained in the folder. If you do not specify a category, LANrev automatically assigns a category to each file depending on its file type.
- If you select a folder to import, the displayed file type is always "Batch upload" and no file size is shown.
- Any description and passphrase you specify applies to all files contained in the folder.
- The **Media file can leave LANrev Safe** setting you specify applies to all files contained in the selected folder that LANrev Safe can display (see "Supported media types" on page 222 for details). Files that LANrev Safe cannot display itself are always allowed to leave LANrev Safe (irrespective of the setting you specify) because it would otherwise be impossible for mobile users to view these files.

Distributing a media file

Once you have imported a media file as described in above, you can distribute it to mobile devices via assigning it to a policy:

1. Drag the media file from the **Assignable Items** > **Media** group to the appropriate group and subgroup of the mobile policy that contains the mobile devices on which you want to make the file available:

    - To install the file in LANrev Safe, drag it to one of the subgroups of the **LANrev Safe Media** group.
    - To install the file in iBooks, drag it to one of the subgroups of the **iBooks Media** group.
      This option is available only for PDF, ePub and iBook books, and files in this group will only be installed on iOS devices running iOS 8 or above.

    The subgroups of these groups differ in how the media file is installed and removed:

    - Auto-install: The media file is downloaded when the device enters the policy. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
    - On-demand: The media file can be downloaded manually by the user. It remains on the device when it leaves the policy and can be deleted manually by the user, if desired.
    - On-demand, auto-remove: The media file can be downloaded manually by the user. It is removed from the device when it leaves the policy.
    - Auto-install, auto-remove: The media file is downloaded when the device enters the policy and removed when it leaves.

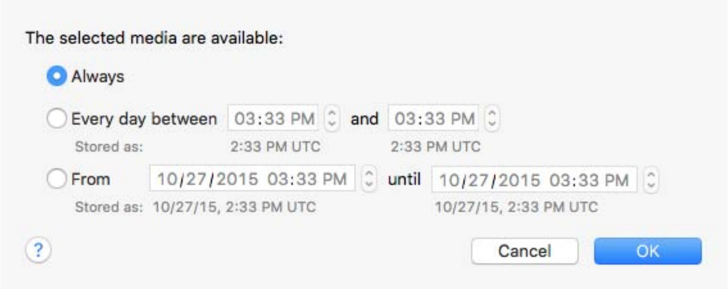
2. If you do not want to restrict the time during which the file is available, you are done. Only if you want to restrict it, continue.

3. Click the **LANrev Safe Media** group inside the policy in the sidebar so that the media files that are assigned to the policy are being displayed in the main part of the window.

   It is not possible to restrict the availability of books in the **iBooks Media** group.

4. Right-click the media file and choose **Set Availability Time** from the context menu.

   The **Set Availability Time** dialog is displayed:



The selected media are available:

● Always

○ Every day between 03:33 PM and 03:33 PM

Stored as: 2:33 PM UTC 2:33 PM UTC

○ From 10/27/2015 03:33 PM until 10/27/2015 03:33 PM

Stored as: 10/27/15, 2:33 PM UTC 10/27/15, 2:33 PM UTC

5. Specify when the file should be available:

   - To make it available for a particular time each day, choose **Every day between** and enter the desired start and end times.
   - To make it available for a one-time period, choose **From** and specify the desired start and end times.

   For further information, see the description of this dialog in “Set Availability Time” on page 642.

6. Click **OK**.

The media file is displayed in the list of files inside LANrev Safe or iBooks (depending on which group you chose) on any mobile device belonging to the policy as soon as the device next contacts the mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

You can send messages (see “Sending a message to mobile devices” on page 236) or e-mails to the users of the devices to notify them of the availability of the new file.

All media files that are available to a device are listed in the **Assignable Items** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Manually installing media files

Media files that have been imported into LANrev for use with LANrev Safe as well as files from the iBooks Store can be manually installed on managed mobile devices under certain conditions:

- The files must be PDF, ePub or iBook files.
- Files for use with LANrev Safe must be permitted to leave LANrev Safe.
- Target devices must run iOS 8 or above.

To manually install media files:

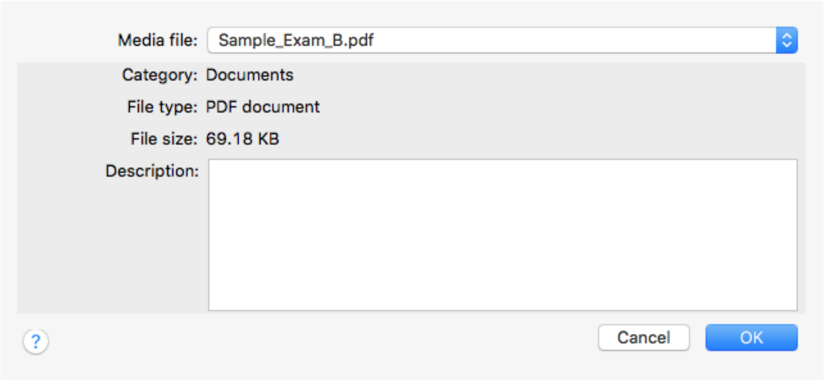
1. To make the desired files available, either:
   - Import them as described in "Importing a media file" on page 223.
     Note that you can import ePub and iBook files, even though LANrev Safe cannot display such files.
     Make sure to check the **Media file can leave LANrev Safe** option in the import dialog.
   - Import a book from the iBooks Store as described in "Distributing iBooks Store books to mobile users" on page 229.

2. In the **Mobile Devices** window, select the devices on which you want to install the media files.

   Note that media files can be installed in this way only on devices running iOS 8 and above.

3. Choose **Commands** > **Install Media File**.

   The **Install Media File** dialog opens:



Media file: Sample_Exam_B.pdf

Category: Documents

File type: PDF document

File size: 69.18 KB

Description:

4. Choose the file that you want to install from the pop-up menu at the top of the dialog.

   Key metadata and a description are displayed in the body of the dialog.

5. Click **OK**.

The file is installed on all selected devices. It may take a few minutes for the information to be reflected in the tables of LANrev Admin.

Providing access to media stored on SharePoint servers

LANrev Safe enables devices on which it is installed to access libraries on SharePoint servers.

The access itself happens completely from within LANrev Safe, using the controls on the settings screen which are described in “Settings screen” on page 969.

No preparation is necessary, neither in LANrev nor in SharePoint (beyond setting up a standard library).

It is, however, possible to configure the SharePoint access from LANrev through configuration profiles. Options include:

- Restrictions on using files from SharePoint outside the LANrev Safe app
- Restrictions on when a device can access SharePoint
- Preconnecting the device with one or more libraries
- Preventing users from manually adding SharePoint libraries to LANrev Safe from their device
- Preventing SharePoint access (by not connecting the device with any libraries and preventing the user from manually adding a library)

To configure the LANrev Safe SharePoint access for mobile devices:

1. Create a configuration profile as described in “Creating a new configuration profile” on page 182.

   In the **Configuration Profile Type** dialog, create a profile for an application and specify LANrev Safe as the app to configure.

2. For each SharePoint library you want the devices’ users to automatically be able to access, create an LANrev Safe SharePoint object in the profile and specify the object’s settings as desired.

   For a description of the available options, see “LANrev Safe SharePoint” on page 674.

3. If you want to prevent the users from adding libraries on their own, uncheck the **Add new SharePoint libraries** option in the LANrev Safe Settings section of the profile.

4. Save the configuration profile and distribute it to the devices you want to configure as described in “Overview of installing configuration profiles on mobile devices” on page 186.

Distributing iBooks Store books to mobile users

You can push-install commercial books from the iBooks Store to mobile users in a similar way to commercial apps or make them available to users of managed devices to install on demand. Books from the iBooks Store can only be distributed to devices running iOS 6.0 or above.

There are two ways to make a book available to mobile users:

- By letting the users download the book from the iBooks Store. In that case, you need only assign the licenses to the users, as described in "Managing VPP app codes and licenses" on page 209.
- By making the book available in LANrev Apps.
  The book record needs to be assigned to the desired users through a policy as an on-demand item, as described in "Distributing a media file" on page 225. It appears in the **iBooks Store** section, and when a user clicks the **iBooks Store** or **Install** button, the VPP license is automatically assigned to the user.
  Note that you cannot push-install books from the iBooks Store.

Creating records for iBooks Store books

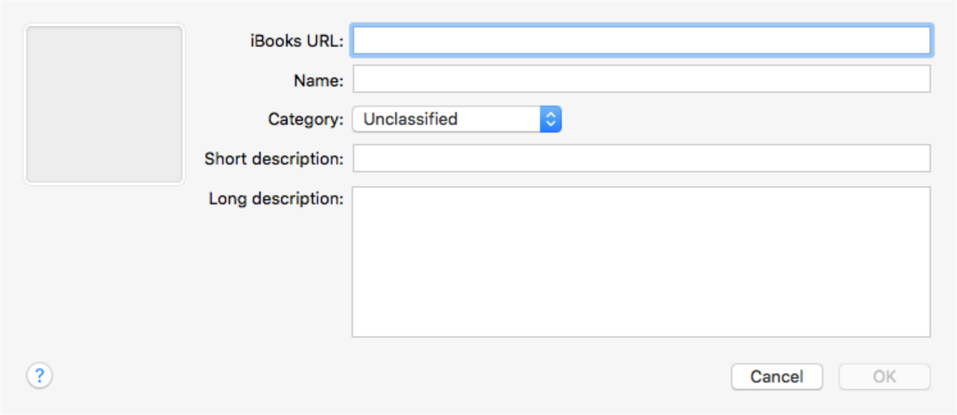
You can create records for books from the iBooks Store that can then be distributed to mobile devices.

These book records contain references to the books, not the actual books themselves, and appear in the **iBooks Store** section of LANrev Apps. Users can install these books from LANrev Apps.

To create and distribute iBooks Store book records:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Books** > **New iBooks Book**.

   The **iBooks Book** dialog opens:



iBooks URL:

Name:

Category: Unclassified

Short description:

Long description:

2. Enter the URL of the book's iBooks Store page in the **iBooks URL** field and press the Tab key or click in another field.

After a moment, LANrev automatically fills the other fields with information from the store.

You can obtain the URL by right-clicking the book’s icon anywhere in the online store and choosing **Copy Link** from the context menu.

3. If desired, edit the information shown.

4. Click **OK** to close the dialog and save the new book record.

5. The new book record appears in the **Assignable Items** > **iBooks Store Books** section in the **Mobile Devices** window.

6. Drag the app package to the **iBooks Store Books** > **On-demand** section of a policy containing the devices to which you want to recommend the book.

   Policies are described in “Working with policies” on page 245.

The next time a device that belongs to that policy contacts the mobile OS vendor’s notification server, the book information is sent to that device. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The package appears on the device in the **iBooks Store** section of LANrev Apps.

Users can install the app by clicking the **Install** button; if they do so, the app is downloaded from the iBooks Store normally. If you have a VPP account with available licenses for the book and the user is assigned to that account, the VPP license is used.

Managing VPP book licenses

Apple’s App Store volume purchase program (VPP) lets you purchase blocks of licenses that enable users to download the corresponding books from the iBooks Store.

The VPP covers both books and apps. Before you can use it to allow users to download licensed books, you must set it up, as described in “Setting up VPP license management” on page 211.

Once the program is set up, you can assign licenses for books from the iBooks Store, as described below. Monitoring these licenses is the same as for app licenses, as described in “VPP license statistics” on page 220.

Apple’s licensing conditions do not allow book licenses to be revoked, once assigned, so there is no option for revoking book licenses.

Assigning VPP book licenses

You can assign book licenses when selecting users, devices, or media files.

Assigning a license when users or devices are selected:

1. In the main part of the **Mobile Devices** window, right-click one or more users or devices and choose **Assign Book Licenses** (for users) or **VPP Licensing** > **Assign Book Licenses to Device Users** (for devices).

   The **Assign Book Licenses to Users** dialog opens.

2. Check all listed books that you want to assign to the selected users or the users of the selected devices.

   To filter the list, you can enter part of the name of the desired book in the search field at the upper right of the dialog.

3. Click **OK**.

Licenses for the marked books are assigned to the selected users. The book is added to the users list of purchased items in the iBooks Store.

Any devices of these users that have been set up in their local settings to automatically download books purchased on other devices will download the assigned books. On other devices, users will have to download the books manually.

Assigning a license when iBooks Store books are selected:

1. Make sure that you have book entries for all books that you want to assign.

   Creating packages is described in “Distributing iBooks Store books to mobile users” on page 229. When setting up a book record, make sure to use the same iBooks Store URL as you have used when purchasing the license.

2. In the main part of the **Mobile Devices** window, right-click one or more iBooks Store books and choose **VPP Licensing** > **Assign Book Licenses to Device Users**.

   The **Assign VPP Licenses** dialog opens, with the selected books listed in the upper half.

3. In the lower half of the dialog, check all users to whom you want to assign the listed books.

   To filter the list, you can enter part of the name of the user you are looking for in the search field at the right of the dialog.

4. Click **OK**.

Licenses for the selected books are assigned to the marked users. The books are added to the users’ lists of purchased items in the iBooks Store.

Any devices of these users that have been set up in their local settings to automatically download books purchased on other devices will download the assigned books. On other devices, users will have to download the books manually.

Working with actions

Actions let you specify what LANrev is to do when a device is added to a smart policy.

Available actions include:

- Sending a message to the device
- Setting roaming options on the device
- Setting activation lock options on the device
- Enabling the activation lock on a shared device
- Setting the wallpaper on the device
- Renaming the device
- Updating the operating system
- Setting the values of custom information fields for the device
- Setting the attention mode on the device
- Setting the lost mode on the device
- Setting the grace period before unlocking the device requires the passcode
- Specifying what kind of diagnostic information the device reports
- Updating the information about the device stored on the server
- Setting the wallpaper on the device
- Remotely locking the device
- Removing the passcode from the device
- Adding the device to the VPP program or removing it
- Sending an invitation to register for the VPP program
- Validating the apps installed on the device
- Removing MDM or configuration profiles
- Configuring devices for a classroom setting

Actions are defined centrally and stored in the **Actions** group in the **Mobile Devices** window, from where they can be assigned to any desired policies.

Details of working with actions are described below.

Creating a new action

To create a new action:

1. In the sidebar of the **Mobile Devices** window, choose the appropriate command from the **Actions** submenu of the context menu:

- **New Send Message Action** to create an action that sends a message to the device that has joined the smart policy.
- **New Send E-Mail Action** to create an action that sends an e-mail to one or more specified addresses (usually those of administrators).
  Note that LANrev can send e-mails only when the SMTP information in the **Notification** tab of the **Server Settings** is filled in.
- **New Send SMS (Text Message) Action** to create an action that sends a text message (SMS) to one or more specified phones (usually those of administrators).
  Note that LANrev can send texts only when the SMS information in the **Notification** tab of the **Server Settings** is filled in.
- **New Set Roaming Options Action** to create an action that configures data and voice roaming permissions on the device.
- **New Set Activation Lock Options Action** to create an action that configures the availability of the iOS activation lock on the device.
- **New Enable Activation Lock Action** to create an action that enables the activation lock on the device.
  This action can be applied only to shared devices enrolled in Apple School Manager.
- **New Set Wallpaper Action** to create an action that set the wallpaper displayed on the device.
  Note that you can also set the wallpaper through a profile, as described in “Working with wallpaper” on page 259.
- **New Set Device Name Action** to create an action that renames the device.
- **New Install iOS Update Action** to create an action that triggers an operating system update on the device.
- **New Validate Applications Action** to create an action that validates enterprise apps installed on the device.
- **New Set Custom Field Value Action** to create an action that sets the value of a manual custom information field for the device.
- **New Update Device Information Action** to update the information stored on the server for the device. (As if **Update Device Information** has been chosen for the device.)
- **New Set Attention Mode Action** to enable or disable the attention mode on the device. (The attention mode is described in “Enabling and disabling the attention mode” on page 239.)
- **New Set Lost Mode Action** to enable or disable the lost mode on the device.
- **New Set Passcode Lock Grace Period Action** to specify how soon after locking the device unlocking it requires a passcode.
- **New Configure Diagnostic Data Transmission Action** to specify what kind of diagnostic data the device reports.
- **New Freeze Device Action** to create an action that changes the access pass phrase on the device and locks it. (This makes the device inaccessible to the local user.)

- **New Clear Passcode Action** to create an action that removes the access pass phrase from the device.
- **New Register User in VPP Action** to create an action that adds the device to the VPP program.
- **New Send VPP Invitation Action** to create an action that send an invitation to register in the VPP program to a user.
- **New Retire User from VPP Action** to create an action that removes the device from the VPP program.
- **New Remove Configuration Profile Action** to create an action that removes a configuration profile from the device.
- **New Demote to Unmanaged Device Action** to create an action that removes the MDM profile and, where applicable, the LANrev client software from the device. (This means that the devices is no longer managed through LANrev.)
- **New Configure Devices for Current Classroom Setup Action** to create an action that configures the device according to the settings in the **Classroom Management** window at the time the action is executed.
  This action can be applied only to devices enrolled in Apple School Manager.

A dialog specific to the action is displayed.

2. Fill in the dialog’s fields as desired.

   For an explanation of the available fields, see the dialog descriptions in:

   - “New Send Message Action” on page 571
   - “New Send E-Mail Action” on page 572
   - “New Send SMS (Text Message) Action” on page 573
   - “New Set Roaming Options Action” on page 574
   - “New Set Activation Lock Options Action” on page 575
   - “New Set Wallpaper Action” on page 577
   - “New Set Device Name Action” on page 578
   - “New Set Custom Field Value Action” on page 581
   - “New Update Device Information Action” on page 582
   - “New Set Attention Mode Action” on page 583
   - “New Set Lost Mode Action” on page 584
   - “New Set Passcode Lock Grace Period Action” on page 585
   - “New Configure Diagnostic Data Transmission Action” on page 586
   - “New Freeze Device Action” on page 587
   - “New Register User in VPP Action” on page 588
   - “New Send VPP Invitation Action” on page 590
   - “New Retire User from VPP Action” on page 592
   - “New Remove Configuration Profile Action” on page 593
   - “New Demote to Unmanaged Device Action” on page 593

3. Click **OK** to save the action.

The new action appears in the **Actions** group of the sidebar and can be assigned to policies, as described in "Specifying actions in policies" on page 247.

Re-executing actions

You can re-execute actions on devices in various ways:

- A single action on a single device: Display the device in the sidebar of the **Mobile Devices** window; expand it and click its **Performed Actions** subcategory; right-click the desired action and choose **Re-execute This Action for This Device** from the context menu.
- A single action on all applicable devices: Display the **Actions** subcategory of the **Assignable Items** category in the sidebar of the **Mobile Devices** window; right-click the desired action in the main table of the window and choose **Re-execute This Action for All Devices** from the context menu.
- A single action on all devices of a policy: Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subcategory; right-click the desired action in the main table of the window and choose **Re-execute This Action for This Policy** from the context menu.
- All actions on a single device: Display the device in the sidebar of the **Mobile Devices** window; expand it and click its **Performed Actions** subcategory; right-click anywhere in the window's table area and choose **Re-execute All Actions for This Device** from the context menu.

In each case, an alert is displayed in which you can choose between re-executing the actions when a target device next checks in and immediately re-executing them.

Any delays and repetitions you have specified for an action also apply when it is re-executed.

Reviewing actions

All actions that have been applied to a device are listed in the **Performed Actions** subgroup of the device when it is expanded in the sidebar of the **Mobile Devices** window.

Deleting actions

To delete an action from LANrev, right-click it in the sidebar of the **Mobile Devices** window and choose **Remove Action** from the context menu.

This deletes the action, including removing it from all policies to which it is assigned.

For removing actions from individual policies, see "Specifying actions in policies" on page 247.

Sending a message to mobile devices

You can send messages from LANrev Admin directly to administered mobile devices (except Windows Phone devices), either manually as described below or automatically by assigning an action to a policy, as described in “Working with actions” on page 232.

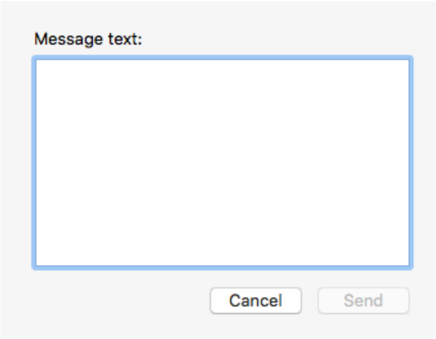
Note that this requires the LANrev Apps application to be installed on the target devices (and having been launched at least once) and push notifications to be enabled on the devices. See “Preparing iOS devices for software installation” on page 195 for information on deploying LANrev Apps on iOS.

To send a message to mobile devices:

1. In the **Mobile Devices** window, select the devices to which you want to send the message.

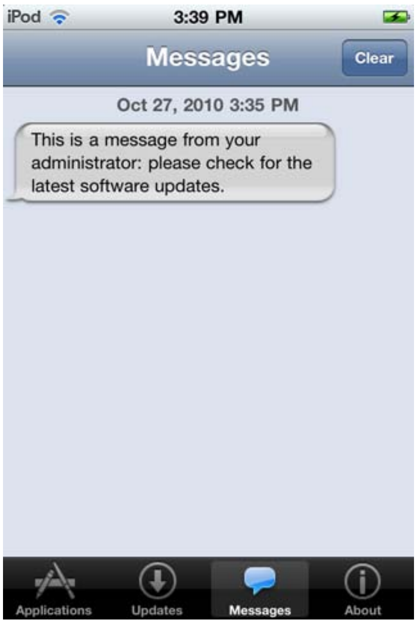
2. Right-click the devices and choose **Send Message to Device** from the context menu.

   The **Message** dialog opens:



3. Enter the message and click **Send**.

The message is sent to all selected mobile devices. It is displayed the next time they contact mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If they are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.



Oct 27, 2010 3:35 PM

This is a message from your administrator: please check for the latest software updates.

Managing mobile device locks

LANrev lets you control locks of mobile devices in several ways:

- You can immediately lock or unlock managed devices, as described in “Locking and unlocking mobile devices” on page 237.
- You can lock managed devices through a policy be using the Freeze Device action. Details on using actions are described in “Working with actions” on page 232.
- You can immediately put a device into attention mode or release it, as described in “Enabling and disabling the attention mode” on page 239.
- You can control the attention mode on the device using the Attention Mode action. Details on using actions are described in “Working with actions” on page 232.
- You can specify the use of the iOS activation lock, either directly as described in “Setting activation lock options” on page 241 or through the Set Activation Lock Options and Enable Activation Lock actions. Details on using actions are described in “Working with actions” on page 232.
- You can enable and disable the Lost mode on supervised devices running iOS 9.3 and up. Details are descried in “Enabling and disabling the Lost mode” on page 240.

Locking and unlocking mobile devices

You can remotely lock mobile devices or remove the passcode from the device. These functions are not available for Windows Phone devices.

To lock a mobile device:

1. In the **Mobile Devices** window, select the devices you want to lock.

2. Right-click the devices and choose **Issue Device Lock** from the context menu.

   A confirmation dialog is displayed. If any of the selected devices does not have passcode, you are prompted to provide one. This passcode will be set on the locked devices.

   For devices running iOS 7.0 and up, you can also specify a message and phone number to be displayed on the lock screen.

3. Click **Lock Device**.

The command is executed on each selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Locking a device is similar to switching it off; to reaccess the device, the user needs to swipe on the start screen and enter the passcode (unless no passcode has been set for the device).

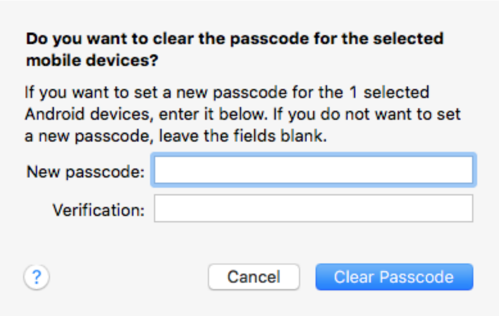
Note that you can also lock devices by assigning an action to a policy. This is described in "Working with actions" on page 232.

To remove the passcode from a mobile device and optionally setting a new one:

1. In the **Mobile Devices** window, select the devices from which you want to remove the passcode.

2. Right-click the devices and choose **Issue Clear Passcode** from the context menu.

   The **Clear Passcode** dialog is displayed:



Do you want to clear the passcode for the selected mobile devices?

If you want to set a new passcode for the 1 selected Android devices, enter it below. If you do not want to set a new passcode, leave the fields blank.

New passcode:

Verification:

3. If you want to set a new passcode, enter it in the **New passcode** and **Verification** fields.

   Setting new passcodes applies only to Android devices. If only iOS devices are selected, the respective fields are not shown in the dialog.

   Note that, if the configuration profile of the device requires a password, the user is prompted for a new password if you do not specify one.

4. Click **Clear Passcode**.

The command is executed on each selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

If you have not specified a new passcode and there is no configuration profile on the device that makes a passcode mandatory, the device is now accessible to anybody without requiring a passcode.

Enabling and disabling the attention mode

Some mobile devices support the so-called attention mode, which you can enable and disable using LANrev.

The attention mode is a transitory lock. In this mode, a message is displayed on the device's screen and no interaction is possible, even after a restart, until you disable the mode again.

The attention mode can be set on:

- iOS: Any supervised device.(Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)
- Android: Devices on which LANrev Apps 2.0.9 or up is installed or running Samsung SAFE on which LANrev Apps 2.0.5 or up is installed.

Setting the attention mode

To enable or disable the attention mode:

1. In the **Mobile Devices** window, select the devices on which you want to set the mode.

2. Right-click the devices and choose **Enable Attention Mode** or **Disable Attention Mode** from the context menu, depending on the desired effect.

If you choose **Enable Attention Mode**, a dialog opens in which you can enter the message to be displayed. Enter the desired message.

If you choose **Disable Attention Mode**, a confirmation dialog is displayed.

3. Click **OK**.

The command is executed on each selected device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Note that you can also set the attention mode by assigning an action to a policy. This is described in "Working with actions" on page 232.

Enabling and disabling the Lost mode

Supervised devices running iOS 9.3 and up support the so-called Lost mode, which you can enable and disable using LANrev.

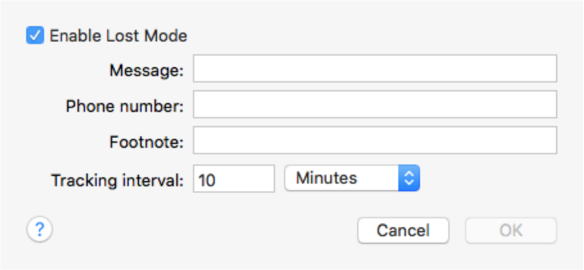
The Lost mode is a transitory lock. In this mode, a message is displayed on the device's screen and no interaction is possible, even after a restart, until you disable the mode again. It also causes to location of the device to be tracked in LANrev.

Setting the Lost mode

To enable or disable the Lost mode:

1. In the **Mobile Devices** window, select the device on which you want to set the mode and choose **Commands** > **Set Lost Mode**.

   The **Set Device Lost Mode** dialog opens:



☑ Enable Lost Mode

Message:

Phone number:

Footnote:

Tracking interval: 10 Minutes

2. If you want to disable the Lost mode, uncheck **Enable Lost Mode** and continue with step 3.

   If you want to enable the Lost mode, check **Enable Lost Mode** and enter the required information (all of which is optional):

- Enter text you want to display in the center or at the bottom of the lock screen in the **Message** and **Footnote** fields, respectively.
  You can use the variables defined by LANrev in the message. For a list of supported variables, see "Variables for mobile devices" on page 458.
- Enter the phone number where the finder of the device can reach you in the **Phone number** field.
  Note that the lost device can call this number although being otherwise locked against use.
- In the **Tracking interval** field, specify the interval in which the position of the device will be determined and recorded in the LANrev database.

3. Click **OK**.

If the Lost mode is disabled, the devices become accessible normally again. If it is enabled, the device becomes inaccessible and displays the specified information on its lock screen. In addition, the device is tracked with the specified frequency, and the locations are stored in the LANrev database. You can view the gathered locations with LANrev Find or in the sidebar of LANrev Admin's **Mobile Devices** window, in the **Device Tracking** section of the device details.

The command is executed on each selected device the next time it contacts its notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Setting activation lock options

From version 7.0, iOS includes the activation lock feature that requires the user's Apple ID before the device can be erased or reactivated.

By default, the activation lock on supervised devices is not active when "Find My iPhone" is switched on.

In cases where activation locking is desired, LANrev lets you enable this connection, which means that the activation lock will be enabled on the device when "Find My iPhone" is switched on.

Activation lock options can only be set on supervised devices running iOS 7 or up.

Enabling and disabling activation locks

Activation locks are handled differently on personal devices and shared devices. To enable activation locks for personal devices:

1. In the **Mobile Devices** window, select the devices on which you want to set the activation locks.

2. Right-click the devices and choose **Set Activation Lock Options** from the context menu.

A dialog is displayed.

3. Click the appropriate button in the dialog:

   - To enable the activation locks, click **Allow Activation**.
     On all selected devices, whenever “Find My iPhone” is enabled on a device, the activation lock is also enabled. When “Find My iPhone” is disabled, so is the activation lock
   - To disable the activation locks, click **Disallow Activation**.
     The activation lock can no longer be enabled on the selected devices; it will remain off regardless of the setting of “Find My iPhone”.
     Note, however, that any activation lock that is already on remains on. (See below for details.)

The activation lock options on all selected devices are changed according to the button you clicked.

To enable the activation lock for shared devices:

1. Select the devices and choose **Commands** > **Activation Lock** > **Enable Activation Lock**.

   If you choose the command normally, a unique bypass code will be generated for each selected device. If you hold down the Option key while choosing the command, a universal bypass code will be generated that is the same for all devices you lock in this manner (even if you do so on different occasions).

2. Specify the message to be displayed on a locked device’s screen.

3. Click **OK**.

LANrev enables the activation lock and stores the bypass codes in its database. Any future activation of the device requires the bypass code to be supplied.

Note that you can also set activation lock options (for personal devices) or enable activation locks (for shared devices) by assigning an action to a policy. This is described in “Working with actions” on page 232.

Disabling the activation lock when it is already active

When “Find my iPhone” has been enabled on a managed device, disabling the activation lock with the procedure described above does not deactivate it.

To switch off an activation lock that is already on, “Find My iPhone" must be switched off, which must be done manually on the device.

Disabling an activation lock

To unlock a device on which the activation lock feature is enabled:

1. In the **Mobile Devices** window, select the device which you want to unlock.
2. Right-click the device and choose **Activation Lock** > **Show Activation Lock Bypass Code** from the context menu.

   The activation lock bypass code for the device is displayed. Copy or note this code.

   For devices under classroom management, two different bypass codes may exist, only one of which is however active at any given time. For such devices, both codes are displayed. The second code should be used if the first one does not unlock the device.
3. Right-click the device and choose **Activation Lock** > **Remove Activation Lock** from the context menu.

   A dialog is displayed.
4. To remove the lock, click **Remove Activation Lock**.

   Another dialog is displayed. Enter the bypass code from step 2 and click **OK**.

The activation lock on the selected device is removed.

Erasing mobile devices

You can remotely erase the entire contents of mobile devices.

IMPORTANT Note that this action is not reversible and that the erased information cannot be recovered from the mobile device (although recovering the data from a backup, should one exist, might be possible). Erasing devices without the consent of their users may expose you to legal liability.

To erase a mobile device:

1. In the **Mobile Devices** window, select the devices you want to erase.
2. Right-click the devices and choose **Erase Device** from the context menu.

   A confirmation dialog is displayed. For devices with internal SD cards, you can choose to erase these cards as well.

   When activation locking is enabled on a device, you can remove the lock as part of erasing the device.

3. Click **Erase Device**.

The next time a selected device contacts the mobile OS vendor’s notification server, all of its data is erased. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Erasing the device removes any user data and all applications that were installed by the user. This effectively resets the device to its factory condition.

The erased device can no longer be administered through LANrev until it has been enrolled again or it has been completely restored from a backup that contains the enrollment profile.

Remotely controlling mobile devices

LANrev lets you view and control the screens of a managed mobile device on which LANrev Remote is installed (which requires Samsung SAFE).

For similar functions related to computers, see “Remotely controlling computers” on page 151.

Setting up remote control

Make sure that LANrev Remote is installed on all mobile devices that you want to control remotely. Also make sure that port 5500 is open in the firewall of the computer on which LANrev Admin is running.

You can configure the settings of LANrev Remote by assigning a configuration profile. Creating a profile is described in “Creating or importing configuration profiles” on page 182; the options available for LANrev Remote are described in “LANrev Remote profiles” on page 678.

Initiating remote control

To remotely control a managed mobile device:

1. In any browser window displaying mobile devices, select the device whose screen you want to share.

2. Right-click the selected device and choose **Remote Control** from the context menu.

3. Depending on how the copy of LANrev Remote is configured, the user may need to accept the connection by tapping **Share Screen** in a dialog presented on the device.

If the user of the mobile device accepts the connection (or LANrev Remote is set up not to ask the user), LANrev opens a new **LANrev Remote** window in which the screen of the mobile device is displayed.

At the bottom of the window, there are additional buttons that simulate the hardware buttons present on some Android devices.

Working with policies

You can automate certain aspects of mobile device administration by using policies.

A policy is a collection of a range of different elements (all of which are optional):

- Managed mobile devices
  Policies cannot contain unmanaged devices, with the exception of the special **Unmanaged devices** policy.
- Commercial applications that are recommended for use on these devices
- Enterprise applications that are either:
  - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
  - Prohibited on these devices
  - Automatically installed on devices that are added to the policy and left on devices that are removed from the policy
  - Allowed on the devices belonging to the policy
  - Allowed on the devices belonging to the policy and deleted from devices that are removed from the policy
- Configuration profiles that are:
  - Mandatory on these devices
  - Available on these devices to be installed by users at their discretion
  - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
  - Forbidden on the devices belonging to the policy
- Media files that are:
  - Automatically installed on devices that are added to the policy and deleted from devices that are removed from the policy
  - Automatically installed on devices that are added to the policy and left on devices that are removed from the policy
  - Allowed on the devices belonging to the policy
  - Allowed on the devices belonging to the policy and deleted from devices that are removed from the policy
- Actions that are performed when mobile devices become members of the policy (smart policies only)
- A device enrollment profile.

Any changes you make to a policy becomes effective on a device the next time the device contacts the mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The details of working with policies are described in:

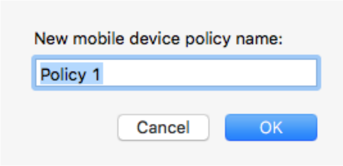
- **Creating a policy** (page 246)
- **Adding and removing mobile devices** (page 247)
- **Specifying actions in policies** (page 247)
- **Specifying applications in policies** (page 249)
- **Specifying configuration profiles in policies** (page 249)
- **Specifying media in policies** (page 250)
- **Automatically assigning device enrollment profiles** (page 59)

Creating a policy

To create a policy to which you manually add devices:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Policies** > **New Policy**.

   The **New Mobile Device Policy** dialog is displayed.



New mobile device policy name: Policy 1

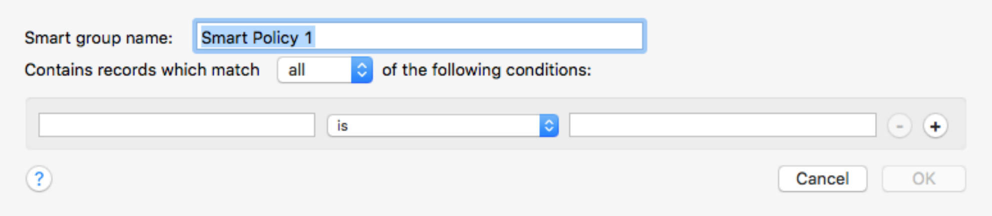
2. Enter the name of the new policy and click **OK**.

The new policy is added to the **Policies** section of the sidebar. It does not contain any devices; you must add them manually as described below in “Adding and removing mobile devices”.

To create a policy to which devices are added automatically according to criteria you specify:

1. In the **Mobile Devices** window, right-click in the sidebar and choose **Policies** > **New Smart Policy**.

   The **Smart Group** dialog is displayed.



Smart group name: Smart Policy 1

Contains records which match all of the following conditions:

is

2. Enter the name of the new policy.

3. Specify the criteria that a mobile device must meet to be included in the group.

   For more information on using this kind of dialog, see “Creating a smart group” on page 140.

4. Click **OK**.

The new policy is added to the **Policies** section of the sidebar. It contains all mobile devices that meet the specified criteria. You cannot manually add or remove devices. If a device later meets the criteria, it is automatically added; likewise a device belonging to the policy is automatically removed when it no longer meets the criteria.

Adding and removing mobile devices

Standard policies allow devices to be manually added or removed, but smart policies do not.

To add a mobile device to a policy:

1. In the **Mobile Devices** window, drag the device that you want to add from any group listing devices to the policy to which you want to add it.

The device is now part of the policy and is listed in the main part of the window when you click the policy in the sidebar.

To remove a mobile device from a policy:

1. In the **Mobile Devices** window, select the devices you want to remove.

2. Right-click the devices and choose **Remove from Policy** from the context menu.

The device is now part of the policy and is listed in the main part of the window when you click the policy in the sidebar.

All policies to which a device belongs are listed in the **Policies** section that is available when the device is expanded in the sidebar of the **Mobile Devices** window.

Specifying actions in policies

For each smart policy, you can specify actions that are to be performed when a device is added to the policy.

Adding actions to a policy

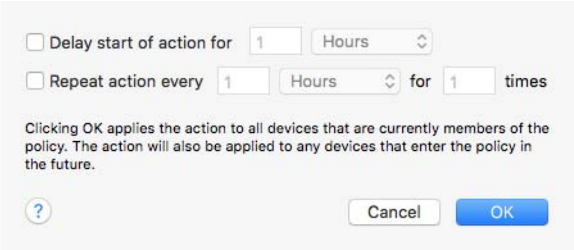
Any actions you want to specify must already been available in the **Actions** group of the **Mobile Devices** window sidebar. See “Working with actions” on page 232 for information on managing actions.

To specify an action in a policy:

1. In the **Mobile Devices** window, drag the action that you want to add from the **Actions** group in the sidebar of the **Mobile Devices**

window to the smart policy to which you want to add it. (Actions cannot be added to standard – non-smart – policies.)

The **Action Assignment Options** dialog is displayed:



□ Delay start of action for 1 Hours

□ Repeat action every 1 Hours for 1 times

Clicking OK applies the action to all devices that are currently members of the policy. The action will also be applied to any devices that enter the policy in the future.

2. Specify whether you want to delay or repeat the action:

   - If you check the delay option, the action is not performed immediately when a device becomes a member of the policy, but only after the specified interval has elapsed.
   - If you check the repeat option, the action is repeated after the specified interval for the specified number of times.

   You can combine both options, for example, to send a message to the device two hours after it has become a member of the policy and then every hour thereafter.

   A delayed or repeated action is not executed when the device is no longer a member of the policy.

3. Click **OK**.

The action is added to the policy. It is executed on all devices that are currently a member of the policy and will be executed on each device that enters the policy in the future.

Any delays and repetitions you have specified apply both to existing and future members. The delay for existing members is calculated from the moment when the action is assigned to the policy.

Changing delay or repetition settings

To change the delay or repetition settings for an action in a computer group:

1. Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subgroup.

   The actions assigned to the policy are displayed in the main part of the **Mobile Devices** window.

2. Right-click the action you want to edit and choose **Change Action Schedule**.

3. Set the delay and repetition as desired.

4. Click **OK**.

The new settings for the action in this policy are saved. They are effective immediately.

Removing actions from a policy

To remove an action from a policy:

1. Expand the policy in the sidebar of the **Mobile Devices** window and click its **Actions** subgroup.

   The actions assigned to the policy are displayed in the main part of the **Mobile Devices** window.

2. Right-click the action you want to remove and choose **Remove Action from Policy**.

The action is removed from this policy. Any remaining repetitions or delayed executions are skipped.

For information on removing an action entirely from LANrev (which also removes it from all policies), see "Deleting actions" on page 235.

Specifying applications in policies

In policies, you can specify applications that are available for installation on the mobile devices that belong to the policy, applications that are automatically installed, and applications that are prohibited on these devices.

Doing so is covered in "Making applications available on mobile devices" on page 200 and "Uninstalling applications from mobile devices" on page 203, respectively.

To recommend commercial apps from the Apple App Store or Google Play to users of mobile devices, see "Distributing App Store or Google Play apps to mobile users" on page 206.

Specifying configuration profiles in policies

In policies, you can specify configuration profiles that are required on the mobile devices that belong to the policy and configuration profiles that are prohibited on these devices.

Adding a profile

1. To add a configuration profile to a policy:

2. Drag the configuration profile from the **Assignable Items** > **Configuration Profiles** group to the desired profile group inside the policy:

   - **Auto-install**: These profiles are automatically installed on the devices belonging to the policy.
   - **On-demand**: Users of the devices belonging to the policy can install these profiles if they so desire. The profiles are listed in the **Available** subsection of the **Profiles** section of

LANrev Apps. On-demand profiles are not supported for Windows Phone devices.

- **Auto-install, auto-remove**: These profiles are automatically installed on any device that is added to the policy and automatically removed from any device that is removed from the policy.
- **On-demand, auto-remove**: Users of devices beloging to this policy can install these profiles if they so desire. The profiles are automatically removed from any device that is removed from the policy.
- **Forbidden Configuration Profiles**: These profiles cannot be installed on the devices belonging to the policy.

The next time a device that belongs to the policy contacts the notification server, the configuration profile is installed and activated, made available, or deleted on that device, depending on the category into which you have put it.

Removing a profile

To remove a configuration profile from a policy:

1. Select the configuration profile in the policy.

2. Right-click the profile and choose **Remove Configuration Profile**.

The profile is removed from the policy. There is no immediate effect on the devices that belong to the policy. That is, when you remove a profile from the policy’s **Auto-install** list, it is not removed from the devices; and when you remove a profile from the **Forbidden** list, it is not installed on the devices.

However, the restrictions on the mobile devices with respect to the configuration profiles are lifted: A previously required profile may now be deactivated or removed, and a previously prohibited profile may now be installed and activated.

Conflicting profile assignments in multiple policies

It is possible that a device belongs to multiple policies, more than one of which contains the same configuration profile. The profile need not be in the same category in all policies.

See “Conflicting policy settings for configuration profiles” on page 192 for information on how cases are handled this leads to multiple conflicting profile assignments for a device.

Specifying media in policies

In policies, you can specify media that is automatically made available to user on every device that is added to the policy.

Doing so is covered in “Distributing a media file” on page 225.

Managing mobile device settings

LANrev lets you remotely configure a number of setting on managed mobile devices:

- Screen mirroring. See “Controlling screen mirroring” on page 251 for details.
- Mobile hotspot settings. See “Controlling personal hotspots” on page 252 for details.
- Wallpaper images. See “Setting wallpaper” on page 253 for details.
- Roaming options. See “Configuring roaming on mobile devices” on page 253 for details.
- Names. See “Naming mobile devices” on page 254 for details.
- Home screen layouts. See “Configuring home screen layouts” on page 254 for details.

Controlling screen mirroring

iOS devices support mirroring their screens and rerouting audio to compatible destination devices via AirPlay. LANrev lets you activate, target, and deactivate this output on iOS devices running iOS 7.0 and up.

Note that activating or retargeting the output requires the consent of the local user of the mobile device.

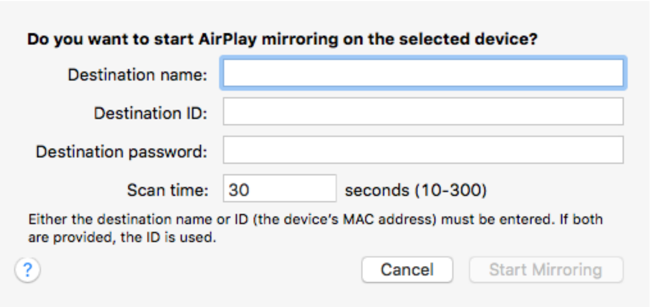
Activating screen mirroring

To activate AirPlay screen mirroring:

1. In the **Mobile Devices** window, select the device on which you want to activate screen mirroring.

2. Right-click the device and choose **Request AirPlay Mirroring** from the context menu.

   The **Request AirPlay Mirroring** dialog is displayed:



Do you want to start AirPlay mirroring on the selected device?

Destination name:

Destination ID:

Destination password:

Scan time: 30 seconds (10-300)

Either the destination name or ID (the device’s MAC address) must be entered. If both are provided, the ID is used.

3. Enter either the name of the target device in the **Destination name** field or its MAC address in the **Destination ID** field.

   Only one of these fields has to be filled in. If you fill in both, the name is ignored.

If you specify the destination ID for an Apple TV device, use the Ethernet MAC address, not the WiFi address.

4. If the target device requires a password to allow AirPlay access, enter the password in the **Destination password** field.

5. If desired, choose a different value in the **Scan time** field.

   This is the timeout for establishing the connection to the destination device. Usually, the default value is fine.

6. Click **Reset Passphrase**.

A confirmation dialog is displayed on the mobile device. If the local user accepts, AirPlay screen mirroring to the specified destination is started.

Retargeting screen mirroring output

To switch active screen mirroring to a different destination device, proceed as described for activating screen mirroring, above. Specify the new destination in step 3.

Deactivating screen mirroring

To switch off AirPlay screen mirroring:

1. In the **Mobile Devices** window, select the devices on which you want to deactivate screen mirroring.

2. Right-click the devices and choose **Stop AirPlay Mirroring** from the context menu.

AirPlay screen mirroring from the devices is stopped.

Controlling personal hotspots

Some mobile devices include a personal hotspot feature that makes their mobile internet connection available to other devices over WiFi. LANrev lets you activate and deactivate this hotspot on iOS devices running iOS 7.0 and up.

Activating or deactivating personal hotspots

To activate or deactivate personal hotspots:

1. In the **Mobile Devices** window, select the devices on which you want to control the hotspots.

2. Right-click the devices and choose **Change Personal HotSpot State** from the context menu.

   A dialog is displayed.

3. Click the appropriate button in the dialog:

- To activate the hotspots, click **Enable Hotspots**.
- To deactivate the hotspots, click **Disable Hotspots**.

The personal hotspots on all selected devices are switched on or off, depending on the button you have clicked.

Setting wallpaper

For supervised devices running iOS 7.1 and up, you can specify the wallpaper of the lock screen and the home screen.

To specify the wallpaper:

1. Select the desired devices in the **Mobile Devices** window.

2. Right-click the devices and choose **Set Wallpaper** from the context menu.

3. In the **Set Wallpaper** dialog, choose the desired image, specify whether it applies to the lock screen, the home screen, or both, and click **OK**.

The wallpaper is set the next time the device contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Note that you can also set the wallpaper of mobile devices by:

- Assigning an action to a policy, as described in "Working with actions" on page 232.
- Specifying the wallpaper in a profile, as described in "Working with wallpaper" on page 259.

Configuring roaming on mobile devices

You can enable and disable data and voice roaming on managed iOS devices.

Note, however, that the local users are not prevented from changing the settings again.

Setting roaming options is not available for Android and iOS 4 devices.

To set the roaming options for managed mobile devices:

1. Select the devices in the **Mobile Devices** window.

2. Right-click the device and choose **Set Roaming Options** from the context menu.

3. In the **Set Roaming Options** dialog, configure the settings as desired.

Settings that are checked will be enabled on the selected devices. Settings that are unchecked will be disabled. Settings in the third neutral state (⊟) will be left unchanged.

The options are set on each device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Note that you can also configure roaming settings of mobile devices by assigning an action to a policy. This is described in "Working with actions" on page 232.

Naming mobile devices

You can rename managed mobile devices from LANrev, provided they are running Android or iOS 8 or above.

To rename a mobile device:

1. Select the device in the **Mobile Devices** window.

2. Right-click the device and choose **Set Device Name** from the context menu.

3. In the **New Mobile Device Name** dialog, enter the desired new name and click **OK**.

The device is renamed the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

The new name is displayed in the **Mobile Device Name** information item.

Note that you can also rename mobile devices by assigning an action to a policy. This is described in "Working with actions" on page 232.

Configuring home screen layouts

LANrev can create configuration profiles for iOS device that specify the arrangement of apps on the home screen, in folders, and in the dock. The profiles can also specify apps that are not displayed on the devices and cannot run on them, as well as the backgrounds of lock and home screens. LANrev contains a specialized graphical editor for these configuration profiles.

Once created, these configuration profiles are managed just as other configuration profiles, as described in "Working with configuration profiles" on page 181.

The details of creating and configuring home screen layout configuration profiles are described in:

- “Creating a home screen configuration profile” on page 255
- “Editing a home screen layout configuration profile” on page 257
- “Positioning icons” on page 257
- “Working with the app list” on page 257
- “Working with folders” on page 258
- “Working with pages” on page 258
- “Hiding apps” on page 258
- “Working with wallpaper” on page 259

Creating a home screen configuration profile

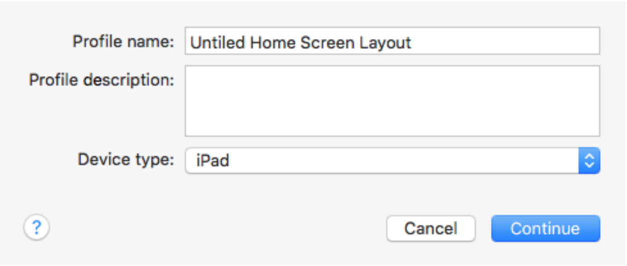
To create a new home screen configuration profile:

1. In the **Mobile Devices** window, either:

   - Right-click in the sidebar and choose **Configuration Profiles and Certificates** > **New Configuration Profile**.
     This opens the **Configuration Profile Type** dialog; choose **iOS home screen configuration profile** in that dialog and click **Continue**.
   - Select devices, right-click one of them and choose **Create Home Screen Layout Configuration Profile** from the context menu. You must select supervised devices running iOS 9.3 or up.

   Both methods are very similar, the difference being that choosing specific devices makes apps that are only installed on the selected devices (but not imported into LANrev) available for placement in the home screen layout editor.

   The Home Screen Layout Profile Settings dialog is displayed:

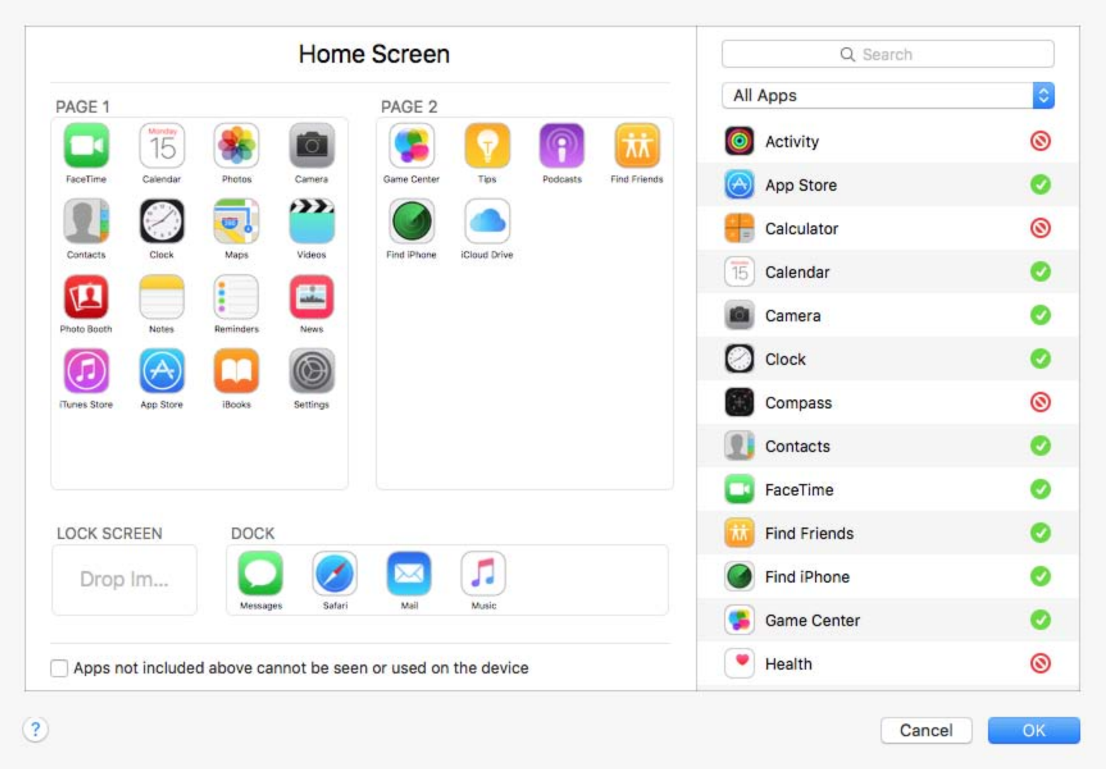

Profile name: Untiled Home Screen Layout
Profile description:
Device type: iPad

2. Specify the name for the profile, describe it, and choose the desired target device.

   The chosen target device determines the number of rows and columns in which you can arrange the icons and the number of available dock icons. It also sets apps to be hidden that are not compatible with the device (such as may be the case with some of Apple’s apps and the iPad).

3. Click **Continue**.

The **Home Screen Layout Editor** dialog is displayed:



The dialog is described in “Home screen layout editor” on page 679.

4. Arrange the icons and specify the backgrounds as desired.

   For a list of available options, see “Configuring home screen layouts” on page 254.

5. Click OK to save the profile.

   Once saved, the profile is managed like any other configuration profile, as described in “Working with configuration profiles” on page 181.

The configuration profile can be installed on supervised devices running iOS 9.3 and up. Installing it has these effects:

- Apps placed on a home screen page, in a folder, or in the dock are positioned on the device as specified if they are present on the device.
  Installing the profile does not automatically install the specified apps, so you must ensure their presence on the device.
- Apps that have been hidden the profile are hidden on the device and can no longer be used. If the same app is later installed on the device, it is automatically hidden as well.
- Apps that are present on the device but not specified in the profile are placed in empty spots left in the profile; if necessary, new home screen pages are added.

If the **Apps not included above cannot be seen or used on the device** option in the layout editor was checked, apps not included in the profile are completely hidden on the device and cannot be launched, even if they are installed again after the home screen layout configuration profile has been installed.

- If a background image has been specified for the home screen or the lock screen, the wallpaper on the device is set accordingly.

Editing a home screen layout configuration profile

To edit an existing home screen layout configuration profile:

1. In the **Mobile Devices** window, double-click the profile you want to edit.

   The Home Screen Layout Profile Settings dialog is displayed.

2. If desired, edit the name for the profile or its description, or choose a different target device and click **Continue**.

   The **Home Screen Layout Editor** dialog is displayed.

3. Change the icon arrangements and the backgrounds as desired.

   For a list of available options, see “Configuring home screen layouts” on page 254.

4. Click OK to save the profile.

The new settings will affect any devices on which the profile is installed in the future, but do not affect any devices on which the profile is already installed. To apply the changes to these devices, you need to reinstall it on them.

Positioning icons

Icons are arranged on the pages of the home screen, in folders, and in the dock mostly by direct manipulation:

- To add an icon to a home screen page, folder page, or the dock, drag it there from the app list or from its current position.
- To remove an icon, point the mouse to it. This displays an “X” badge on the icon; click that “X” to remove the icon.
- To move an icon to a different position, drag it there.

Working with the app list

You can filter the app list:

- To display just apps with particular names, enter a part of the name in the search field above the list.
- To display just a particular category of apps, choose that category from the pop-up menu.
  The available choices are described in “App list” on page 681.

Both filtering options are cumulative. For example, to see only utility apps with “user” in their names, enter “user” in the search field and choose **Category “Utilities”** from the menu.

Working with folders

Icons can be arranged in folders:

- To create a folder, drag an icon on top of another icon.
  Folders can only be created on home screen pages or in the dock, not inside other folders.
- To dissolve a folder, drag all objects (or all objects except one) out of it.
  Pressing Command-A selects all icons in the current folder page.
- To delete a folder, point the mouse to its icon. This displays an “X” badge on the icon; click that “X” to remove the folder.
  Removing a folder also removes all objects inside it.
- To display the contents of a folder, double-click the folder’s icon on the home screen page.
- To rename a folder, display its content and double-click the folder’s name displayed at the top of the editor.
- To add an icon to a folder, drag it on top of the folder icon.
  Folders cannot be added to other folders.
- To move an icon out of a folder, display the folder contents and drag the desired icon to the **< Home Screen** label at the top left of the home screen layout editor.

Working with pages

Icons on the home screen and in folders are arranged on individual pages:

- To rearrange pages, drag them by their label (for example, **Page 1**) to the desired new position.
  You cannot move home screen pages into folders or folder pages to the home screen or to other folders.
- To add a page, place an icon on the **New Page** pseudo-page at the right.
  You may need to scroll the list of pages to display the **New Page** page.
- To remove a page, move all icons on it to other location or to the app list.

Hiding apps

Hiding apps effectively blacklists them: They are no longer visible on devices on which the home screen layout configuration profile is installed and cannot be launched. Even installing them again on the device does not change that as long as the profile remains in effect:

- To hide an app, right-click it and choose **Hide** from the context menu.
  Hiding an app removes it from the home screen pages and marks it with a red stop icon 🚫 in the app list.

- To make a hidden app visible, right-click it in the app list and choose **Make Visible** from the context menu.
  You can also just drag the app's icon from the app list to the home screen.

Note that you can use this feature to hide most built-in apps, but some elementary apps, such as Settings and Phone, cannot be hidden.

Working with wallpaper

In a home screen layout configuration profile, you can specify wallpaper for the lock screen and home screen:

- To set the wallpaper for the home screen, drag the desired image to any home screen or folder page.
  All home screen and folder pages have the same wallpaper.
- To set the wallpaper for the lock screen, drag the desired image to the lock screen area at the bottom left of the editor dialog.
- To remove a lock screen or home screen wallpaper, right-click it and choose **Remove Wallpaper** from the context menu.

Note that you can also:

- Set wallpaper for individual devices as described in "Setting wallpaper" on page 253.
- Set wallpapers for groups of devices automatically by assigning an action to a policy, as described in "Working with actions" on page 232.

Geotracking mobile devices

You can record the locations of iOS or Android devices in LANrev, which is especially helpful if the device is lost or stolen.

For similar functions related to administered computers, see "Tracking computers" on page 164. Note that tracking is also enabled if iOS devices are put into Lost mode, although the main purpose of this mode is locking the devices, as described in "Enabling and disabling the Lost mode" on page 240.

NOTE For information on geotracking iOS devices without activating the Lost mode, contact HEAT Support.

Enabling geotracking of mobile devices requires three major steps:

1. LANrev Apps must be installed on the devices, as described in "Preparing iOS devices for software installation" on page 195 (for iOS devices) and "Enrolling mobile devices" on page 50 (for Android devices), respectively.

2. A passphrase for enabling tracking must be set, as described in "Setting passphrases for mobile devices", below.

3. Tracking must be enabled for the devices, as described in "Enabling geotracking on mobile devices" on page 262.

Collected mobile device locations can be shown either numerically or on a map, as described in "Displaying geotracking information" on page 265.

NOTE LANrev Apps must be running on the mobile device for geotracking to work. It does not need to be the front application, but if a user terminates it, geotracking is no longer possible. (A restart is unproblematic, as LANrev Apps is automatically relaunched when it was running before the restart.)
You can usually get a user to reopen LANrev Apps by sending him or her a message (as described in "Sending a message to mobile devices" on page 236). Viewing the message launches LANrev Apps.

NOTE While geotracking can often be helpful when recovering a stolen mobile device, it is not a reliable theft recovery system by itself. Among other things, a thief can prevent geotracking by switching the mobile device off or by resetting it to the factory condition (erasing LANrev Apps in the process).

Setting passphrases for mobile devices

A passphrase must be set on a mobile devices before geotracking can be enabled on it. The passphrase is to ensure the legitimacy of any tracking requests sent to the device.

A passphrase can be set either individually per device, or a group of devices can have the same passphrase.

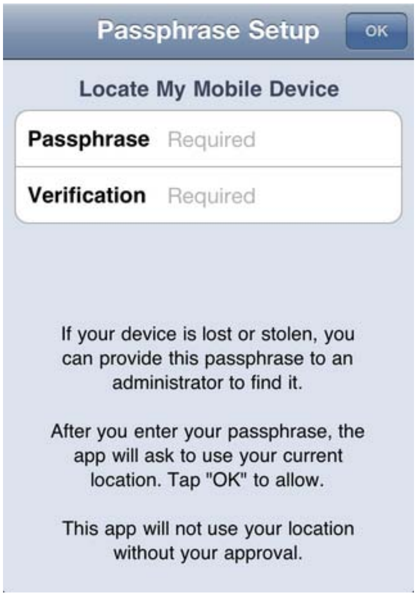
Setting a passphrase individually

If you want to specify an individual passphrase for a device:

1. Install LANrev Apps normally on the device, as described in "Preparing iOS devices for software installation" on page 195 (for iOS devices) and "Enrolling mobile devices" on page 50 (for Android devices), respectively.

   Note: For information on geotracking iOS devices, contact HEAT Support.

2. When LANrev Apps is launched for the first time, the user is first prompted for the server address and then asked to enter a passphrase:



If your device is lost or stolen, you can provide this passphrase to an administrator to find it.

After you enter your passphrase, the app will ask to use your current location. Tap "OK" to allow.

This app will not use your location without your approval.

3. Users must enter the same passphrase in both the **Passphrase** and **Confirm** fields before they can click **OK** to use LANrev Apps.

   The passphrase can consist of any number of characters; it is not restricted to digits.

   Unless the user tells you this passphrase, you cannot enable tracking. If this passphrase is intended to track the device only in emergency situations – when the device is lost or stolen – it is advisable for the user to write down the passphrase in a safe location

The mobile device now has a passphrase. Geotracking for the device can be enabled when the user provides the passphrase to you, as described in “Enabling geotracking on mobile devices” on page 262.

The passphrase cannot be changed on the device. If users want to change the passphrase, they must contact an administrator who resets the passphrase for them, after which they can enter a new passphrase as described above. See “Resetting a passphrase”, below, for more information.

Setting one passphrase for a group of devices

If you want to specify the same passphrase for a large group or all of your managed devices:

1. After LANrev Apps has been installed, go to the LANrev support page at www.heatsoftware.com/support and follow the provided link.

As part of the request, you'll need to provide the desired passphrase. You may also need to sign a legal waiver.

HEAT Software will return an encrypted token to you that is based on a combination of your serial number and the passphrase. You will also receive instructions on using this token to modify LANrev Apps.

2. Follow the instructions provided to set the passphrase on all devices.

   Note that this process requires the user to accept the new passphrase on the device.

All mobile devices on which this procedure was performed and on which the users have accepted the change now have the same passphrase. Geotracking for the device can be enabled using this passphrase, as described in "Enabling geotracking on mobile devices" on page 262.

Resetting a passphrase

You can reset the passphrase on a managed mobile device. This removes the current passphrase and requires a new passphrase to be set, either locally by the user as described in "Setting a passphrase individually", above, or remotely by you, as described in "Setting one passphrase for a group of devices", above.

Passphrases can only be reset on one device at a time.

To reset a passphrase:

1. In the **Mobile Devices** window, select the device on which you want to reset the passphrase.
2. Right-click the device and choose **Reset Tracking Passphrase** from the context menu.

   A confirmation dialog is displayed.
3. Click **Reset Passphrase**.

The current passphrase is removed from the device and a new one must be set before LANrev Apps can be used again on that device.

Enabling geotracking on mobile devices

When iOS or Android devices have been properly set up, as described in "Setting passphrases for mobile devices" on page 260, geotracking can be enabled on them.

IMPORTANT Because the location of a mobile device often is also the location of its user, tracking mobile devices is subject to privacy or data protection laws in many jurisdictions.

Usually, the express consent of the user of the device is required before it may be tracked. In addition, there may be regulations governing how long gathered data may be stored and how and by whom it may be accessed.
Failure to obtain the required consent or observe other applicable legal regulations may expose you to civil and/or criminal liability.

NOTE For information on geotracking iOS devices, contact HEAT Support.

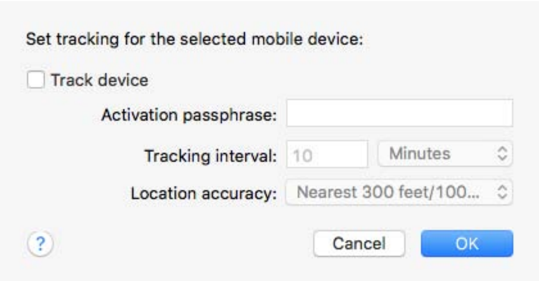
To enable geotracking on mobile devices:

1. In the **Mobile Devices** window, select all devices on which you want to enable geotracking.

2. Right-click the devices and choose **Track Device** from the context menu.

   Note that, if you select multiple devices, all must have the same passphrase.

   The **Mobile Device Tracking** dialog is displayed:

   Set tracking for the selected mobile device:

   □ Track device

   Activation passphrase:

   Tracking interval: 10 Minutes

   Location accuracy: Nearest 300 feet/100...

3. Check the **Track device** option.

4. Enter the passphrase of the devices in the **Activation passphrase** field.

   See "Dealing with lost passphrases", below, for information on what to do when a passphrase has been lost.

5. Set the desired tracking interval and location accuracy.

   Shorter tracking intervals allow for more fine-grained tracking but can create huge amounts of data. For example, tracking 50 devices with an interval of five minutes creates more than five million records per year.

   Better location accuracy lets you pinpoint a device's position with greater precision but is more intrusive of the bearer's privacy. When the desired accuracy is not technically achievable, location data may have a lower accuracy than specified.

Note that you can change the interval and accuracy at a later time, for example, when the device is lost or stolen.

6. Click **OK**.

Geotracking is enabled on each device the next time it contacts the mobile OS vendor's notification server. (See "How managing mobile devices works" on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Dealing with lost passphrases

If tracking is not enabled on a device and the passphrase has been forgotten, there is normally no way to enable tracking when the device is stolen or lost.

(When the device is still available, the situation is easily remedied by resetting the passphrase, as described in "Resetting a passphrase" on page 262.)

To let you enable tracking even in such unfortunate circumstances, HEAT Software can provide you with device-specific code that lets you enable tracking:

1. Go to the LANrev support page at www.heatsoftware.com/support and follow the provided link to enter your request.

   As part of the request, you and the (legal) user of the device may need to sign legal waivers.

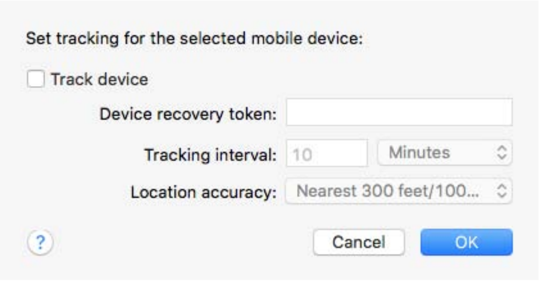
   HEAT Software will send you a special document for LANrev.

2. Send the information shown in the document back to HEAT Software.

   You will receive an encrypted device recovery token.

3. Right-click the device in the **Mobile Devices** window, press the Option key, and choose **Track Device** from the context menu.

   The **Mobile Device Tracking** dialog opens in a special mode:



Set tracking for the selected mobile device:

□ Track device

Device recovery token:

Tracking interval: 10 Minutes

Location accuracy: Nearest 300 feet/100...

4. Enter the device recovery token in the **Device recovery token** field and click **OK**.

Geotracking is enabled on the selected device the next time it contacts the mobile OS vendor’s notification server. (See “How managing mobile devices works” on page 6 for more information.) If devices are online via WiFi or a mobile network, this happens quickly, usually within a minute, but if they are not connected (switched off or out of range of any accessible network), it will happen once the device has reconnected to a network.

Displaying geotracking information

You can display collected locations of mobile devices numerically or graphically on a map.

Displaying locations numerically

To display locations numerically, add the information items from the **Mobile Device Information** > **Device Tracking** category to any group in the **Mobile Devices** window that displays mobile devices.

Displaying locations on a map

To display mobile device locations on a map:

1. In the **Mobile Devices** window, select the location which you want to display.

   If you select a device, the last known location will be shown.

2. Right-click the device and choose **Show Location on Google Maps** or **Show Location on Bing Maps** from the context menu.

A new window is opened in your standard web browser, and the location is shown in Google Maps or Bing Maps, respectively.

Managing classrooms

LANrev can act as a bridge between your school management data from Apple School Manager (ASM) and your device data. In particular, LANrev can create and assign the education profiles which are required to be installed on classroom devices.

Usually, the organizational information – such as user records and class configurations – will be kept in ASM or in specialized tools and exported to LANrev for combining with device data and creating education profiles.

Most aspects of the classroom management are handled in the **Classroom Management** window, which is described on page 649.

For details of managing classroom data in LANrev, see these sections:

- “Setting up classroom management” on page 266

- “Importing classroom data” on page 268
- “Exporting classroom data” on page 269
- “Managing classroom persons” on page 270
- “Managing classroom devices” on page 273
- “Managing classes” on page 274
- “Configuring devices” on page 275

Note that describing the use and concepts of Apple School Manager is beyond the scope of this section. For that kind of information, see Apple’s ASM documentation.

NOTE LANrev can import classroom management information from ASM, but the structure of ASM does not allow for exporting data back to ASM from LANrev. Therefore, you cannot change any information in your ASM account from within LANrev.

Setting up classroom management

Setting up access to your Apple School Manager (ASM) account in LANrev is minimal and mostly automatic.

However, you will want to make sure that the classroom management preferences in LANrev are set correctly for your needs. These preferences determine how LANrev imports ASM data, and their proper setting ensures that the data are imported as expected.

Configuring access to your ASM account

Your ASM account is the same account as your device enrollment program (DEP) account, and the same setup is required for both:

1. Enable your DEP account for school management, if this has not happened yet.

   This must be done on Apples website and cannot be performed with LANrev. Contact Apple for details, if required.

2. Configure your DEP account in LANrev, as described in “Using ADEP” on page 56.

   Depending on the order in which things happen, you will be in one of two situations:

   - If your DEP account was enabled for school management before you set it up in LANrev, you do not need to do anything else. LANrev automatically recognizes ASM. You are now done.
   - If you had configured your DEP account in LANrev before it was enabled for school management by Apple, you must perform the next steps.

3. In the **Server Center** window, click **Server Settings** in the sidebar and then click the **MDM** tab to display the MDM settings.

4. Click the **Configure** button in the **Apple device enrollment program accounts** section.

   The **Apple Device Enrollment Program Accounts** opens which displays all configured DEP accounts.

5. Select the account that is enabled for school management and verify that LANrev shows “Apple School Management: Yes” in the account details section in the lower half of the dialog.

6. Click **OK** to close the dialog.

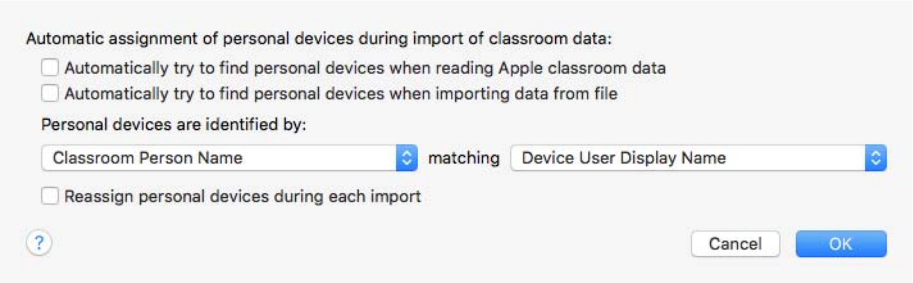
LANrev is now connected to your ASM account.

Setting up classroom management preferences

To set classroom management preferences:

1. Open the **Classroom Management** window and click the Settings toolbar button.

   The **Classroom Settings** dialog opens:



Automatic assignment of personal devices during import of classroom data:

□ Automatically try to find personal devices when reading Apple classroom data

□ Automatically try to find personal devices when importing data from file

Personal devices are identified by:

Classroom Person Name matching Device User Display Name

□ Reassign personal devices during each import

2. Set the options as desired:

   - If you want to create personal device assignments for classroom persons based on known device assignments in LANrev, check **Automatically try to find personal devices when reading Apple classroom data**.
     If you check that option, LANrev will check each person in the data loaded from ASM and try to match it with a user record that exits in the general LANrev database. If it finds a matching user record, it adds any devices to which that user is already assigned to the classroom management database as personal devices of that user.
     If you check this option, you must specify how ASM users are matched with LANrev users. See the next step for details.
   - If you want to perform the same kind of matching with data that you import from a file, check **Automatically try to find personal devices when importing data from file**.
     As above, you must specify how ASM users are matched with LANrev users, as described in the next step.

- If you want the assignment of personal devices to be performed each time data for a particular user is imported, check **Reassign personal devices during each import**. If that option is not checked, personal devices are only assigned to a user the first time that user is imported (either from ASM or a file).

3. If you have specified any assignment of personal devices in the previous step, set up how LANrev matches ASM users with LANrev users:

   - From the left-hand **Personal devices are identified by** list, choose a piece of information that is available in the imported school management data.
   - From the right-hand list, choose a LANrev information item.

   LANrev will consider an ASM user and a LANrev user to be the same person if the pieces of information you have chosen is identical.

   Therefore, it is important that you chose information that is unique in both systems. For example, choosing **Classroom Person Name** will lead to unexpected results if the ASM data contains multiple persons with the same name.

The LANrev classroom management is now set up to correctly import any data from ASM or from files.

Importing classroom data

LANrev can import data directly from ASM as well as from external files that you may have exported from a different management system.

Importing ASM data

To import ASM data:

1. In the **Classroom Management** window, click the Load from ASM button.

   Or choose **Server** > **Reload Apple School Management Data**.

LANrev reads the data from your ASM account configured in the server settings. (See “Configuring access to your ASM account” on page 266 for details.) During the import, it processes the data as specified in the classroom settings, as described in “Setting up classroom management preferences” on page 267.

To update the imported data, click the button or choose the menu command again.

Importing classroom data from a file

To import classroom data from an exported file:

1. Create the export file in the system that currently holds the data.

   The file must be a JSON file with a specific format, as described in “Classroom data import file format” on page 486. How this file is created will depend on the system from which you export the data; see that system’s documentation for further information.

2. Choose **Server** > **Import Classroom Data**.

   An Open dialog is displayed; choose the file you have exported in step 1 and click **Open**.

LANrev imports the data from the file. During the import, it processes the data as specified in the classroom settings, as described in “Setting up classroom management preferences” on page 267.

Exporting classroom data

You can export the classroom data from LANrev, for example, to import it into dedicated school management software. (Note that Apple School Manager does not support importing data.)

You can export all data or only some records, and you can select the types of information to export.

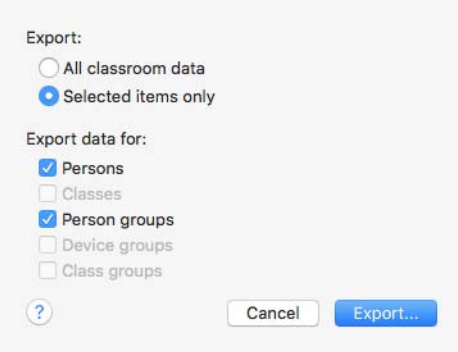
To export classroom data:

1. If you want to export only some records, select those records now in the **Classroom Management** window.

   For example, if you only want to export data for teachers, select the teachers you want to export.

2. Click the Export Data button in the **Classroom Management** window.

3. The **Export Classroom Data** dialog opens:



Export:
○ All classroom data
● Selected items only

Export data for:
☑ Persons
□ Classes
☑ Person groups
□ Device groups
□ Class groups

4. If you want to export just the selected records, choose **Selected items only**. Otherwise, choose **All classroom data**.

5. In the **Export data for** section, check all data categories that you want to export.

   If you have chosen to export only selected items, you can only check categories that apply to these items. For example, if you have selected persons, you cannot choose to export classes.

   Note that exporting groups exports the group definitions, not the contents of the groups. For example, if you check only **Person groups**, no person records are exported, just the definitions of the person groups.

6. Click **Export**.

   A standard Save dialog is displayed.

7. Specify a name and location for the export file and click **Save**.

LANrev exports the specified information as a JSON file. For details on the file format, see “Classroom data import file format” on page 486.

Managing classroom persons

Persons relevant in classroom settings are usually imported from external sources, as described in “Importing classroom data” on page 268.

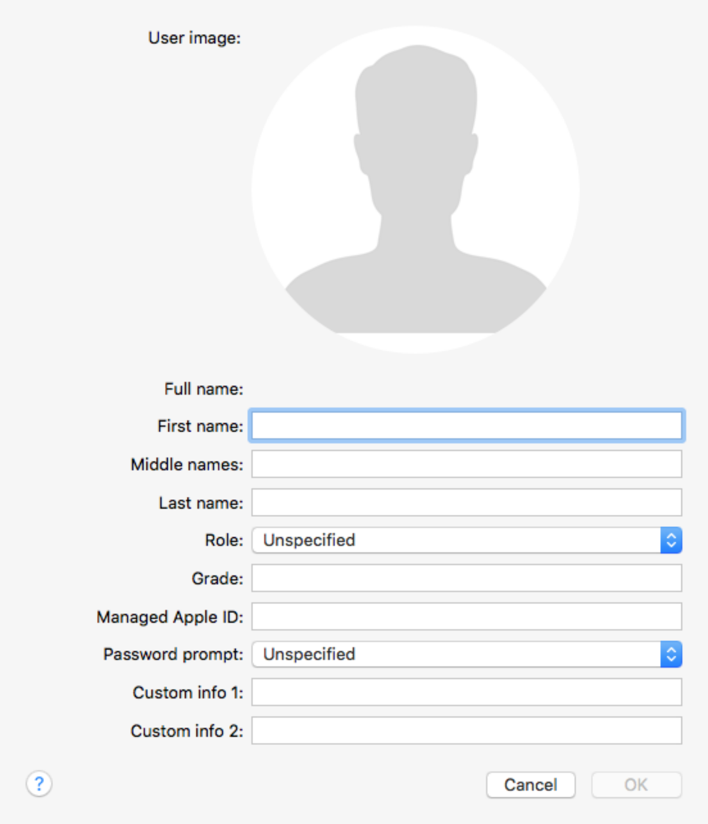
However, you can add, modify, and delete person records in LANrev, if necessary.

Creating a person

To create a person record:

1. Right-click in the **Classroom Management** window’s sidebar and choose **Persons > New Person** from the context menu.

2. The **Person** dialog is displayed:



User image:

Full name:

First name:

Middle names:

Last name:

Role: Unspecified

Grade:

Managed Apple ID:

Password prompt: Unspecified

Custom info 1:

Custom info 2:

3. Fill in the information for the person as required.

   All information is optional, except for at least one name component (first name, middle initial, or last name).

4. Optionally, add a portrait photo. There are several options for doing so:

   - Select the image well and paste an image.
   - Drag an image file from the desktop into the image well.
   - Click the image well to open an image editing sheet, which also lets you create a new image with the camera or load an existing image.
     This image editing sheet is part of macOS; for details on using it, see the macOS documentation.

5. Click **OK**.

LANrev creates a record for the person with the specified information in its database.

Editing a person

To edit a person record:

1. Double-click the person’s entry in the **Classroom Management** window table area or right-click it in the sidebar and choose **Edit Person** from the context menu.

   The **Person** dialog opens (see above), displaying the data of the person.

2. Edit the information as desired and click **OK**.

   Note that some data may not modifiable when the person has been imported from Apple School Manager.

LANrev updates the record for the person with the specified information.

Deleting a person

To delete a person from the LANrev database, select the person in the **Classroom Management** window, right-click, and choose **Remove Person** from the context menu.

Note that deleting a person will not prevent the record from being created anew when data containing it is imported. In particular, if the person is still present in Apple School Manager (ASM), updating the LANrev information from ASM will recreate the record.

Adding a person to a class

To add a person to a class as a teacher or student, drag it to the respective section of the class entry in the sidebar of the **Classroom Management** window:

- To assign a person as a teacher, drag it to **Teachers** > **Class Roster Assignments**.
- To assign a person as a student, drag it to **Students** > **Class Roster Assignments**.

Note that the role that is noted in the record of a person does not determine in what capacity they are added to a class. Thus you can add a student to a class as a teacher or a teacher as a student.

Removing a person from a class

To remove a person from a class:

1. In the sidebar of the **Classroom Management** window, click the as a student, drag it to **Students** > **Class** subsection of the section from which you want to remove the person – **Teachers** or **Students**.

   The persons from that section are displayed in the table area.

2. Right-click the person in the table area and choose **Remove Person from Group**.

LANrev removes the person from the class, but leaves it in the database and also leaves it assigned to other classes, if it is assigned to any.

Managing classroom devices

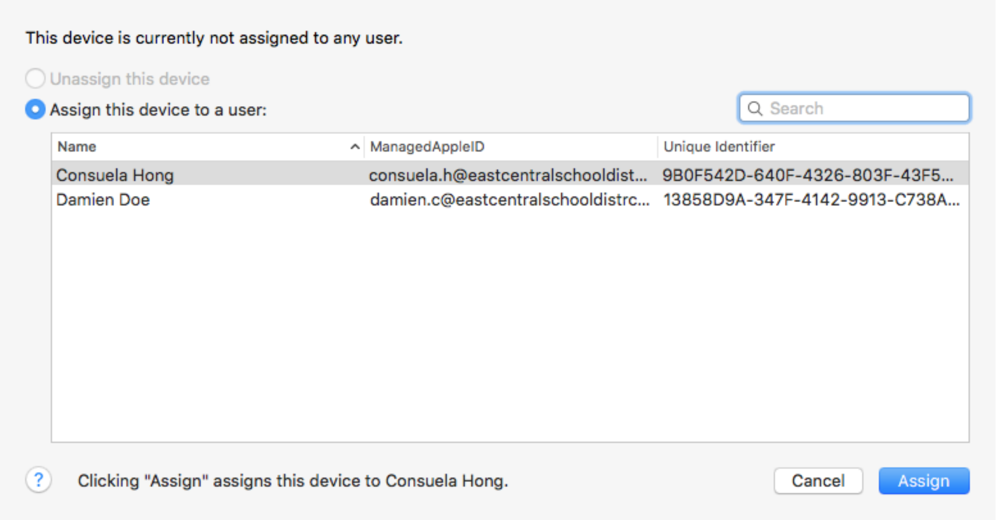
You can manage the assignment of devices in the **Classroom Management** window.

Assigning a personal device

To assign a device as a personal device to a user:

1. Right-click the device in the table area of the **Classroom Management** window and choose **Classroom Management** > **Manage Personal Device Assignment** from the context menu.

   The **Manage Personal Device Assignment** dialog opens:



This device is currently not assigned to any user.

○ Unassign this device

● Assign this device to a user:

Name	ManagedAppleID	Unique Identifier
Consuela Hong	consuela.h@eastcentralschooldist...	9B0F542D-640F-4326-803F-43F5...
Damien Doe	damien.c@eastcentralschooldistrc...	13858D9A-347F-4142-9913-C738A...

Clicking "Assign" assigns this device to Consuela Hong.

2. Click **Assign this device to a user** and choose the desired user from the list displayed in the dialog.

3. Click **Assign**.

LANrev marks the device as assigned to the chosen user.

Unassigning a personal device

You can assign a personal device to a different user or you can completely unassign it so that it is no longer assigned to any user as a personal device.

To assign a personal device to a different user, simply assign it to that user as described above. LANrev automatically unassigns it from its current user if any.

To completely unassign a personal device:

1. Right-click the device in the table area of the **Classroom Management** window and choose **Classroom Management** > **Manage Personal Device Assignment** from the context menu.

   The **Manage Personal Device Assignment** dialog opens.

2. Click **Unassign this device**.

3. Click **Assign**.

LANrev marks the device as not assigned to any user as a personal device.

Managing classes

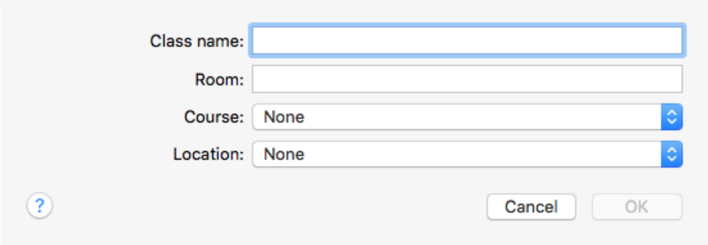
In the context of Apple School Manager, a class is a combination of instructors, students, a room, and a course.

Creating a class

To create a new class:

1. In the **Classroom Management** window, right-click the sidebar and choose **Classes** > **New Class** from the context menu.

   The **Class** dialog opens:



Class name:

Room:

Course: None

Location: None

2. Enter a name for the class.

3. Optionally, enter a room, a course, and/or a location.

   Courses and locations are chosen from a list; if the information you need is not on the list, you can add it using the **New Course** or **New Location** command, respectively

4. Click **OK** to save the new class.

Editing a class

To edit a class record:

1. Double-click the class entry in the **Classroom Management** window table area or right-click it in the sidebar and choose **Edit Class** from the context menu.

The **Class** dialog opens (see above), displaying the data of the class.

2. Edit the information as desired and click **OK**.

LANrev updates the record for the class with the specified information.

Deleting a class

To delete a class from the LANrev database, select the class in the **Classroom Management** window, right-click, and choose **Remove Class** from the context menu.

Note that deleting a class will not prevent the record from being created anew when data containing it is imported. In particular, if the class is still present in Apple School Manager (ASM), updating the LANrev information from ASM will recreate the record.

Configuring devices

When you have modified the classroom setup in LANrev, you must configure the affected devices for the changes to become effective.

You can either configure specific devices, or you can configure all devices of a class.

To configure specific devices:

1. In the **Classroom Management** window, select the devices you want to modify.

2. Right-click the selected devices and choose **Classroom Management** > **Configure Devices for Current Classroom Setup** from the context menu.

   A dialog is displayed in which you can choose to configure only the selected devices or the selected plus any related devices.

3. Unless you have a specific reason for configuring only the selected devices, click **Update Selected and Related**.

   Many changes can affect devices in addition to those who have been modified. If not all of those devices are updated as well, the overall configuration becomes inconsistent, and unexpected results may occur. Clicking **Update Selected and Related** ensures that the classroom configuration stays consistent across all devices.

LANrev transparently creates the required education profiles for all affected devices and applies them.

To configure all devices of one or more classes:

1. In the **Classroom Management** window, select the classes for which you want to update the devices.

2. Right-click the selected classes and choose **Classroom Management** > **Configure All Devices Used in Selected Classes** from the context menu.

LANrev transparently creates the required education profiles for all affected devices and applies them.

Working with shared devices

LANrev lets you manage shared devices, including setting mobile devices up to be shared. Shared devices must be iPads running iOS 9.3 or up with at least 32 GB of storage.

Working with shared mobile devices is described below in these sections:

- "Setting up shared devices" on page 276
- "Logging out a user of a shared device" on page 276
- "Deleting the local data of the user of a shared device" on page 276

Setting up shared devices

Mobile devices are configured to be shared as part of their enrollment process. They must be enrolled through the Apple device enrollment program (ADEP) and their status as shared must be declared in the device enrollment profile.

Using ADEP, including setting up device enrollment profiles, is described in "Using ADEP" on page 56.

Logging out a user of a shared device

Shared devices can have multiple configured and resident users, but only one user can be logged in at any time. You can log out this user from LANrev Admin:

1. In the **Mobile Devices** window, select the devices on which you want to log out users.

2. Right-click any selected device and choose **Shared Devices** > **Log Out User**.

   A confirmation alert is displayed. Clicking **Log Out** in this alert logs out the current user of the device.

Deleting the local data of the user of a shared device

Shared devices normally manage the data of their users automatically, deleting it from the device and reloading from iCloud as needed.

When required, you can use LANrev Admin to manually remove a user's data from the device:

1. If the users whose data you want to remove are still logged into the devices, log them out, as described in "Logging out a user of a shared device" on page 276.

   Data of users who are still logged in cannot be deleted.

2. In the **Mobile Devices** window, select the devices on which you want to remove user data.

   You can select multiple devices.

3. Right-click any selected device and choose **Shared Devices** > **Delete User Data**.

   A dialog is displayed.

4. Enter the Apple ID of the user whose data you want to remove.

5. If you want to delete data even if it is not yet synchronized with iCloud, check the **Delete data even when it is not yet backed up** option.

6. Click **OK** to remove the data.

IMPORTANT Deleting user data that has not yet been backed up may lead to irrecoverable data loss. Use this option only when you are certain that no important data can be lost.

The data is removed only locally on the device. It remains available in iCloud.

Working with Samsung KNOX

LANrev supports managing Samsung KNOX on compatible Android devices, including setting up and protecting workspaces as well as installing software and configuration profiles:

Working with KNOX devices is described below in these sections:

- "Setting up KNOX support" on page 278
- "Creating and removing KNOX workspaces" on page 278
- "Locking and unlocking KNOX workspaces" on page 278
- "Resetting the passwords of KNOX workspaces" on page 279
- "Using configuration profiles" on page 279
- "Managing KNOX apps" on page 280

Setting up KNOX support

To enable LANrev to work with KNOX on managed devices, you must specify your KNOX accounts:

1. In the **Server Center** window, click the **Server Settings** entry in the sidebar and click the **MDM** tab.

2. In the **Samsung KNOX licenses** section, click **Configure**.

   The **Samsung KNOX Licenses** dialog opens (which is described in “Samsung KNOX Accounts dialog” on page 794).

   Note that the **Configure** button is available only to administrators with the **Modify Samsung KNOX Accounts** privilege.

3. Click the **+** button to add an account. Specify the name and license key in the lower part of the dialog.

4. Repeat this process for any additional accounts you want to specify and then click **OK**.

You can now use LANrev to assign managed mobile devices to these accounts.

Creating and removing KNOX workspaces

To create or remove KNOX workspaces:

1. Select the mobile devices in the **Mobile Devices** window.

2. Right-click the devices and choose the desired command from the context menu:

   - To create KNOX workspaces on the devices, choose **Create KNOX Workspace** and specify the account to which the workspaces belong. Devices that do not support KNOX are unaffected by this command.
   - To remove existing KNOX workspaces from the devices, choose **Remove KNOX Workspace**. This also removes any KNOX applications, data stored by these applications, and KNOX configuration profiles. Devices without a KNOX workspace are unaffected by this command.

   The two commands are also available from the **Commands** menu.

Locking and unlocking KNOX workspaces

You can lock KNOX workspaces and unlock them again:

1. Select the mobile devices in the **Mobile Devices** window.

2. Right-click the devices and choose the desired command from the context menu:

- To lock any KNOX workspaces on the devices, choose **Lock KNOX Workspace**. Devices on which there is no KNOX workspace are unaffected by this command.
- To unlock all locked KNOX workspaces on the devices, choose **Unlock KNOX Workspace**. Devices without a locked KNOX workspace are unaffected by this command.

The two commands are also available from the **Commands** menu.

A locked KNOX workspace is inaccessible from the device: The local user can access neither the KNOX apps nor their data. Unlocked workspaces are accessible normally, that is, after entering their passwords.

Resetting the passwords of KNOX workspaces

If the user of a mobile device with a KNOX workspace has forgotten the workspace's password, you can reset the password:

1. Select the mobile devices in the **Mobile Devices** window.

2. Right-click the devices and choose **Reset KNOX Workspace Password**.

   Devices on which there is no KNOX workspace are unaffected by this command. The command is also available from the **Commands** menu.

Resetting the password removes the existing password from the workspace. When the user next tries to access the workspace, he or she is prompted to specify a new password before access is granted.

Note that resetting a KNOX password temporarily removes the password protection: Anybody with physical access to the device can also access the KNOX workspace until a new password has been specified.

Using configuration profiles

Configuration profiles for KNOX workspaces are handled just like any other profile by LANrev:

- To create a configuration profile for a KNOX workspace, proceed like for any other profile, specifying "Samsung KNOX" as the profile type when you choose **New Configuration Profile**.
  Creating new configuration profiles or importing existing profiles created elsewhere is described in "Creating or importing configuration profiles" on page 182.
- You do not need to do anything special to install KNOX configuration profiles: LANrev automatically recognizes the profile type and installs such profiles in the KNOX workspaces. (It is not possible to install KNOX profiles outside of workspaces or install non-KNOX profiles in KNOX workspaces.)

Installing and removing configuration profiles is described in “Overview of installing configuration profiles on mobile devices” on page 186.

Managing KNOX apps

Android apps can be installed in KNOX workspaces like they are installed on standard Android devices.

When you install an Android application or when you add it to a policy for automated installation, you can choose whether to install it as a standard Android application or in KNOX.

Note that, when you choose to install an app in KNOX, it will not be installed on any selected devices that do not contain a KNOX workspace.

Working with mobile apps is described in “Installing software on mobile devices” on page 197.

Creating placeholder records for mobile devices

In general, LANrev can only work with mobile devices which have been enrolled in MDM administration. However, a very limited subset of the functionality is also available for devices that have not yet been enrolled.

To use this capability, you must manually create a placeholder record for each mobile device in question, as explained below.

Functions available for placeholder records are limited to:

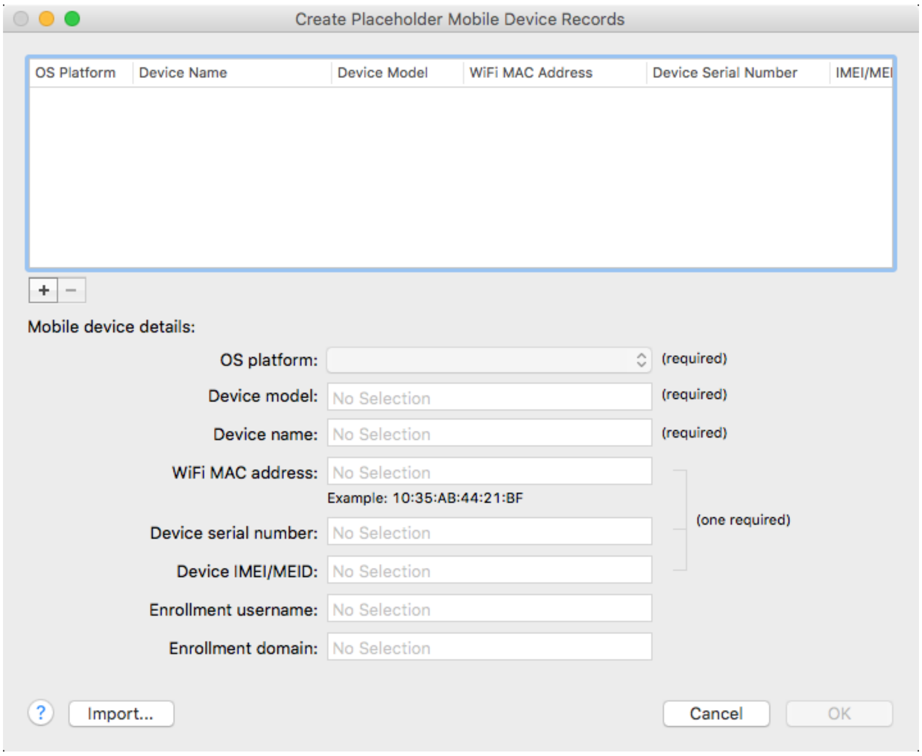
- Displaying them in browser windows. No information is displayed beyond the data that was entered when the placeholder record was created.
  Display-related functions of browser windows – such as sorting, finding, or exporting – also extend to placeholder records, but functions that actually access the device – such as gathering information or sending commands – do not.
- Assigning them to mobile device policies (which is done in the same way as with actually enrolled devices) so that the devices are immediately assigned the desired configurations when they enroll.

Creating placeholder records for mobile devices

To create placeholder records for one or more mobile devices that have not yet been enrolled in the MDM:

1. Choose **Server** > **Create Placeholder Mobile Device Records**.

The **Create Placeholder Mobile Device Records** dialog opens:



2. Click the **+** button.

   The entry fields in the dialog become active.

3. Enter the information for the placeholder record you are about to create.

   The enrollment username and domain are optional, all other information is required. (Although you need only specify one of the MAC address, the serial number, and the IMEI/MEID number and can omit the other two.)

   Instead of manually entering the information from each record, you can also click the **Import** button to import the data from a tab-delimited text file. The file format is described in “Create Placeholder Mobile Device Records” on page 494.

4. To create additional placeholder records, repeat step 2 and 3.

5. Click **OK** to save the placeholder records displayed in the dialog.

Deleting placeholder records

To delete existing placeholder records:

1. In any browser window, select the records you want to delete.

2. Right-click the selected records and choose **Remove from Server** from the context menu.

The records are deleted after you have confirmed that you want to do so.

Chapter 7 Working with files

LANrev includes a range of functions for working with files on administered computers. You can copy, move, delete, rename, and open files as well as create aliases and folders. You can also transfer files from your computer to administered computers.

These functions are described in:

- “Copying and moving files” on page 283
- “Deleting files” on page 284
- “Renaming files” on page 285
- “Opening files on administered computers” on page 286
- “Viewing files from administered computers” on page 286
- “Creating aliases for files” on page 288
- “Creating folders” on page 289
- “Transferring files to administered computers” on page 290

Several file-related operations are described elsewhere in this manual:

- Distributing documents and media to managed mobile devices is described in “Distributing media to mobile devices” on page 221.
- Distributing software to administered desktop computers is described in “Installing software” on page 293.
- Distributing software to managed mobile devices is described in “Installing software on mobile devices” on page 197.
- Working with the registries of Windows computers is described in “Editing the registry” on page 174.

NOTE It is easier to work with files that are listed in the Files table of the LANrev database. Searching for files to include them in the database is described in “Gathering information on files” on page 102.

Copying and moving files

LANrev lets you copy or move files on administered computers to a different location on the same computer.

To move or copy files:

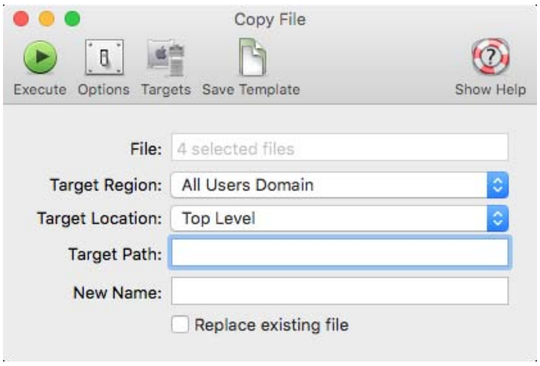
1. In any browser window showing files, select the files that you want to copy or move.

   Note: If you would rather specify the computers first or if the file is not available in the LANrev database, there is an alternative method for specifying the command target that is described in “An alternative method of specifying files” on page 292.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Copy File/Folder** or **Move File/Folder**, depending on the desired action.

   The **Copy File** or the **Move File** dialog opens. Both dialogs are very similar; the **Copy File** dialog is shown here:



File: 4 selected files
Target Region: All Users Domain
Target Location: Top Level
Target Path:
New Name:
□ Replace existing file

   Note: If you have selected only a single file, the path of that file is displayed in the **File** *field.*

3. Choose the target region and location and enter the path where the files are to be copied or moved.

   The available target regions and locations are discussed in “Copy File/Folder” on page 441.

4. If you want to give the copied or moved files new names, enter the desired new name.

   Note: If you have selected more than one file from the same target computer, trying to rename files will lead to errors.

5. If you want the copied or moved files to replace any files in the target folder that have the same name, check **Replace existing file**.

IMPORTANT Deleted file cannot be recovered, short of using specialized tools that may or may not be successful.

6. Click **Execute**.

LANrev copies or moves the files as specified. Any errors are noted in the command history.

Deleting files

You can use LANrev to delete files on administered computers.

IMPORTANT Deleted files cannot be recovered, short of using specialized tools that may or may not be successful.

To delete files:

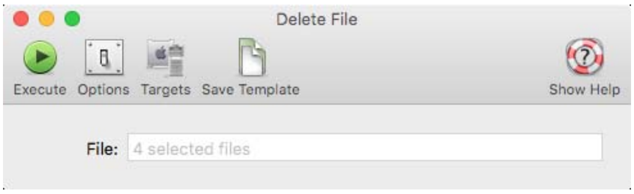
1. In any browser window showing files, select the files that you want to delete.

   Note: If you would rather specify the computers first or if the file is not available in the LANrev database, there is an alternative method for specifying the command target that is described in "An alternative method of specifying files" on page 292.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Delete File/Folder**.

   The **Delete File** dialog opens:



File: 4 selected files

   Note: If you selected only a single file, the path of that file is displayed in the **File** *field.*

3. Click **Execute**.

LANrev deletes all specified files immediately; there is no confirmation, and files are not just moved to the Trash.

Renaming files

LANrev lets you rename files on administered computers.

To rename files:

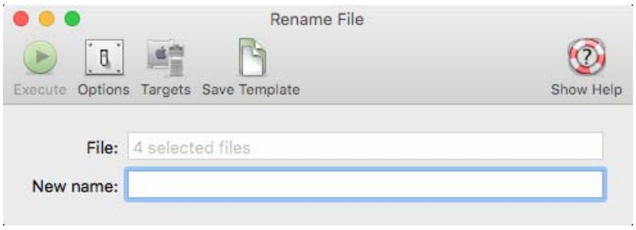
1. In any browser window showing files, select the files that you want to rename.

   Note: If you would rather specify the computers first or if the file is not available in the LANrev database, there is an alternative method for specifying the command target that is described in "An alternative method of specifying files" on page 292.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Rename File/Folder**.

The Rename **File** dialog opens:



File: 4 selected files

New name:

Note: If you selected only a single file, the path of that file is displayed in the **File** *field.*

3. Enter the new name for the files.

   Note: If you have selected more than one file from the same directory on the same computer, trying to rename them will lead to errors.

4. Click **Execute**.

LANrev renames the files.

Opening files on administered computers

You can use LANrev to open files on administered computers locally, that is, on the computers on which they reside. Since these files can be not only documents but also scripts and applications, this feature provides a way to perform some maintenance tasks.

This is described in "Executing local files" on page 170.

Viewing files from administered computers

Many kinds of files from administered computers can be viewed on administrator workstations. This includes any kind of text file (such as pure text, HTML, or code files) as well as standard types of system logs.

To view a file on one or more administered computers:

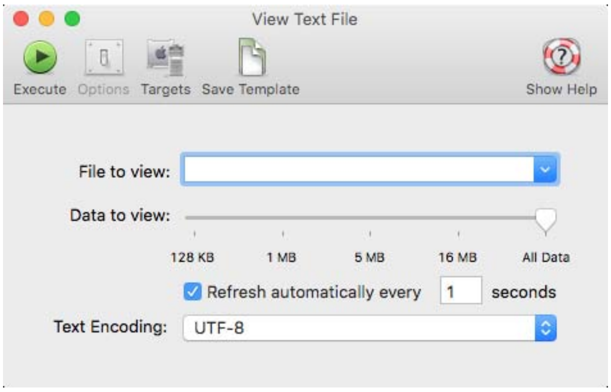
1. In any browser window, select the computers on which you want to view files.

   Note: If you select files in an LANrev browser window before choosing the **View Text File** *command, those files are pre-entered into the "***File to view"** *field (see below).*

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **View Text File**.

The **View Text File** dialog opens:



File to view:

Data to view: 128 KB 1 MB 5 MB 16 MB All Data

☑ Refresh automatically every 1 seconds

Text Encoding: UTF-8

3. To specify the file you want to view, do one of the following:

   - Enter the file’s full path in the **File to view** field.
     For macOS files, you can use the tilde (~) to refer to the current user’s home directory.
     For files on Windows target computers, you can use variables in the path.
   - Drag the file from any LANrev browser window to the **File to view** field, making sure to put the text insertion mark in the field first.
   - Choose one of the predefined files from the pop-up menu.

4. If you are specifying a large file and do not want to view all of it, use the Data to view slider to restrict the amount of data from the file that LANrev is to display. LANrev displays the specified amount of data at the end of the file.

5. To automatically refresh the file display in regular intervals, check the **Refresh automatically** option and specify the desired interval.

6. Choose the text encoding of the file you are about to view.

   Note: Normally, we recommend that you choose UTF-8, which includes automated line-by-line checking of the actual encoding with conversion performed as required.

7. Click **Execute**.

LANrev displays the content of the file in a new window on your workstation. If you have added multiple computers to the target list, the files at the specified location on all computers are displayed, each in its own window.

You can search the displayed files using the commands from the Find submenu or filter the displayed lines using the filter field at the top of the window. You can also save entire files to disk.

Creating aliases for files

LANrev lets you create aliases of files (shortcuts on Windows) on administered computers in any location on the same computer.

To create aliases of files:

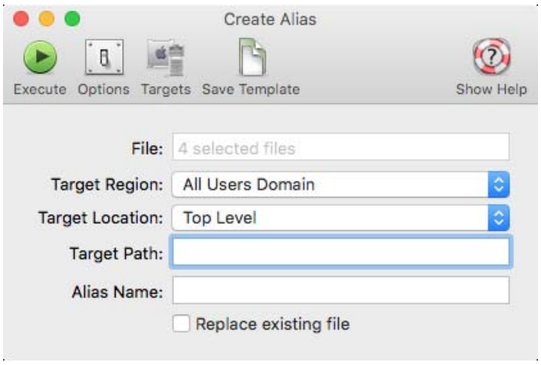
1. In any browser window showing files, select the files of which you want to create aliases.

   Note: If you would rather specify the computers first or if the file is not available in the LANrev database, there is an alternative method for specifying the command target that is described in "An alternative method of specifying files" on page 292.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Create Alias**.

   The **Create Alias** dialog opens:

   File: 4 selected files
   Target Region: All Users Domain
   Target Location: Top Level
   Target Path:
   Alias Name:
   □ Replace existing file

   Note: If you had selected only a single file, the path of that file is displayed in the **File** *field.*

3. Choose the target region and location and enter the path where the aliases are to be created.

   The available target regions and locations are discussed in "Copy File/Folder" on page 441.

4. If you want to give the aliases names that are different from the default names created by the operating system, enter the desired new name.

   Note: If you have selected more than one file from one target computer, trying to name the aliases will lead to errors.

5. Click **Execute**.

LANrev creates the aliases at the indicated locations on the same computers as the specified files.

Creating folders

LANrev lets you create new folders on administered computers in any desired location.

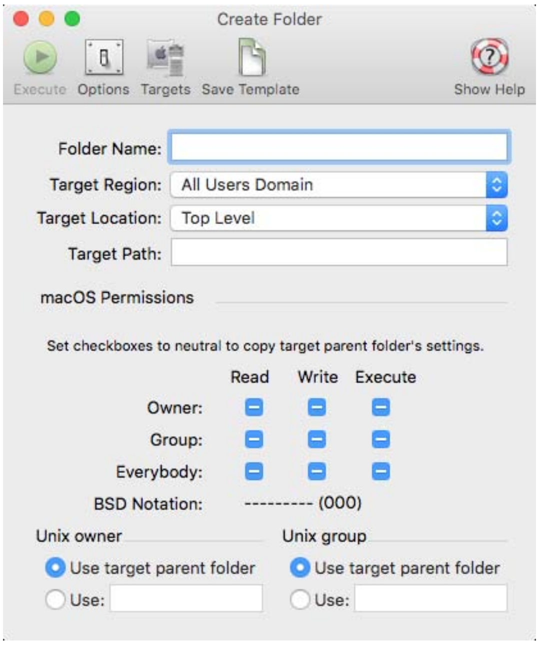
To create folders:

1. In any browser window showing files, select the computers on which you want to create the folders.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Create Folder**.

   The **Create Folder** dialog opens:



Folder Name:

Target Region: All Users Domain

Target Location: Top Level

Target Path:

macOS Permissions

Set checkboxes to neutral to copy target parent folder's settings.

	Read	Write	Execute
Owner:	⊟	⊟	⊟
Group:	⊟	⊟	⊟
Everybody:	⊟	⊟	⊟

BSD Notation: --------- (000)

Unix owner
● Use target parent folder
○ Use:

Unix group
● Use target parent folder
○ Use:

3. Choose the target region and location and enter the path where the folders are to be created.

   The available target regions and locations are discussed in "Copy File/Folder" on page 441.

4. If you create folders on macOS computers, specify their access permissions, owner, and group.

   In each case, you can choose between letting the folders inherit these settings from their parent folder or providing an explicit setting.

5. Click **Execute**.

LANrev creates the folders at the indicated locations.

Transferring files to administered computers

You can use LANrev to transfer files from your workstation to any location on administered computers.

This feature is primarily intended to allow you to quickly replace damaged files or provide missing files and perform similar support tasks. While you can use it to perform software installations as well, that is not its main intended application; we recommend that you check out the Software Distribution Center for software distribution, as described in "Installing software" on page 293.

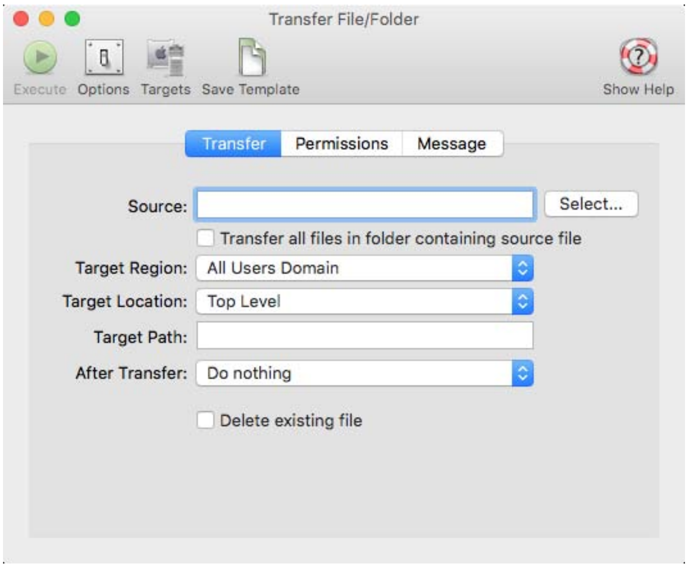
To transfer a file or folder from your workstation to administered computers:

1. In any browser window showing files, select the computers to which you want to transfer the files.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Transfer File/Folder**.

   The **Transfer File/Folder** dialog opens:



Source:

□ Transfer all files in folder containing source file

Target Region: All Users Domain

Target Location: Top Level

Target Path:

After Transfer: Do nothing

□ Delete existing file

3. Specify the file, folder, or macOS disk image that you want to transfer, either by entering the path in the **Source** field or by clicking the **Select** button and choosing the desired object.

4. If you have selected a file, you can check the **Transfer all files in folder containing source file** option to transfer the entire contents of the folder in which the selected file is located to the target computers.

   If this option is not checked, only the file itself is transferred.

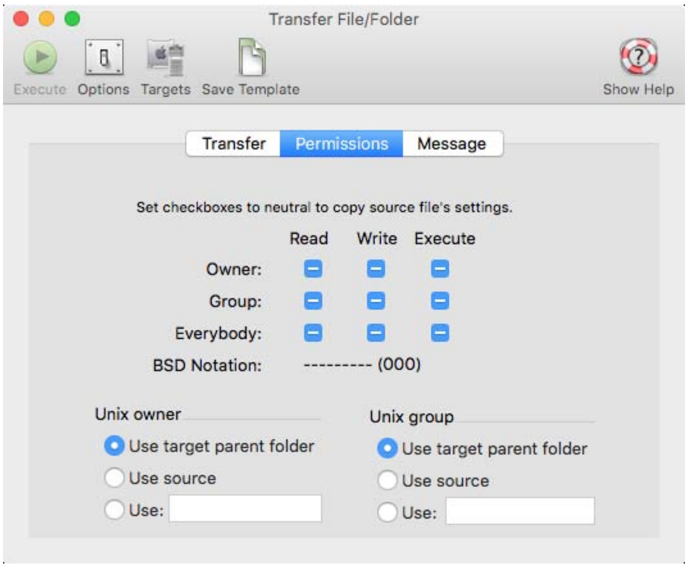
5. If you have selected a disk image, you can check the **Transfer contents of disk image** option to transfer the contents of the selected disk image file instead of the file itself.

   In this case, the target settings in the dialog pane become unavailable; the files from the disk image are always copied to the boot volume at the same paths they have on the disk image.

6. Choose the target region and location and enter the path where the folders are to be created.

   The available target regions and locations are discussed in “Copy File/Folder” on page 441.

7. If you copy the file or folder to macOS computers, click the **Permissions** tab to specify the access permissions, owner, and group.



Set checkboxes to neutral to copy source file's settings.

	Read	Write	Execute
Owner:	⊟	⊟	⊟
Group:	⊟	⊟	⊟
Everybody:	⊟	⊟	⊟
BSD Notation:	--------- (000)		

Unix owner
● Use target parent folder
○ Use source
○ Use:

Unix group
● Use target parent folder
○ Use source
○ Use:

   For owner, group, and each permission, you can choose between letting the folders inherit the setting from the source item on your computer or providing an explicit setting. For owner and group, you can also let the item inherit the setting from the enclosing folder on the target computer.

8. If you want to send a message to the user before the transfer begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “Sending messages” on page 144.

   If you provide a **Cancel** button in the message dialog, the transfer is aborted on a target computer if a user clicks **Cancel**.

   Note: If a message has been specified, this is indicated by a diamond in the dialog’s **Message** *tab.*

9. Click **Execute**.

LANrev transfers the file or folder to the indicated location on the target computers. Any errors are noted in the command history.

An alternative method of specifying files

The file-manipulating procedures in this chapter all assume that you are specifying the desired files by selecting them in the **Files** window or another browser window displaying files and then adding the target computers (if there is more than one target).

Sometimes, it is easier to start with specifying the computers first and then entering the path of the file. In this case, the file does not need to be in the Files table of the LANrev database, meaning that you do not have to search for it before being able to manipulate it.

NOTE This procedure does not work on multiple files at the same time.

To use this alternative method of working with files:

1. In any browser window, select the computers on which you want to manipulate the files.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose the desired file-related command.

   The command's dialog opens.

3. In the **File** field, enter the path of the file.

4. Proceed with specifying the command options and executing the command, as described in the respective procedures.

Chapter 8

Installing software

While you can use LANrev to manually install software on administered computers (see below), it really shines when you use the Software Distribution Center to automatically distribute software to any number of computers.

The Software Distribution Center can automatically install a specific range of applications on new computers as soon as they are put on the network. Or you can use it to distribute newly introduced or updated applications to specific workgroups or the organization.

NOTE Installing software on administered mobile devices works differently and does not use the Software Distribution Center. See “Installing software on mobile devices” on page 197 for details.

Using the Software Distribution Center is explained in:

- “Overview” on page 294
- “Setting up distribution points” on page 296
- “Setting up payloads” on page 302
- “Setting up software packages” on page 304
- “Setting up metapackages” on page 312
- “Exporting and importing software packages and metapackages” on page 318
- “Managing volume purchases of Mac App Store apps” on page 319
- “Managing VPP licenses for computer applications” on page 321
- “Setting up computer groups” on page 324
- “Performing installations” on page 331
- “Performing ad hoc installations” on page 332
- “Automated patch management” on page 333
- “Reinstalling a macOS computer” on page 336
- “Reinstalling a Windows computer” on page 340

Creating installer packages

The Software Distribution Center is designed to work with software installer packages. You can create such packages with the LANrev InstallEase companion tool that is included with LANrev.

See the tool’s documentation for details on its use.

Installing software manually

While the Software Distribution Center is a powerful tool for software rollouts and other repeated installations, it is not always the optimal tool. When you just want to distribute a few files or do a one-off installation, other LANrev functions are usually quicker:

- To copy individual files to one or more administered computers, we recommend using the **Transfer File/Folder** command, as described in “Transferring files to administered computers” on page 290.
- To run an installer application on one or more administered computers (if you do not plan to do so repeatedly), you can use the **Execute macOS File** or **Execute Windows File** commands, depending on the target platform. They are described in “Executing files from your computer” on page 167.

Monitoring installed software

LANrev lets you monitor which software is installed on client computers. This is not done by evaluating the log of software installations through LANrev but by scanning the computers for software and installer receipts. The process is described in “Manually gathering information on installed software” on page 100.

Overview

The Software Distribution Center is a module of LANrev Server that offers automatic server-based software distribution. It is controlled from the **Server Center** window.

This section explains the basics of the Software Distribution Center structure, setup, and use. It also includes references to detailed instructions.

Prerequisites

Some features of the Software Distribution Center can be used only by administrators whose accounts have certain rights set.

Configuring administrator accounts is described in “Administrator accounts” on page 72.

Structure

The software distribution system has four key components:

- **Distribution points** are servers that host the files to be installed. There can be any number of distribution points, allowing you to place them in a way that minimizes network traffic.
  One of the distribution points is defined as the master; all others are mirror servers. The software installers present on the master distribution point are automatically distributed to the mirror servers so that all distribution points always have the same range of software available without requiring any manual maintenance.

There is comparatively little network traffic to a LANrev server (in its capacity as the Software Distribution Center) as it does not itself distribute the software installers.
- **Payloads** are files or folders that are to be installed. They can be created from local files but are always stored on distribution points.
- **Software packages** are combinations of references to payloads with metadata regarding the target requirements and scheduling of the installation.
  Software packages come in two flavors: Standard packages contain payloads, while metapackages contain other software packages (including metapackages).
- **Computer groups** are collections of computers on which the same software will be installed.

When these components are set up, the actual installation is almost completely automatic, requiring you only to indicate which software packages are to be installed in which computer groups.

Setup

Setting up the Software Distribution Center consists mainly of defining the key components – distribution points, payloads, software packages, and computer groups. This is done in the LANrev Admin’s **Server Center** window, as described in the following sections:

- “Setting up distribution points” on page 296
- “Setting up payloads” on page 302
- “Setting up software packages” on page 304
- “Setting up computer groups” on page 324

Only in some cases do you need to configure agents:

- Where you have assigned more than one LANrev server to some or all agents. This requires you to specify for each agent which of the LANrev servers is to act as the software distribution server. This is necessary because, while any number of inventory servers can be assigned to one agent, each agent may have only one software distribution server.
- Where the software distribution server is not the inventory server (that is, main LANrev server) assigned to the agent.

In this case, you need to explicitly assign the desired software distribution server to the agent using the **Agent Settings** command. This is described in “Assigning software distribution or license monitoring servers to agents” on page 81.

You can use the same command to specify the interval in which the agent queries the software distribution server for new software.

Setting up distribution points

Distribution points are computers designated to hold software installers for the Software Distribution Center and distribute them to agents.

Distribution point basics

Any macOS or Windows computer can be used as a distribution point. A folder on this computer must be specified in which the software installers will be kept for distribution to clients.

LANrev Agent must be installed on each distribution point. The software distribution server setting must be correctly specified on each of these agents (using the **Servers** tab in the **Agent Settings** dialog): It must point to the main LANrev server.

One of the distribution points is set to be the master. All payloads are initially uploaded only to this master distribution point by LANrev Admin. LANrev then distributes the packages transparently in the background to the other distribution points, called mirrors.

Choosing a server as a distribution point

For reasons of reliability and performance we strongly recommend to use only dedicated servers as distribution points, that is, computers on which only server processes are running and that are not used as workstations by local users.

NOTE Make sure to update the LANrev agent on a distribution point computer to the latest version (or the same version as that of LANrev Server). Otherwise, you may experience difficulties in distributing software.

There is no problem in principle in letting a distribution point run on the same computer as LANrev Server.

LANrev's support for multiple distribution points lets you – if the hardware is available – to place distribution points throughout your network, close to the served workstations. Ideally, each network zone would have its own distribution point to minimize interzone traffic.

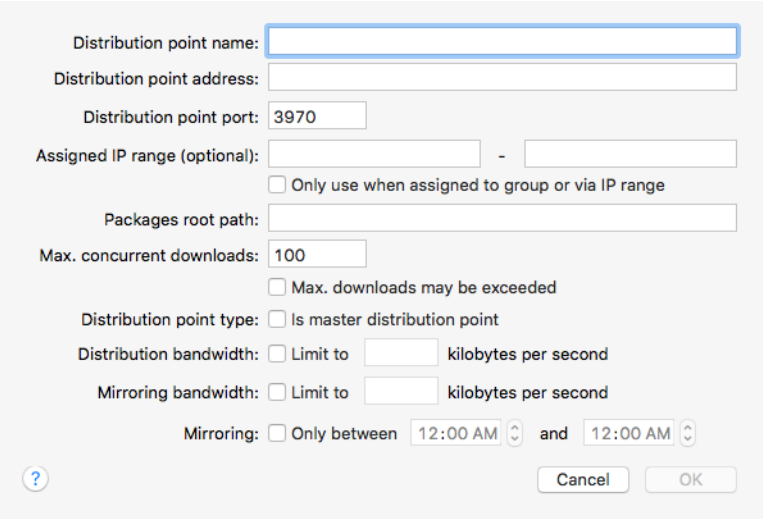
NOTE As the software distribution server – the central LANrev server – creates a low amount of traffic, there is no significant performance penalty in having just a single such server.

Specifying the distribution point in the Software Distribution Center

To make the distribution point available in the Software Distribution Center:

1. From the action menu of the **Server Center**, choose **New Distribution Point**.

   The **Distribution Point** dialog opens:



Distribution point name:

Distribution point address:

Distribution point port: 3970

Assigned IP range (optional): -

□ Only use when assigned to group or via IP range

Packages root path:

Max. concurrent downloads: 100

□ Max. downloads may be exceeded

Distribution point type: □ Is master distribution point

Distribution bandwidth: □ Limit to kilobytes per second

Mirroring bandwidth: □ Limit to kilobytes per second

Mirroring: □ Only between 12:00 AM and 12:00 AM

2. Enter the desired name in the **Distribution point name** field.

   This name is used only inside the LANrev system; you can choose whatever name you like.

3. Enter the distribution point address – either the IP number or the DNS name – and the port on which LANrev Agent on the distribution point communicates.

   Note: We recommend that you do not change the default port unless you have a specific reason for doing so.

4. In a setup with multiple distribution points, any distribution point can normally serve any agent. If you want to restrict a distribution point to a certain group of clients (for example, one particular satellite office), specify a range of IP addresses in the **Assigned IP range** fields.

   Note: You can also assign a distribution point to a computer group, making it the preferred distribution point for downloads from computers in that group. To assign a distribution point to a group, click the Distribution Points icon in the Server Center window after you have completed specifying the distribution point and drag it to the desired computer group.

5. Set the **Only use when assigned to group or via IP range** option as desired:

- If the option is checked, the distribution point only serves clients to which it has been assigned, irrespective of any settings in the packages it serves.
- If the option is unchecked, the distribution point may also serve clients to which is has not been expressly assigned, with software packages:
  - Where the distribution point is set to “Any”.
  - Where the distribution point is set to “From assigned distribution point if available” and no distribution point assigned to the client is available.

6. Enter the path of the folder in which LANrev is to store the software installers on this distribution point.

   Note: The contents of this folder is managed entirely by LANrev. Do not manually delete from or add to this folder.

7. Specify the maximum number of concurrent software downloads (agents downloading the software installers) the distribution point will provide.

   If you want this limit to be exceedable in cases where an agent wants to download an installer but no distribution point has available download slots, check **Max. downloads may be exceeded**.

   If the option is unchecked, the download attempts by the agent will be deferred in situations where no distribution point has download capacity. That means that the software installation on the clients concerned will still happen, only at a later time.

8. If you want this distribution point to be the master distribution point, check the **Is master distribution point** option.

   If the option is unchecked, the distribution point will become a mirror that receives all its software installers automatically from the master distribution point.

   There must always be exactly one master distribution point. Because the master distribution point must be up and running for the proper functioning of the software distribution and because it receives more traffic than mirror distribution points, we recommend that you designate a reliable computer with high-bandwidth network connections as the master distribution point.

9. If you want to limit how much network bandwidth is used for downloads from this distribution point to clients, check the **Distribution bandwidth** option and enter the desired limit.

10. If you want to limit how much network bandwidth is used for mirroring between this distribution point and the master distribution point, check the **Mirroring bandwidth** option and enter the desired limit.

You cannot limit the mirroring bandwidth for the master distribution point.

11. If mirroring is to be limited to a certain time of the day (for example, after hours), check the **Only between** option and enter the desired interval.

    Note: Because of a limitation in the operating system, midnight at the end of the day cannot be specified as "24:00" when using a 24-hour clock. Enter "0:00" instead.

    You cannot limit the mirroring period for the master distribution point.

12. Click **OK** to close the dialog.

13. To store the distribution point specification on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

    You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new distribution point becomes available to the Software Distribution Center only after you have done so.

Editing distribution points

To edit an existing distribution point definition:

1. Select the server in the **Server Center** window and choose **Edit Distribution Point** from the action menu.

   The **Distribution Point** dialog opens.

2. Make the desired changes and click **OK**.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Changing the master distribution point

There must always be exactly one master distribution point in the software distribution system. Changing it – designating a different distribution point as the master – therefore requires a specific procedure. The exact steps are different depending on whether the new server has been used as a mirror distribution point before or not.

If the new server already is a mirror distribution point:

1. Make sure that the intended new master distribution point has all the software that the current master distribution point has.

   If you have recently made changes to payloads or have created new ones, you may want to compare the total size of the contents of the package root folders on the computers.

2. Edit the existing master distribution point specification as described in **Editing distribution points**, above. Uncheck the **Is master distribution point** option and click **OK**.

3. Edit the specification for the intended new master distribution point in the same way, checking the **Is master distribution point** option.

   LANrev displays a dialog informing you of options to transfer the required payloads.

4. Click the **Manually Copy Folder** button.

   You do not actually need to copy anything as all required installers are already present on the new master distribution point.

5. From the Server menu, choose **Save Distribution and Licensing Info** to upload the new definitions to LANrev Server.

The new master distribution point is now active; the previous master distribution point is now a mirror distribution point.

If the new master distribution point has not been used as a distribution point so far:

1. Make sure that LANrev Agent is installed on the intended new master distribution point.

2. Manually create the package root folder on the intended new master distribution point.

3. Copy the entire contents of the package root folder from the existing master.

   Note: There is an alternative process for switching master distribution points in which LANrev Admin re-uploads all the payloads. If you want to follow that process, make sure that the source files for all payloads are available on your computer. Note, however, that all automatically created software patches are lost in this procedure and must be redownloaded from Apple's and Microsoft's servers. Delete all these patches from the Software Distribution System before switching the server.

4. Define the new master distribution point as described in **Specifying the distribution point in the Software Distribution Center**, above. Make sure to check the **Is master distribution point** option.

5. Edit the existing master server specification as described in **Editing distribution points**, above. Uncheck the **Is master distribution point** option and click **OK**.

   LANrev displays a dialog informing you of options to transfer the required software installers.

6. Click the **Manually Copy Folder** button.

   You do not actually need to copy anything now as you have already done so in step 3, above.

   Note: If you follow the alternative procedure, click the **Re-Upload Payloads** *button.*

7. From the **Server** menu, choose **Save Distribution and Licensing Info**.

   If you follow the alternative method, LANrev Admin will now attempt to upload the source files for all payloads to the new master distribution point. If this does not succeed for all payloads, LANrev Admin notifies you of the fact and marks all payloads that could not be uploaded as “Source missing” in the **Upload Status** column.

   Note: You may need to add the column to the **Server Center** *window to see the information.*

   Open each failed payload and respecify the source file. When you are done, choose **Save Distribution and Licensing Info** again.

The new master distribution point is now active; the previous master distribution point is now a mirror. If you have chosen to re-upload payloads, it may take a while before the distribution point is ready, depending on the number and size of the payloads.

Removing distribution points

To remove an existing distribution point definition:

1. Select the distribution point in the **Server Center** window and choose **Remove Distribution Point** from the action menu.

   A confirmation message is displayed.

2. Confirm the decision.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

   Until you do this, the distribution point is still available.

NOTE Before you can remove the last remaining distribution point, you must delete all computer groups, payloads, software packages, and disk images in the Software Distribution Center.

Setting up payloads

Payloads are files or folders that are to be installed on the client computers. Payloads are stored on distribution points and referenced in installation packages.

NOTE Due to limitations of the Windows operating system, payloads for macOS clients must be created on administrator computers running macOS.

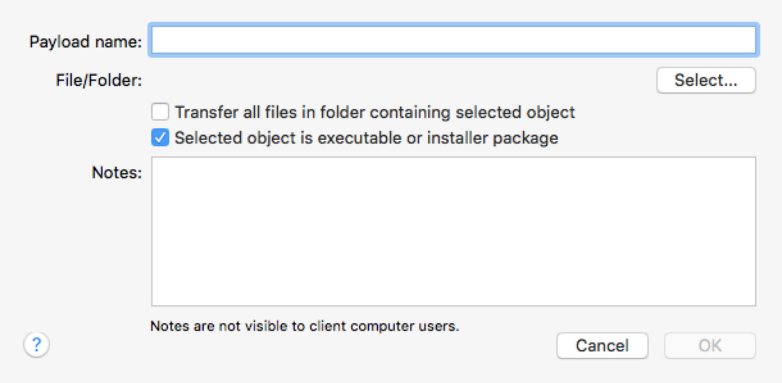
NOTE Setting up payloads is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 758 for details.

To set up a payload:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu, choose **Software Distribution** > **New Payload**.

   The **Payload** dialog opens:



Payload name:

File/Folder:

□ Transfer all files in folder containing selected object

☑ Selected object is executable or installer package

Notes:

Notes are not visible to client computer users.

3. Enter the desired name in the **Payload name** field.

   This is the name by which the payload will be known in LANrev; you can choose whatever name you like.

4. Click the **Select** button and specify the file or folder to install.

   If you want to create a package for macOS targets, you must do so on a macOS computer.

   Note: You can use LANrev InstallEase to create custom installers.

   You can specify a disk image (created manually or with LANrev InstallEase) as the file. In that case, any files in the disk image are copied to the same locations on the target hard disk; any missing folders are automatically created by LANrev.

5. If the specified file is not self-contained – that is, if it requires additional files to be present, as is usually the case for MSI installers – make sure that these files are located in the same folder as the installer and check **Transfer all files in folder containing executable**.

6. If the selected file is an application, a system script, or an installer package, check **Selected object is executable or installer package**.

7. Optionally you can enter a short description of the package in the **Notes** field.

8. Click **OK** to close the dialog.

9. To store the payload on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu. LANrev uploads the payload to the master distribution point, compressing and encrypting it in the process. It also creates a checksum that is verified by agents during installations. When the payload has been successfully uploaded to the master server, its specification is stored on LANrev Server. Mirroring to any additional distribution points happens automatically in the background.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new software package becomes available to the Software Distribution Center only after you have done so.

Editing payloads

To edit existing payloads:

1. Select the payload in the **Server Center** window and choose **Edit Payload** from the action menu.

   The **Payload** dialog opens.

2. Make the desired changes and click **OK**.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Removing payloads

To remove existing payloads:

1. Select the payloads in the **Server Center** window and choose **Remove Payloads** from the action menu.

   A confirmation message is displayed.

2. Confirm the decision.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

   Until you do this, the payloads are still available.

Setting up software packages

Software packages are combinations of references to payloads on a distribution point and additional metadata. They represent a software installation within the Software Distribution Center.

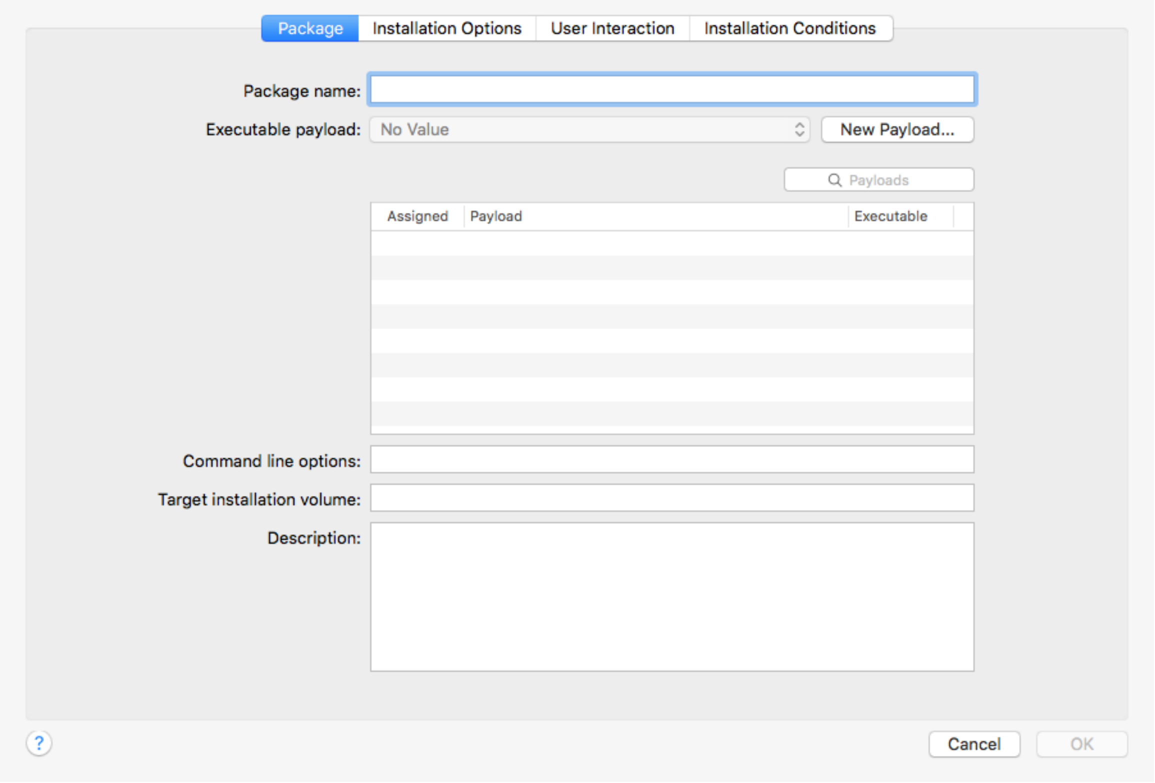
NOTE Setting up software packages is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 758 for details.

To set up a software package:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu, choose **New Software Package**.

   The **Software Distribution Package** dialog opens:



In the **Package** tab, you specify the payloads to be used.

Note: Never use the LANrev Agent updater as the payload in packages you generate. LANrev automatically generates update packages for agents, and you must only use those packages. See "Updating the Agent" on page 62 for details on updating agents.

3. Enter the desired name for the software package in the **Package name** field. Optionally you can also enter a short description of the package in the **Description** field.

   This name is used only inside the LANrev system; you can choose whatever name you like.

4. Specify the payloads that are to be included in the package.

   All payloads that are available on the distribution points are listed in the dialog pane.

   You can add new payloads by clicking the **New Payload** button; proceed as described in "Setting up payloads" on page 302.

   You can filter the displayed payload by entering parts of their names in the search field above the list of payloads.

   Check all payloads that are to be included in the package.

5. From the **Executable payload** pop-up menu, choose the executable payload of the package.

   There must always be exactly one executable payload in each package, This is the payload that is launched by the agent after all payloads have been copied to the target computer.

6. Optionally, you can specify command-line options in the **Command line options** field.

   You can include environment variables in the options, as described in "Environment variables" on page 176.

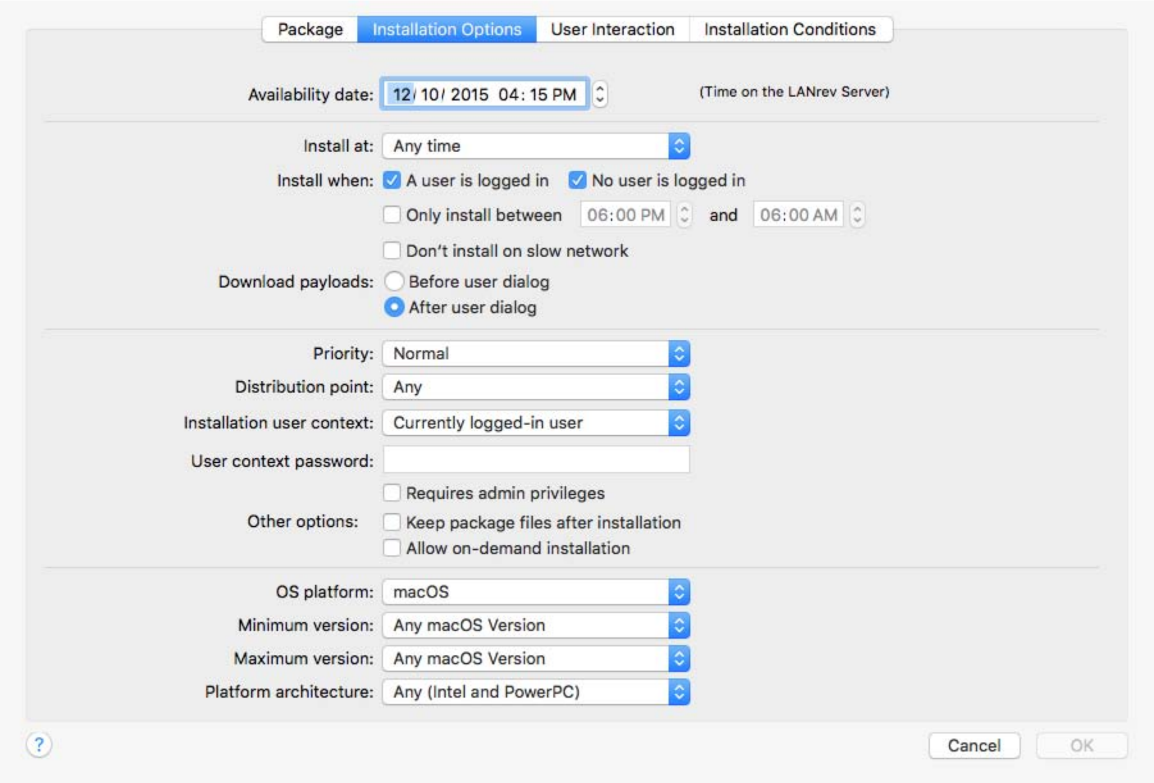
   When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, LANrev adds the `/qn` option (`/quiet /norestart` for MSU files) to run the installer silently.

   When you add your own options or when another type of installer is selected, you have to provide the command line parameters for a silent installation yourself.

7. For macOS installers, you can specify a desired installation volume in the **Target installation volume** field.

   If this field is left empty, the installation will be performed on the boot volume.

To specify requirements and timing options, click the **Installation Options** tab:



Availability date: 12/ 10/ 2015 04: 15 PM (Time on the LANrev Server)

Install at: Any time

Install when: ☑ A user is logged in ☑ No user is logged in

□ Only install between 06:00 PM and 06:00 AM

□ Don't install on slow network

Download payloads: ○ Before user dialog

● After user dialog

Priority: Normal

Distribution point: Any

Installation user context: Currently logged-in user

User context password:

Other options: □ Requires admin privileges

□ Keep package files after installation

□ Allow on-demand installation

OS platform: macOS

Minimum version: Any macOS Version

Maximum version: Any macOS Version

Platform architecture: Any (Intel and PowerPC)

8. If you do not want to make the software package available immediately, enter the earliest time when agents can install it in the **Availability date** field.

9. Normally, agents install software packages meant for them as soon as they become available. The **Install at** pop-up menu and **Install when** options lets you modify this behavior:

   - You can instruct the agent to wait until the next startup of the administered computer or user login (choose **Next startup** or **Next login**). The latter is particularly useful when the installer requires a user to be logged in.
   - You can specify that the package can be installed when a user is logged in on the target computer, when no user is logged in, or in both cases.
     Note: It is possible to check both options, which is indeed the default. At least one of the two options must be checked. When the user is allowed to refuse the installation (in the **User Interaction** *pane, see below), the package can only be installed when a user is logged in.*
   - You can also specify that installations only happen during certain times, for example, after hours when the office is not busy (**Only install between**).

10. If the package is to be installed only over fast networks, check **Don't install on slow network**.

A network is considered slow when its nominal data rate is less than 100 Mbit/s.

11. Specify via the **Download payloads** setting when the agent is to download the payloads, before or after a user dialog is displayed.

    Downloading the payloads before displaying the dialog makes for snappier responses after the user answers the dialog but may mean unnecessary network traffic if the user refuses the installation. Downloading the payloads after displaying the dialog avoids unnecessary traffic but makes users wait for the download to happen after they have agreed to the installation.

    If no user dialog is displayed, the **Download payloads** setting is ignored.

12. Specify a priority if desired. The priority determines the order in which an agent installs packages when several are available simultaneously.

13. If you want to restrict the distribution points from which an agent may download the payloads of this software package to assigned distribution points (from the agent’s local subnet or from a computer group to which the agent’s computer belongs), choose an option from the **Distribution point** pop-up menu.

    If you choose **From assigned distribution point if available**, the agent tries to download the payloads from an assigned distribution point. If no such distribution point is available, it chooses a different one. If you choose **From assigned distribution point only**, the installation fails if there is no assigned distribution point.

    Note that, irrespective of this setting, distribution points where the **Only use when assigned to group or via IP range** option is checked will never serve this package to clients to which they have not been assigned. See step 5 of “Specifying the distribution point in the Software Distribution Center” on page 297 for details.

14. Specify the user account that is to be used for installations.

    Normally, this will be the current local user on each computer. You can specify a different account. For Windows only, you must also specify the account’s password in this case. When you specify a Windows domain username, you must prefix it with the domain and \.

    You can also specify that the installation be performed in the context of the system user.

    If the installation requires administrator privileges on macOS, check the **Requires admin privileges** option.

    Note: This latter option does not change the used account; it merely temporarily boosts the privileges available to the installation process.

15. If you want the installation files to remain on the target computers after the installation has finished, check **Keep package files after installation**.

    If this option is unchecked, the agents delete the downloaded payloads after the installation is complete.

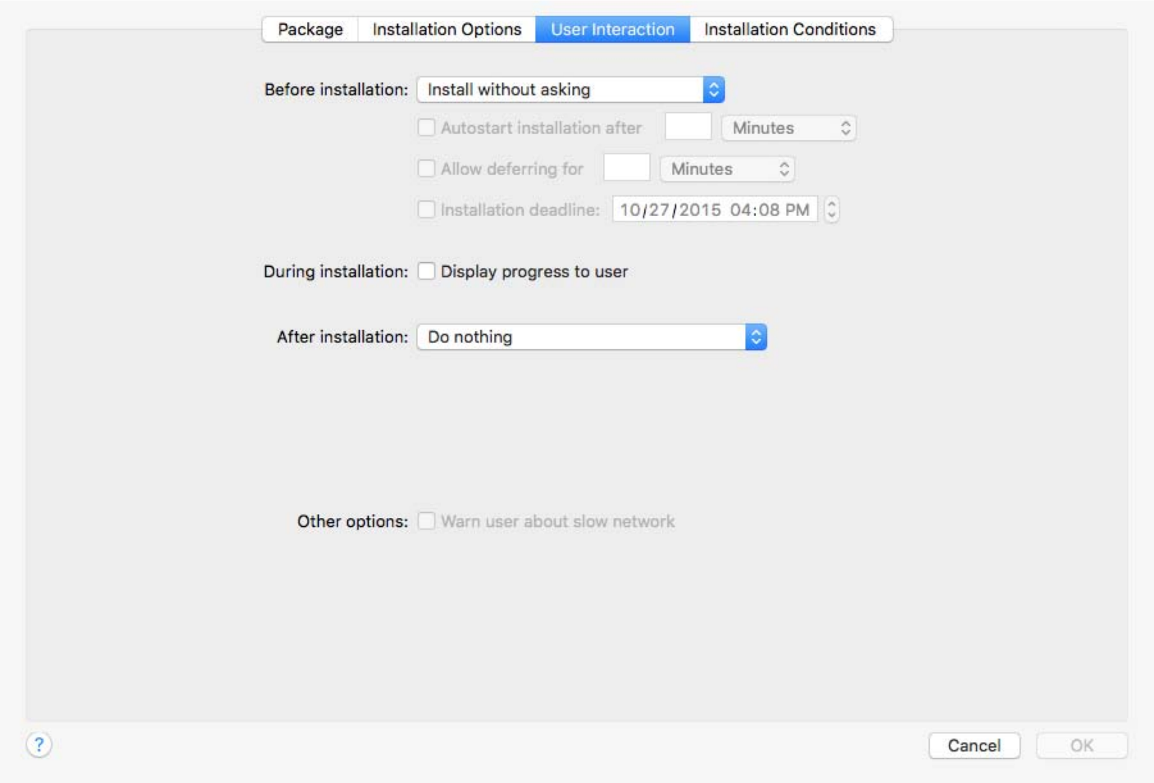
16. If you want the users to start the installation of this package on their own schedule – creating a package for pull installation instead of push installation – check the **Allow on-demand installation** option.

    Checking this option disables a number of other options in the **Installation Options** and **User Interaction** panes.

17. Specify the operating system platform – macOS or Windows, optionally restricted to just client or just server systems – and any minimum and/or maximum versions required by the software.

    If desired, choose an option from the **Platform architecture** pop-up menu to restrict installation of the package to Intel or PowerPC processors (macOS) or 32-bit or 64-bit systems (Windows), respectively.

18. Click the **User Interaction** tab to specify which information is presented to users and what interaction options they have for the installation:



Before installation: Install without asking

□ Autostart installation after [ ] Minutes

□ Allow deferring for [ ] Minutes

□ Installation deadline: 10/27/2015 04:08 PM

During installation: □ Display progress to user

After installation: Do nothing

Other options: □ Warn user about slow network

19. Specify in the **Before installation** pop-up whether the user is to be notified or have the option to postpone or refuse the installation.

Depending on the option chosen, additional settings become available:

You can specify that the installation is automatically started after a certain time if the notification should not be answered by the user.

You can also specify that the installation cannot be postponed for more than a certain interval or beyond a certain date.

Note: If you specify both an interval and a deadline, the earlier of the two resulting dates is effective.

20. If the user is to be informed of the progress of an installation under way, check **Display progress to user**.

21. From the **After installation** pop-up menu, choose the desired action that LANrev Agent is to perform when the installation is complete.

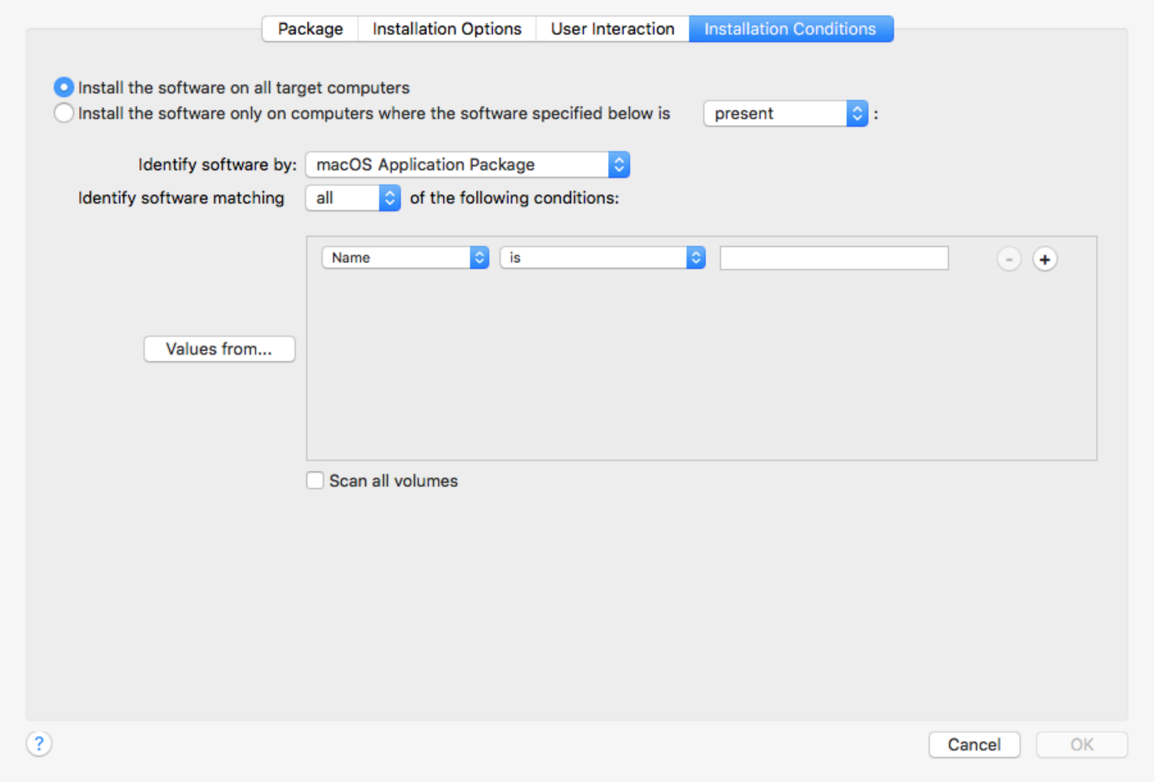
    Depending on your choice, additional options may become available.

    You can specify an interval after which a notification is automatically closed.

    When a restart is to be performed, you can specify that the user is notified in advance. You may give him or her the opportunity to defer the restart, specify that the restart happens automatically after a certain time when the notification is not answered, and have the notification reappear in regular intervals.

22. If desired, check **Warn user about slow network** to inform users when their network connection to the distribution point has a nominal speed of less than 100 Mbit/s.

23. If desired, click the **Installation Conditions** tab to limit the package to be installed only on computers that meet certain prerequisites:



● Install the software on all target computers
○ Install the software only on computers where the software specified below is present :

Identify software by: macOS Application Package
Identify software matching all of the following conditions:

Name is

□ Scan all volumes

24. To have the software installed on all computers that belong to the computer groups to which the package is assigned, choose **Install the software on all target computers**.

    To have it installed only on certain computers, choose **Install the software only on computers where the software specified below is** and specify the appropriate conditions. The available settings are similar to the ones in “Setting up license specifications” on page 349.

25. If an executable payload containing an Adobe CS3 or CS 4 installer or updater is assigned to this software package, you can set additional options as described in **Setting options for Adobe CS3 and CS 4**, below.

26. Click **OK** to close the dialog.

27. To store the software package specification on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu. LANrev creates the package definition on the LANrev server.

    You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new software package becomes available to the Software Distribution Center only after you have done so.

Setting options for Adobe CS3 and CS 4

If a software package is assigned a payload containing an Adobe CS3 or CS 4 installer or updater, an additional pane, **Adobe CS Options**, becomes available.

NOTE The settings in this tab are not compatible with Adobe CS 5 or newer. For remotely distributing these versions of Adobe CS, prepare an installer using Adobe Application Manager Enterprise Edition (AAMEE) and use that installer to create a standard software distribution package in LANrev Admin.

To set Adobe CS options:

1. Click the **Adobe CS Options** tab.
2. Click **Use the following settings for installation**.

   If you click **Use command line options for installations**, all other settings in this pane are disregarded. If you choose that options, customize the installer’s behavior via the command line options in the **Package** pane, as described in step 6 of the previous procedure.
3. Check the desired components for installation or uninstallation in the scrolling list.
4. From the **Action** pop-up menu, choose whether to install or uninstall the software.
5. If desired, enter a serial number in the **Serial number** field.
6. Check the other options as desired.

   The options are explained in “Adobe CS Options” on page 708.

Editing software packages

To edit existing software package definitions:

1. Select the packages in the **Server Center** window and choose **Edit Software Package** from the action menu.

   The **Software Distribution Package** dialog opens.
2. Make the desired changes and click **OK**.
3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Besides changing options for the packages, you can also use this process to specify different payloads, for example, when a new version has become available.

Removing software packages

To remove existing software package definitions:

1. Select the packages in the **Server Center** window and choose **Remove Software Package** from the action menu.

   A confirmation message is displayed.

2. Confirm the decision.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

   Until you do this, the software packages are still available.

Setting up metapackages

Metapackages are combinations of references to software packages and additional metadata. They represent a software installation within the Software Distribution Center.

NOTE Setting up metapackages is possible only for administrators with the **Modify Software Package** right. See "New Administrator" on page 758 for details.

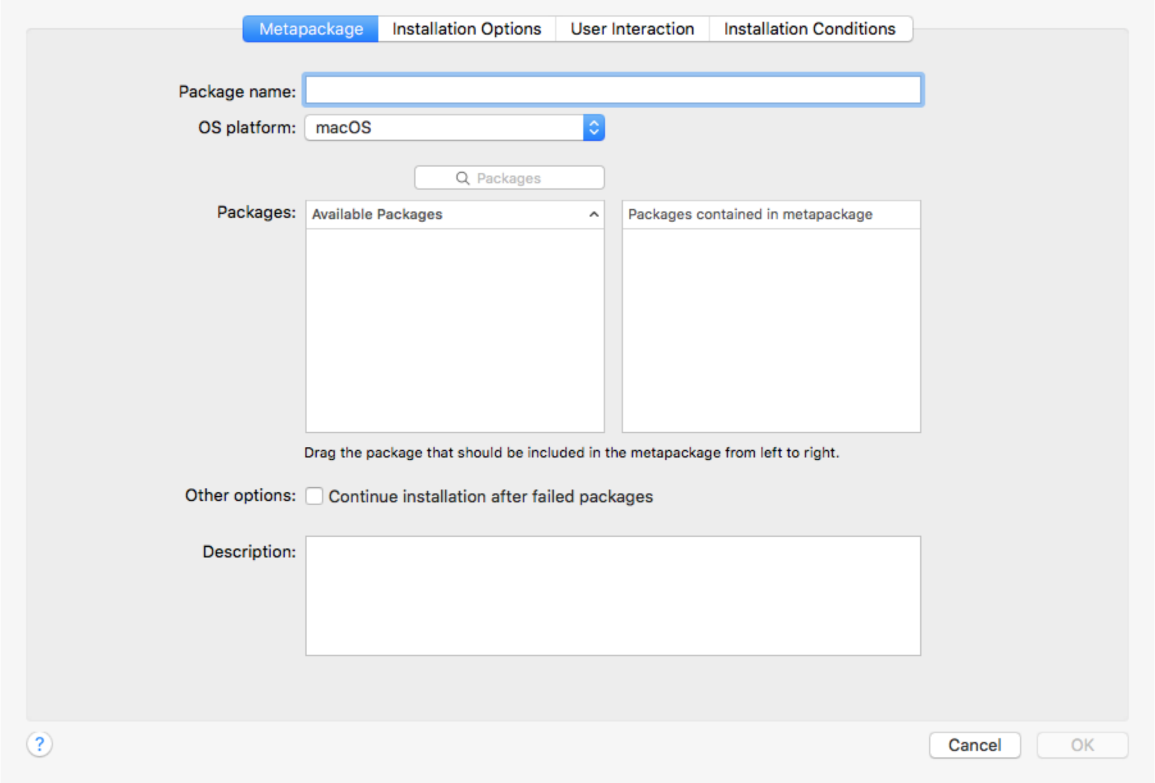
To set up a metapackage:

NOTE The settings you make for the metapackage override any conflicting settings for the software packages and metapackages included in the metapackage.

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu, choose **Software Distribution** > **New Metapackage**.

The **Metapackage** dialog opens:



Package name:

OS platform: macOS

Packages:

Drag the package that should be included in the metapackage from left to right.

Other options: □ Continue installation after failed packages

Description:

In the **Package** tab, you specify the packages to be used.

3. Enter the desired name for the metapackage in the **Package name** field. Optionally you can also enter a short description of the package in the **Description** field.

   This name is used only inside the LANrev system; you can choose whatever name you like.

4. Choose the desired target operating system platform from the **OS platform** pop-up menu.

5. Specify the software packages that are to be included in the metapackage.

   All packages that are available on the distribution points, including other metapackages, are listed in the dialog pane.

   You can filter the displayed packages by entering parts of their names in the search field above the list of packages.

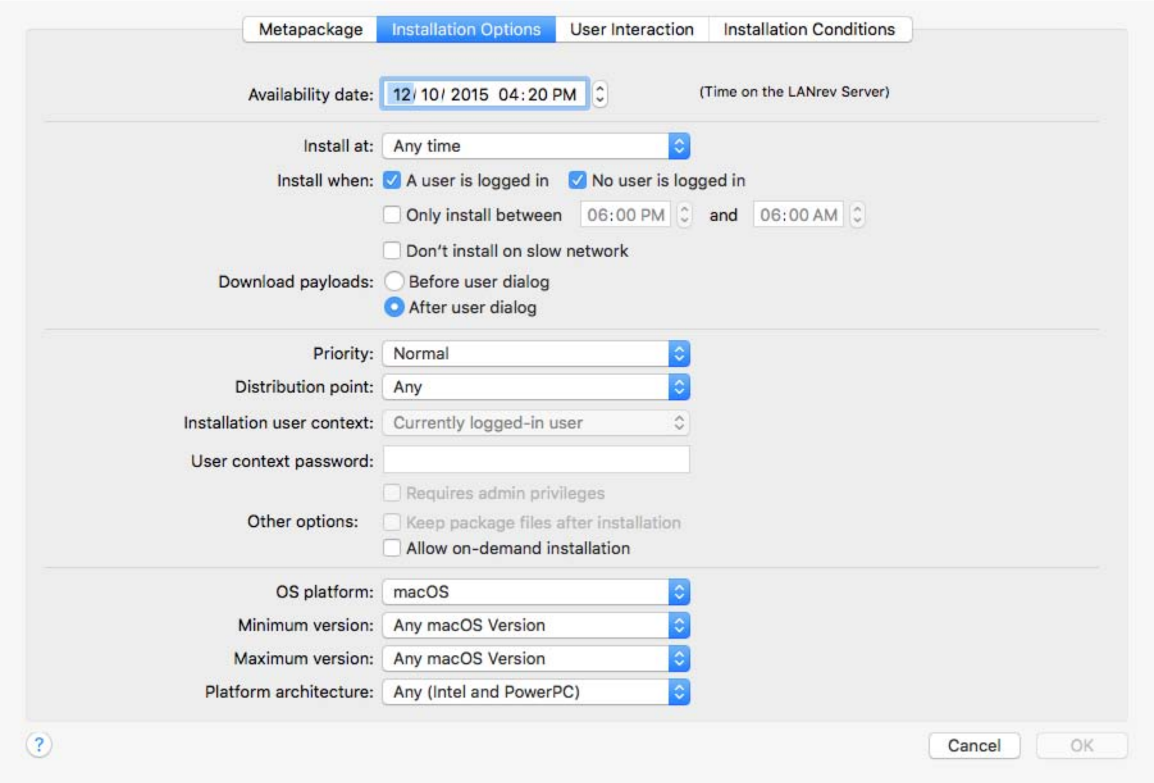
   Drag all payloads that are to be included in the metapackage from the left-hand list to the right-hand list.

   You can reorder packages in the right-hand list by dragging them higher or lower in the list. LANrev installs packages contained in a metapackage in the order in which they are listed.

6. If you want LANrev to continue installing packages on a client even after the installation of one package fails, check **Continue installation after failed packages**.

   If the option is unchecked, a failed package causes the installation of the metapackage to stop.

7. To specify requirements and timing options, click the **Installation Options** tab:



Availability date: 12/ 10/ 2015 04:20 PM (Time on the LANrev Server)

Install at: Any time

Install when: ☑ A user is logged in ☑ No user is logged in

□ Only install between 06:00 PM and 06:00 AM

□ Don't install on slow network

Download payloads: ○ Before user dialog

● After user dialog

Priority: Normal

Distribution point: Any

Installation user context: Currently logged-in user

User context password:

Other options: □ Requires admin privileges

□ Keep package files after installation

□ Allow on-demand installation

OS platform: macOS

Minimum version: Any macOS Version

Maximum version: Any macOS Version

Platform architecture: Any (Intel and PowerPC)

8. If you do not want to make the metapackage available immediately, enter the earliest time when agents can install it in the **Availability date** field.

9. Normally, agents install metapackages meant for them as soon as they become available. The **Install at** pop-up menu and **Install when** options lets you modify this behavior:

   - You can instruct the agent to wait until the next startup of the administered computer or user login (choose **Next startup** or **Next login**). The latter is particularly useful when the installer requires a user to be logged in.
   - You can specify that the metapackage can be installed when a user is logged in on the target computer, when no user is logged in, or in both cases.
     Note: It is possible to check both options, which is indeed the default. At least one of the two options must be checked. When the user is allowed to refuse the installation (in the **User Interaction** *pane, see below), the package can only be installed when a user is logged in.*

- You can also specify that installations only happen during certain times, for example, after hours when the office is not busy (**Only install between**).

10. If the package is to be installed only over fast networks, check **Don’t install on slow network**.

    A network is considered slow when its nominal data rate is less than 100 Mbit/s.

11. Specify via the **Download payloads** setting when the agent is to download the payloads of the contained packages, before or after a user dialog is displayed.

    Downloading the payloads before displaying the dialog makes for snappier responses after the user answers the dialog but may mean unnecessary network traffic if the user refuses the installation. Downloading the payloads after displaying the dialog avoids unnecessary traffic but makes users wait for the download to happen after they have agreed to the installation.

    If no user dialog is displayed, the **Download payloads** setting is ignored.

12. Specify a priority if desired. The priority determines the order in which an agent installs packages when several are available simultaneously.

13. If you want to restrict the distribution points from which an agent may download the payloads for this metapackage to assigned servers (from the agent’s local subnet or from a computer group to which the agent’s computer belongs), choose an option from the **Distribution point** pop-up menu.

    If you choose **From assigned distribution point if available**, the agent tries to download the payloads from an assigned distribution point. If no such distribution point is available, it chooses a different one. If you choose **From assigned distribution point only**, the installation fails if there is no assigned distribution point.

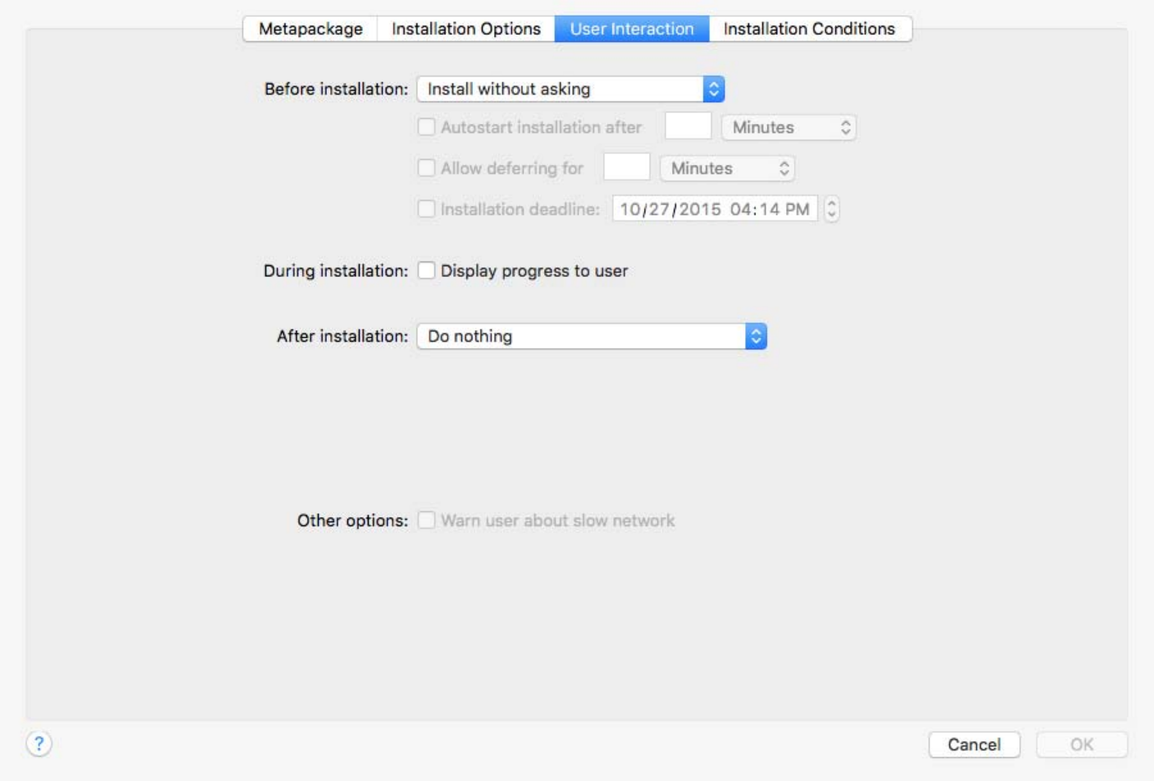
14. The user context cannot be set in a metapackage; it is taken from the individual packages.

    Likewise, the software packages determine which payloads are kept after installation and which are deleted.

15. Specify the operating system platform – macOS or Windows, optionally restricted to just client or just server systems – and any minimum and/or maximum versions required by the software.

    If desired, choose an option from the **Platform architecture** pop-up menu to restrict installation of the package to Intel or PowerPC processors (macOS) or 32-bit or 64-bit systems (Windows), respectively.

16. Click the **User Interaction** tab to specify which information is presented to users and what interaction options they have for the installation:



Before installation: Install without asking

□ Autostart installation after Minutes

□ Allow deferring for Minutes

□ Installation deadline: 10/27/2015 04:14 PM

During installation: □ Display progress to user

After installation: Do nothing

Other options: □ Warn user about slow network

17. Specify in the **Before installation** pop-up whether the user is to be notified or have the option to postpone or refuse the installation.

    Depending on the option chosen, additional settings become available:

    You can specify that the installation is automatically started after a certain time if the notification should not be answered by the user.

    You can also specify that the installation cannot be postponed for more than a certain interval or beyond a certain date.

    Note: If you specify both an interval and a deadline, the earlier of the two resulting dates is effective.

18. If the user is to be informed of the progress of an installation under way, check **Display progress to user**.

19. From the **After installation** pop-up menu, choose the desired action that LANrev Agent is to perform when the installation is complete.

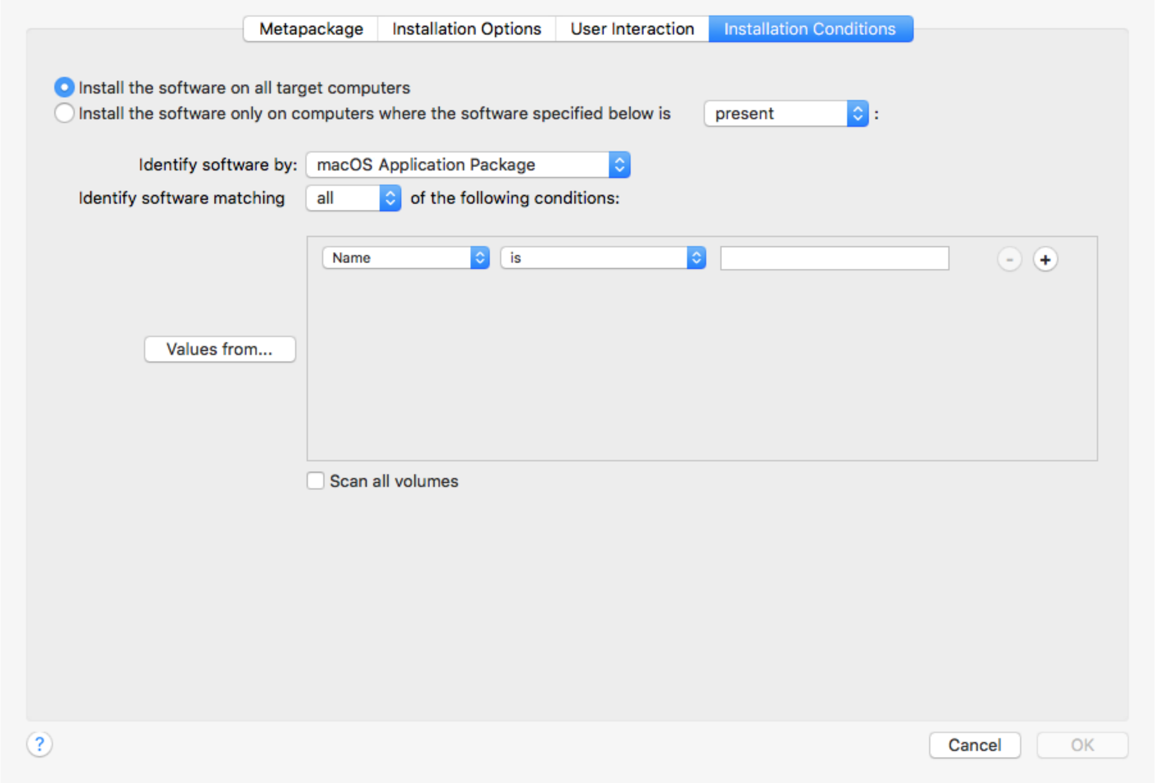
    Depending on your choice, additional options may become available:

You can specify an interval after which a notification is automatically closed.

When a restart is to be performed, you can specify that the user is notified in advance. You may give him or her the opportunity to defer the restart, specify that the restart happens automatically after a certain time when the notification is not answered, and have the notification reappear in regular intervals.

20. The **Warn user about slow network** setting is taken from the individual software packages.

21. If desired, click the **Installation Conditions** tab to limit the package to be installed only on computers that meet certain prerequisites:



● Install the software on all target computers
○ Install the software only on computers where the software specified below is present :

Identify software by: macOS Application Package
Identify software matching all of the following conditions:

Name is

□ Scan all volumes

22. To have the software installed on all computers that belong to the computer groups to which the metapackage is assigned, choose **Install the software on all target computers**.

    To have it installed only on certain computers, choose **Install the software only on computers where the software specified below is** and specify the appropriate conditions. The available settings are similar to the ones in “Setting up license specifications” on page 349.

23. Click **OK** to close the dialog.

24. To store the metapackage specification on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu. LANrev creates the package definition on the LANrev server.

    You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new metapackage becomes available to the Software Distribution Center only after you have done so.

Editing metapackages

To edit existing metapackage definitions:

1. Select the metapackages in the **Server Center** window and choose **Edit Software Package** from the action menu.

   The **Metapackage** dialog opens.

2. Make the desired changes and click **OK**.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes in the Software Distribution Center.

Besides changing options for the metapackages, you can also use this process to specify different contained packages.

Removing metapackages

To remove existing metapackage definitions:

1. Select the metapackages in the **Server Center** window and choose **Remove Software Package** from the action menu.

   A confirmation message is displayed.

2. Confirm the decision.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes in the Software Distribution Center.

   Until you do this, the metapackages are still available.

Exporting and importing software packages and metapackages

You can export packages from LANrev for importing into another installation.

Exported packages contain all settings, including the required payloads.

NOTE Exporting and importing packages is possible only for administrators with the **Modify Software Package** right. See “New Administrator” on page 758 for details.

Exporting packages or metapackages

To export a software package or metapackage:

1. In the **Server Center** window, select the software packages or metapackages you want to export.
2. Right-click and choose **Export Package** from the context menu.

   A standard Save dialog is displayed.
3. Specify the name and location for the exported packages and click **Save**.

The packages are exported as a package file (a folder that looks like a file)

Depending on the size of the payloads contained in the packages, this process may take a while.

Importing packages or metapackages

To import a software package or metapackage:

1. Choose **File** > **Import** > **Software Packages**.

   A standard Open dialog is displayed.
2. Select the exported package you want to import and click **Open**.

The packages are imported into your installation of LANrev Server and are thereafter available for installation on managed computers.

Depending on the size of the payloads contained in the packages, this process may take a while.

Managing volume purchases of Mac App Store apps

You can make available licenses for commercial apps from the Mac App Store to computer users. The users can then download the apps from the Mac App Store to their personal devices.

If users have set their Macs to automatically download software purchased on other Macs, any software for which a license is assigned to a user is automatically installed.

Creating app packages for Mac App Store apps

You can create app packages for Mac App Store apps. Licenses for these apps can then be assigned to macOS devices.

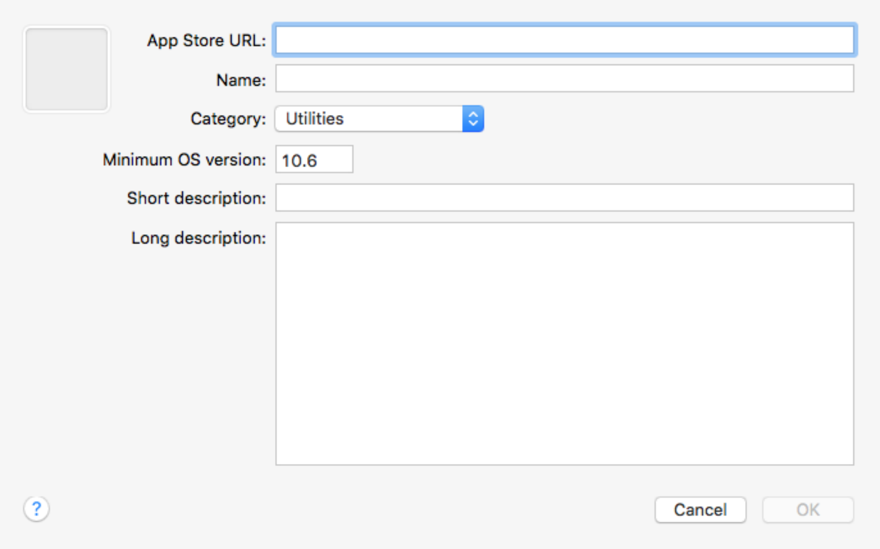
These app packages contain references to the apps, not the actual apps themselves, and appear in the Mac App Store Applications section of the Server Center.

To create and distribute packages for volume-licensed apps:

1. Make sure that VPP licensing is set up correctly, as described in "Setting up VPP license management" on page 211.

2. In the **Server Center** window, right-click in the sidebar and choose **Software Distribution** > **New Mac App Store Application Package**.

   The **Mac App Store Application** dialog opens:



App Store URL:
Name:
Category: Utilities
Minimum OS version: 10.6
Short description:
Long description:

3. Enter the URL of the app's App Store page in the **App Store URL** field and press the Tab key or click in another field.

   You can obtain the URL by choosing **Copy Link** from the small menu to the right of the price tag in the application's listing.

   Entering the URL and leaving this field fills in some of the other fields with information downloaded from the App Store.

4. If desired, edit the **Name**, **Category**, **Short description**, or **Long description** fields.

   You can also edit the **Minimum OS** version field, but we recommend that you do so only if you have a concrete reason.

5. Click **OK** to close the dialog and save the new app package.

6. The new app package appears in the **Mac App Store Applications** group in the **Server Center** window.

7. You can now assign the VPP license represented by the package to users as described in “Assigning and revoking VPP app licenses” on page 321.

8. You can also manually install app packages using the **Install Mac App Store Application** command.

Managing VPP licenses for computer applications

Apple’s App Store volume purchase program (VPP) lets you purchase blocks of licenses that enable users to download the corresponding macOS apps.

Setting up the license management is explained in “Setting up VPP license management” on page 211.

For details of managing volume licenses for Mac App Store apps, see:

- **Assigning and revoking VPP app licenses** (page 321)
- **VPP license statistics for Mac App Store apps** (page 324)

NOTE Assigning book licenses is described in “Managing VPP book licenses” on page 230. The steps described there for the **Mobile Devices** window can also be performed on computers or users in the **Server Center** window.

Assigning and revoking VPP app licenses

Licenses for Mac App Store apps can be assigned to users or removed again when users, devices, or apps are listed in the **Server Center** window.

Any assignment requires that the VPP is properly set up, as described in “Setting up VPP license management” on page 211. In particular, the users in question must have been registered with the program and they must have specified their Apple ID.

Assigning VPP app licenses

You can assign app licenses when selecting users, devices, or apps.

Assigning a license when users or devices are selected:

1. In the main part of the **Server Center** window, right-click one or more users or devices and choose **VPP Licensing** > **Assign Application Licenses to Device Users**.

   The **Assign Application Licenses** dialog opens.

2. Check all listed apps that you want to assign to the selected users or the users of the selected devices.

   To filter the list, you can enter part of the name of the desired app in the search field at the upper right of the dialog.

3. Click **OK**.

Licenses for the marked apps are assigned to the selected users. The app is added to the users list of purchased items in the iTunes store.

Any devices of these users that have been set up in their local settings to automatically download apps purchased on other devices will download the assigned apps. On other devices, users will have to download the apps manually.

Assigning a license when apps are selected:

1. Make sure that you have created app packages for all apps that you want to assign.

   Creating packages is described in “Managing volume purchases of Mac App Store apps” on page 319. When setting up a package, make sure to use the same app store URL as you have used when purchasing the license.

2. In the main part of the **Server Center** window, right-click one or more 3rd-party apps and choose **Assign Application Licenses to Users**.

   The **Assign VPP Licenses** dialog opens, with the selected apps listed in the upper half.

3. In the main part of the **Server Center** window, right-click one or more 3rd-party apps and choose **Assign Application Licenses to Users** or **Assign Application Licenses to Devices**.

   The **Assign VPP Licenses** dialog or the **Assign Application Licenses to Devices** dialog opens, respectively, with the selected apps listed in the upper half.

4. In the lower half of the dialog, check all users or devices, respectively, to whom you want to assign the listed apps.

   To filter the list, you can enter part of the name of the user or device you are looking for in the search field at the right of the dialog.

5. Click **OK**.

Licenses for the selected apps are assigned to the marked users. The apps are added to the users’ lists of purchased items in the iTunes store.

Any devices of these users that have been set up in their local settings to automatically download apps purchased on other devices will download the assigned apps. On other devices, users will have to download the apps manually.

Revoking VPP app licenses

As with assigning licenses, you can revoke app licenses when selecting users, devices, or apps.

The licenses for some apps may be declared irrevocable by Apple. Such licenses cannot be revoked (whether in LANrev or otherwise) once they have been assigned; the procedures below do not apply to these licenses.

Revoking a license when users or devices are selected:

1. In the main part of the **Server Center** window, right-click one or more users or devices and choose **VPP Licensing** > **Revoke Application Licenses**.

   The **Revoke Application Licenses** dialog opens. It lists all apps with licenses that are assigned to at least one of the selected users.

2. Check all listed apps for which you want to revoke the license from the selected users or the users of the selected devices.

   To filter the list, you can enter part of the name of the desired app in the search field at the upper right of the dialog.

3. Click **OK**.

Licenses for the marked apps are revoked from the selected users. The apps remain on the user’s device but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

Revoking a license when apps are selected:

1. In the main part of the **Server Center** window, right-click one or more 3rd-party apps and choose **Revoke Application Licenses**.

   The **Revoke Application Licenses** dialog opens, with the selected apps listed in the upper half.

2. In the lower half of the dialog, check all users or devices from which you want to revoke the licenses for the listed apps.

   To filter the list, you can enter part of the name of the user or device you are looking for in the search field at the right of the dialog.

3. Click **OK**.

Licenses for the selected apps are revoked from the marked users. The apps remain on the users' devices but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

VPP license statistics for Mac App Store apps

LANrev offers to way to monitor the number of VPP licenses available for a Mac App Store app.

Individual apps

To view the licenses for an individual app:

1. Click the desired app in the sidebar of the **Server Center** window.

   The detail view for the item is displayed.

2. Click the **Volume Licenses** tab.

   The number of purchased, assigned, and available licenses is displayed in the upper part of the tab.

   Note that the **Volume Licenses** tab is only available for Mac App Store apps, as other applications cannot be part of the VPP.

Monitoring licenses in tables

To view the licenses for multiple apps in a table:

1. Display a table containing Mac App Store apps.

   This can either be the **Mac App Store Applications** section of the **Server Center** window or a browser window displaying the desired kind of information.

2. Add one or more of the relevant information items to the table, depending on what you want to monitor.

   - App Store VPP Licenses Purchased
   - App Store VPP Licenses Assigned
   - App Store VPP Licenses Remaining

Setting up computer groups

Computer groups are collections of computers that are to be handled the same for software distribution or license monitoring. One computer can belong to multiple computer groups, allowing great flexibility through overlapping groups.

There are standard and smart computer groups:

- Standard computer groups are maintained manually – computers are added and removed by explicit administrator decision. The group is defined by the computers it contains.

- Smart computer groups are maintained automatically. They are defined by one or more criteria and contain all computers meeting those criteria. LANrev automatically adds a computer to a group when it meets the criteria and automatically removes it when it no longer does.

Although standard and smart groups can largely be used in the same way, they are defined and edited differently, as described below.

For information about adding actions to a smart computer group, see “Specifying actions in computer groups” on page 329.

NOTE The same computer groups are available for license monitoring and software distribution.

Setting up standard computer groups

Standard computer groups are arbitrary collections of computers that are maintained manually.

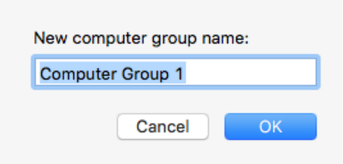
NOTE Instead of setting up a standard computer group from scratch as described below, you can also duplicate an existing group by dragging it to the desired category header in the sidebar of the **Server Center** window while holding down the Option key.

To set up a standard computer group:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu, choose **Computer Groups** > **New Computer Group**.

   The **New Computer Group** dialog opens:



New computer group name: Computer Group 1

3. Enter the desired name and click **OK**.

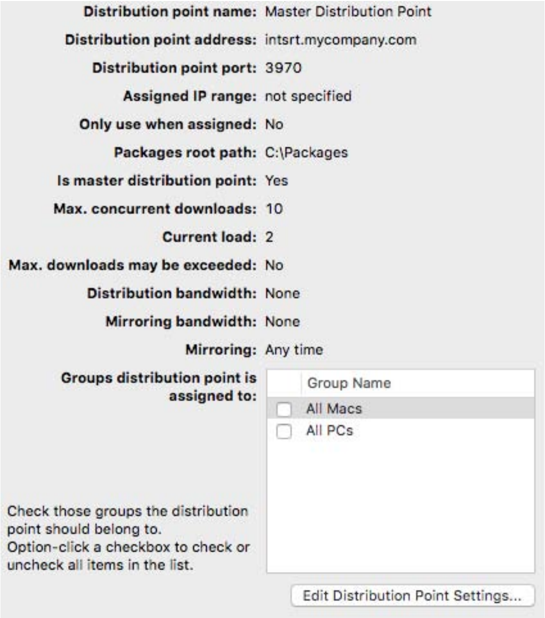
   The new group appears in the **Server Center** window’s sidebar.

4. To add computers to the group, drag them on top of the group icon from the table area, for example, from the **Unassigned Computers** default computer group, or from any browser window displaying computers.

To remove computers, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

5. If desired, you can assign distribution points to groups. Computers from a group will prefer these assigned servers for installer downloads.

   To assign a distribution point to a group, select the distribution point in the **Server Center** window's sidebar, displaying its details in the window:



Distribution point name: Master Distribution Point
Distribution point address: intsrt.mycompany.com
Distribution point port: 3970
Assigned IP range: not specified
Only use when assigned: No
Packages root path: C:\Packages
Is master distribution point: Yes
Max. concurrent downloads: 10
Current load: 2
Max. downloads may be exceeded: No
Distribution bandwidth: None
Mirroring bandwidth: None
Mirroring: Any time
Groups distribution point is assigned to:

	Group Name
☐	All Macs
☐	All PCs

Check those groups the distribution point should belong to.
Option-click a checkbox to check or uncheck all items in the list.

   Check all groups to which you want to assign the server.

6. To store the computer group specification on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new computer group becomes available only after you have done so.

Setting up smart computer groups

If any browser window contains a smart group with the desired criteria, you can simply drag it into **Computer Group** entry in the sidebar of the

Server Center window. Otherwise, you can create the smart computer group from scratch.

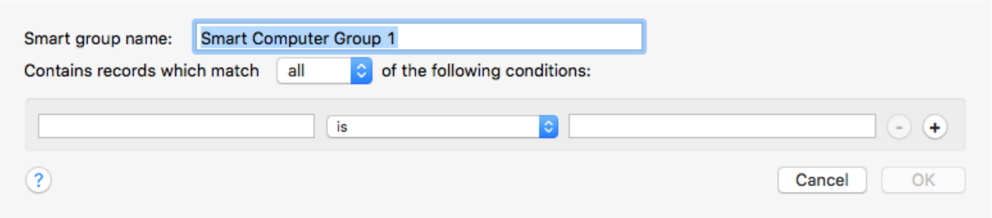
NOTE Instead of setting up a smart computer group from scratch as described below, you can also duplicate an existing group by dragging it to the desired category header in the sidebar of the **Server Center** window while holding down the Option key.

To create a new smart computer group:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu, choose **Computer Groups** > **New Smart Computer Group**.

   The **Smart Group** dialog opens:



Smart group name: Smart Computer Group 1

Contains records which match all of the following conditions:

is

3. Enter the name for the new computer group and define the conditions that computers must meet to be included in the computer group.

   To define a condition, specify an information item in the left-hand text field, choose a comparison operator from the pop-up menu, and enter a comparison value in the right-hand text field. (For some information items, there is no comparison value.)

   When the text insertion mark is in a field, you can drag a column from the Columns drawer into the field.

   With the **+** and **–** buttons, you can add and remove conditions.

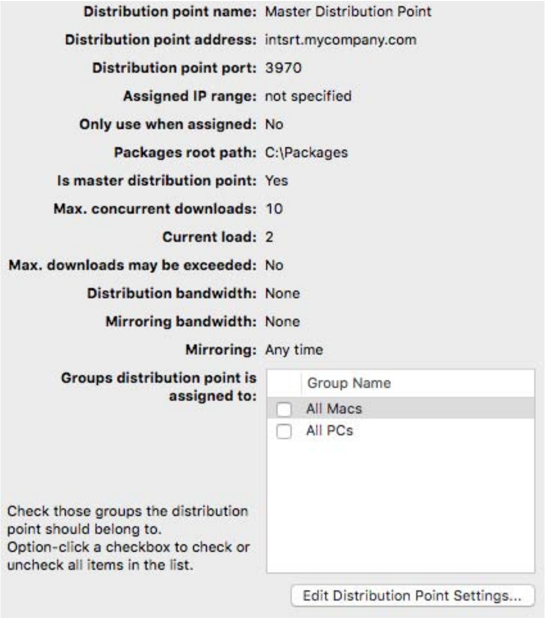
4. If you have specified more than one condition, specify through the upper pop-up menu whether computers must meet one or all of the conditions.

5. Click **OK**.

   The new group appears in the **Server Center** window's sidebar.

6. If desired, you can assign distribution points to groups. Computers from a group will prefer these assigned servers for installer downloads.

To assign a distribution point to a group, select the server in the **Server Center** window’s sidebar, displaying the server’s details in the window:



Distribution point name:	Master Distribution Point
Distribution point address:	intsrt.mycompany.com
Distribution point port:	3970
Assigned IP range:	not specified
Only use when assigned:	No
Packages root path:	C:\Packages
Is master distribution point:	Yes
Max. concurrent downloads:	10
Current load:	2
Max. downloads may be exceeded:	No
Distribution bandwidth:	None
Mirroring bandwidth:	None
Mirroring:	Any time
Groups distribution point is assigned to:	Group Name □ All Macs □ All PCs

Check those groups the distribution point should belong to.
Option-click a checkbox to check or uncheck all items in the list.

Check all groups to which you want to assign the server.

7. To store the computer group specification on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new computer group becomes available only after you have done so.

Editing computer groups

To change the group’s name or (for smart computer groups) change its definition, select it in the sidebar and choose **Edit Computer Group** from the action menu and enter the new name or redefine the group’s criteria.

To add computers to a standard (non-smart) group, drag them on top of the group icon from the table area, for example, from the **Unassigned Computers** default computer group, or from any browser window displaying computers.

To remove computers, select them in the group, right-click them and choose **Remove from Group** from the context menu. A confirmation message is displayed.

Choose **Save Distribution and Licensing Info** from the **Server** menu to activate the changes.

Removing computer groups

To remove an existing computer group definition:

1. Select the group in the **Server Center** window and choose **Remove Computer Group** from the action menu.

   A confirmation message is displayed.

2. Confirm the decision.

3. Choose **Save Distribution and Licensing Info** from the **Server** menu to store the changes.

   Until you do this, the computer group is still available.

Specifying actions in computer groups

For each smart computer group, you can specify actions that are to be performed when a computer is added to the policy.

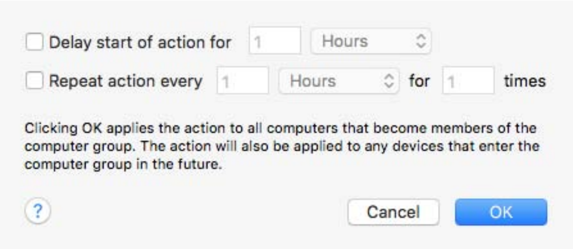
Adding actions to a computer group

Any actions you want to specify must already been available in the **Actions** group of the **Server Center** window sidebar. See “Working with actions” on page 178 for information on managing actions.

To specify an action in a policy:

1. In the **Server Center** window, drag the action that you want to add from the **Actions** group in the sidebar to the smart computer group to which you want to add it. (Actions cannot be added to standard – non-smart – computer groups.)

   The **Action Assignment Options** dialog is displayed:



☐ Delay start of action for 1 Hours

☐ Repeat action every 1 Hours for 1 times

Clicking OK applies the action to all computers that become members of the computer group. The action will also be applied to any devices that enter the computer group in the future.

2. Specify whether you want to delay or repeat the action:

   - If you check the delay option, the action is not performed immediately when a computer becomes a member of the policy, but only after the specified interval has elapsed.
   - If you check the repeat option, the action is repeated after the specified interval for the specified number of times.

   You can combine both options, for example, to send a message to the computer two hours after it has become a member of the policy and then every hour thereafter.

A delayed or repeated action is not executed when the computer is no longer a member of the policy.

3. Click **OK**.

The action is added to the policy. It is executed on all computers that are currently a member of the computer group and will be executed on each computer that enters the computer group in the future.

Any delays and repetitions you have specified apply both to existing and future members. The delay for existing members is calculated from the moment when the action is assigned to the computer group.

Changing delay or repetition settings

To change the delay or repetition settings for an action in a computer group:

1. Expand the computer group in the sidebar of the **Server Center** window and click its **Actions** subgroup.

   The actions assigned to the computer group are displayed in the main part of the **Server Center** window.

2. Right-click the action you want to edit and choose **Change Action Schedule**.

3. Set the delay and repetition as desired.

4. Click **OK**.

The new settings for the action in this computer group are saved. They are effective immediately.

Removing actions from a computer group

To remove an action from a computer group:

1. Expand the computer group in the sidebar of the **Server Center** window and click its **Actions** subgroup.

   The actions assigned to the computer group are displayed in the main part of the **Server Center** window.

2. Right-click the action you want to remove and choose **Remove Action from Policy**.

The action is removed from this computer group. Any remaining repetitions or delayed executions are skipped.

For information on removing an action entirely from LANrev (which also removes it from all policies), see “Deleting actions” on page 180.

Performing installations

Once the software distribution system has been set up as described in the previous sections of this chapter, any installation process is a very simple matter.

To initiate a new installation process:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. Make sure that the software installation package or metapackage has been properly defined.

3. Drag the package from the table area to all computer groups to which the software is to be distributed.

Software installation will begin automatically shortly thereafter. (See below for details.) You can monitor the progress of the individual installation processes in the subgroups of the **Installation Status** subcategory in the sidebar.

The available subgroups are described in “Software Distribution” on page 692.

NOTE Installations may not begin immediately for a variety of reasons, among them that you have set a later availability date or chosen an option from the software package’s **Installation time** pop-up menu.

Installation process

The actual installation process is completely automatic. It involves these main steps:

- The agents contact their assigned software distribution server to check whether there is new software available for them. The server and the contact interval is set in the Agent Settings dialog that is described in “Agent Settings” on page 405.
- The server checks to which computer groups an agent belongs and reviews all software packages and metapackages assigned to those computer groups:
  - Is the software package already available (as per the setting in the package definition)?
  - Does the agent meet the operating system requirements?
  - Are the optional auxiliary requirements from the package definition met (installation time during the day, user logged in, etc.)?
  - Is the package not yet installed on the agent’s computer?
- If all these questions are answered with “yes”, the LANrev server notifies the agent of the availability of a new package and provides the location of the payloads on one of the distribution points.
- The agent downloads the payloads from the distribution point.

If the package specifies a user notification or allows the user to postpone or cancel the installation, the agent displays the message before or after downloading the payloads, as specified in the package.

- The agent executes the executable payload locally according to the specifications in the package.
- During the installation process, the agent reports the progress to the LANrev server. When the installation is done, the result is reported – success or failure, and error details in the case of failure.
- LANrev Admin displays the results in the **Software Distribution** > **Installation Reports** section of the Server Center.

Performing ad hoc installations

In addition to standard software distribution using distribution groups, LANrev also lets you directly install software packages and metapackages on selected computers.

This is useful if there already are suitable software packages but the group of target computers is not permanent enough to warrant setting up a distribution group.

Ad hoc installations may not be ideal if:

- There is no software package. In this case, one of the methods described in “Installing software manually” on page 293 may be more appropriate.
- You expect to have to install software to the same group of computers more than very occasionally. In this case, we recommend that you set up a distribution group.

Ad hoc installations require payloads, software packages, and distribution points to be set up.

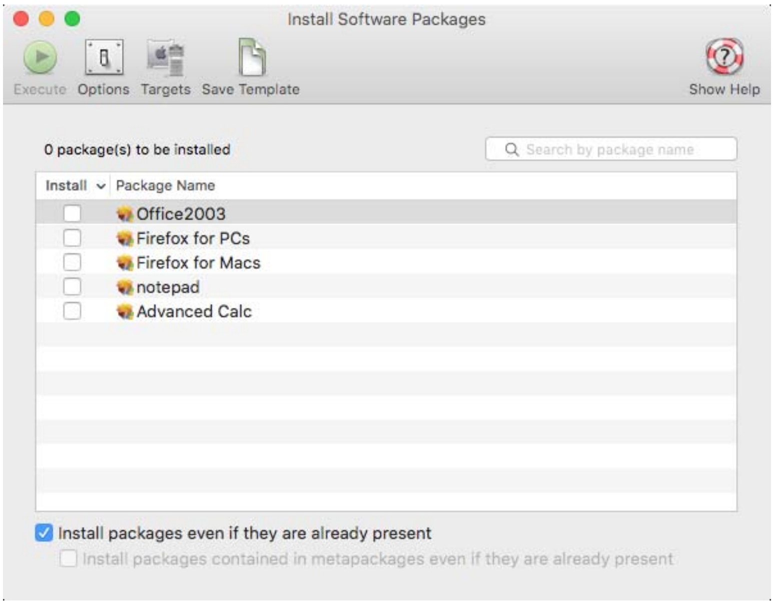
To install software packages ad hoc:

1. In any browser window, select the computers on which you want to install the software packages.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Install Software Packages**.

The **Install Software Packages** dialog opens:



0 package(s) to be installed

Install	Package Name
□	Office2003
□	Firefox for PCs
□	Firefox for Macs
□	notepad
□	Advanced Calc

☑ Install packages even if they are already present

□ Install packages contained in metapackages even if they are already present

3. Check the packages and metapackages that you want to install.

4. If you want to install selected packages and metapackages on a target computer even if that package has already been installed there, check the **Install packages even if they are already present** option.

   If you also want to install all packages contained in selected metapackages regardless of whether they have already been installed, check **Install packages contained in metapackages even if they are already present** as well.

5. Click **Execute**.

Software installation will begin automatically shortly thereafter. Any settings in the packages regarding the installation time are disregarded. Settings regarding user interaction are honored, however.

LANrev Admin displays the installation results in the **Software Distribution** > **Installation Reports** section of the Server Center

NOTE You can also launch this command by selecting the desired packages in the **Server Center** window, right-clicking them, and choosing **Install Selected Software Packages** from the context menu. In that case, you need to add the target computers to the command window.

Automated patch management

The software distribution system offers automated management of operating system patches and other updates from Apple and Microsoft as well as certain third-party patches without any additional setup. The only administrative action required is approval of packages that are made available automatically.

Overview

The automated patch management covers all software updates that Apple and Microsoft make available via the automatic update functions in their operating systems, in particular:

- Free operating system updates and service packs
- Driver patches for macOS computers
- Free software updates for application software such as Pages, iTunes, or Internet Explorer

You can thus install an operating system in its shipping version (for example, macOS 10.12) and let all patches automatically be installed, creating a fully up-to-date system with no additional effort.

The patch management also covers a range of popular third-party productivity and utility applications and security patches. Third-party patch management is available for clients running macOS 10.6 and above, Windows Vista and above, or Windows Server 2003 and above. A list of supported applications is available in article 22276 in the knowledge base.

NOTE For even easier installation of operating systems on computers that already have a LANrev agent, see “Reinstalling a Windows computer” on page 340.

Process

Automated patch management patches follows this process:

1. Agents are set up to participate.

   This requires setting the appropriate options in the **Agent Settings** dialog.

   Note: When the **Use only LANrev for OS updates** *option is enabled for an Agent, the update mechanism of the OS is disabled for that computer. However, users can manually re-enable it until the next restart of the Agent. If you want to prevent even this temporary access, we recommend that you set up a solution based on configuration profiles, group policies, or a firewall.*

2. The availability of a patch is determined.

   For operating system patches, this is done by the agents on the administered computer, which query the operating system for applicable patches. Any patches that are listed as rejected on LANrev Server (see step 5) are removed from the returned list.

For third-party patches, LANrev Server checks a back-end server for new patches, based on its database of software installed on administered computers.

Note: After installation of LANrev, it may take several hours before operating system patches first become available in the LANrev patch management and up to 48 hours for third-party patches.

Checks for available patches are performed whenever a software distribution check is performed. Automatic checks are configured in the **Servers** pane of the **Agent Settings** dialog. Manual checks can be made using the **Gather Installed Software** command and checking either or both of the **Check for missing … patches** options.

3. If any patches are found, the Software Distribution Center is checked for the presence of the patch.

4. If the patch is not present, it is automatically downloaded and a payload and software package are created from it. This package is placed in the **Unconfirmed Updates** smart group within the respective subgroup of the Software Distribution section of the Server Center.

   For example, a new patch for a Windows application would be put in **Software Distribution** > **Windows Third-Party Patches** > **Unconfirmed Patches**.

5. When patches have been downloaded to the **Unconfirmed Updates** smart group, they must be approved by you before any further processing happens.

   To approve patches, drag them to all groups containing computers on which the patch is to be installed. If you do not want to install a particular patch, drag it to the **Rejected Updates** group.

   Operating system patches are installed on all computers in these groups where **Include in OS patch management** has been checked in the agent settings; third-party patches are installed on computers where **Include in third-party patch management** has been checked.

   Note: You can reverse the decision to reject a patch at any time. (You can also reverse the decision to accept a patch, but that will not reverse any installations that may already have happened.)

   The software package contains information about the intended target computers. It is installed on only those client computers where it is –according to that information – actually required.

   We recommend that you drag operating system patch packages that you want to accept to the respective predefined computer group for the operating system; that is, to the **All Macs** group for macOS and to **All PCs** for Windows.

Note: The minimum and maximum OS information displayed by the **Software Distribution Package** *dialog for automatically generated operating system patch installation packages is used for determining the eligible target computers and can therefore not be edited.*

Third-party patch packages behave slightly differently. In particular, some of them perform a full installation, which will install the software also on computers that did not previously have it. For installing third-party patches, we therefore recommend that you create specific groups that only contain computers on which the software in question is already installed. (You can do so using the Installed Software information items.)

6. Software installation from here on follows the same process as for other software packages, as described in "Installation process" on page 331, with only one deviation: Operating system patch packages are installed only when they apply to the individual computer according to the local Software Update or Windows Update utilities. So, a package that is not needed on a particular client would not be installed, even though it is assigned to a group to which the computer belongs.

Finding missing patches

To find computers that are missing applicable patches (and the missing patches), use the **Missing Patches** window which automatically lists all computers with missing patches.

You can create smart groups in the **Missing Patches** window to focus on patches or computers of particular interest.

Deactivating patch management

You can deactivate the patch management for individual agents or completely for the entire LANrev system.

To deactivate it for individual agents, open the Agent Settings dialog for those agents and uncheck the **Include in patch management** option.

To deactivate the patch management completely, switch it off for all agents, as described above.

Reinstalling a macOS computer

Using the software distribution system, LANrev can remotely reinstall the operating system (including additional software, if desired) on client macOS computers.

No manual steps beyond initiating the process are needed, let alone physically visiting the computer. All that is required is that a LANrev agent is already installed on the computer.

Remotely reinstalling client computers running OS X 10.11 (El Capitan) and up is not possible when System Integrity Protection (SIP) is enabled on those computers.

IMPORTANT This process completely reinstalls a target computer's hard disk. It is in its nature to irrecoverably delete the target volume's previous contents. Before going ahead, you should therefore make absolutely sure that no important data is lost.

Reinstalling macOS client computers requires just a few simple steps:

- Create a disk image with the desired hard disk contents.
- Optionally create a disk image specification in the Software Distribution Center (when you expect to use the image repeatedly).
- Select the target macOS computers, choose **Reinstall macOS Computer**, and specify the disk image to be used.

When you tell LANrev to reinstall a client computer, it stops all processes running on that computer, erases the specified hard disk – optionally preserving user folders and network settings –, copies the disk image's contents to the hard disk, and reboots the computer.

To reinstall a macOS computer:

1. Install on a hard disk volume the operating system.

2. Install and configure the LANrev agent.

   In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

   Note: If you do not include LANrev Agent on the disk image, reinstallation is still possible but LANrev will be unable to administer the reinstalled client computers until LANrev Agent is installed on them once more.

3. Install any additional software that you want to be present on the client computers.

4. Create a disk image from the boot volume, for example, using Apple's Disk Utility, and save it on your computer.

   The disk image file must be saved in Apple's .dmg format or any other format that can be mounted on the client computers without requiring additional software.

   For performance reasons, we recommend saving the image file as a compressed image, using the appropriate option in Disk Utility.

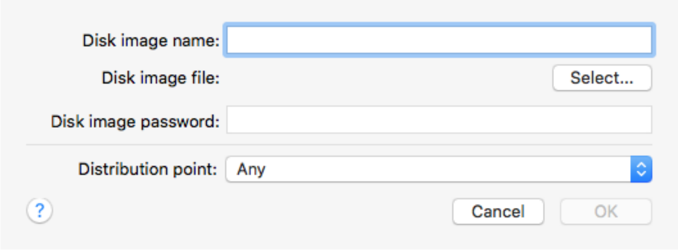
5. If you plan to use the image only once, skip to step 10.

   If you plan to reuse the disk image, create a disk image specification as described in the following steps.

   Note: Setting up disk images as described in the next steps is possible only for administrators with the **Modify Disk Image** *right. See "New Administrator" on page 758 for details.*

6. Open the **Server Center** window, right-click in the left-hand sidebar, and choose **Software Distribution** > **New Disk Image** from the context menu.

   The **Disk Image** dialog opens:



7. Enter the disk image specification:

   - **Disk image name**: The name that you want to give the disk image specification for purposes of identifying it within LANrev.
   - **Disk image file**: The file that contains the disk image. LANrev supports Apple's .dmg format as well as any other disk image that can be mounted without additional software on the target computer, for example, ISO images (.iso) or Active Disk Image images (.adi).
   - **Disk image password**: If the image is password-protected, enter the password here.
   - **Distribution point**: This option specifies from which distribution points the target computer may download the image:
     - **Any**: The image can be downloaded from any distribution point on which it is found.
     - **From assigned distribution point if available**: The image is downloaded from a distribution point that is assigned to the target computer's subnet or a computer group to which the target computer belongs. If the image is not available on any such distribution point, it is downloaded from another distribution point.
     - **From assigned distribution point only**: As above, but if the image is not available, the installation fails.

8. Click **OK** to save the disk image specification.

   If desired, create more disk image specifications.

9. From the **Server** menu, choose **Save Distribution and Licensing Info** to store the changes on the server.

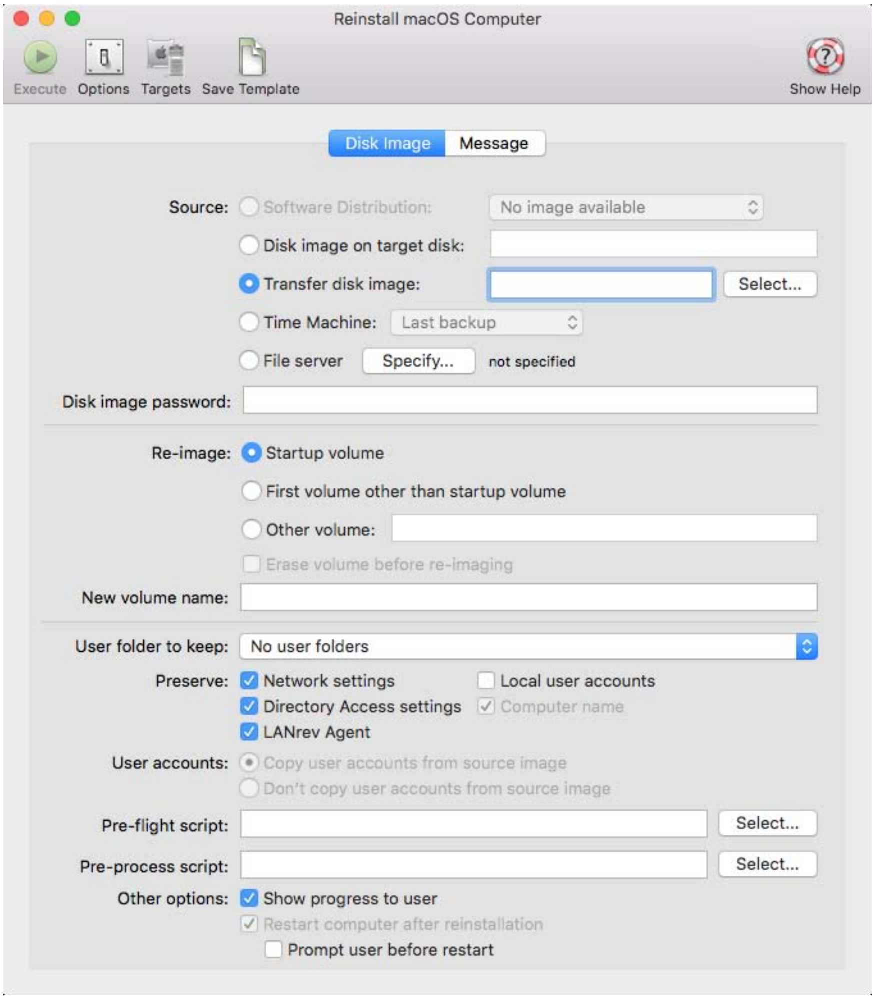
   You can start using the new disk image through the Software Distribution Center when the upload is complete.

   Note: While disk images can be stored in the Software Distribution Center, they cannot be assigned to computer groups as software packages can. Applying a disk images to a clients computer is only possible by explicitly selecting that computer and choosing the Reinstall macOS Computer command.

10. In any browser window, select the macOS computers that you want to reinstall.

11. From the **Commands** menu, choose **Reinstall macOS Computer**.

    The **Reinstall macOS Computer** dialog opens:



Source: ○ Software Distribution: No image available
○ Disk image on target disk:
● Transfer disk image: Select...
○ Time Machine: Last backup
○ File server Specify... not specified

Disk image password:

Re-image: ● Startup volume
○ First volume other than startup volume
○ Other volume:
□ Erase volume before re-imaging

New volume name:

User folder to keep: No user folders

Preserve: ☑ Network settings □ Local user accounts
☑ Directory Access settings ☑ Computer name
☑ LANrev Agent

User accounts: ● Copy user accounts from source image
○ Don't copy user accounts from source image

Pre-flight script: Select...

Pre-process script: Select...

Other options: ☑ Show progress to user
☑ Restart computer after reinstallation
□ Prompt user before restart

12. In the **Disk image source** section, specify the disk image that is to be the source of the reinstallation.

The individual options in this dialog are described in “Reinstall macOS Computer” on page 420.

13. In the **Destination** section, specify the volume on which the disk image’s content is to be installed.

IMPORTANT The option to install on the first volume other than the startup volume is primarily intended to allow you to reinstall the (sole) local volume of a computer that has been booted from a network volume. If there are more than two volumes on a client, there is no way to tell which of the non-startup volumes will be chosen. We strongly recommend against using this option on computers with more than two mounted volumes.

14. In the **Options** section, specify execution options such as scripts to be executed before or after the installation, settings to keep, or user interaction options.

15. If you want to send a message to the user before the installation begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “Sending messages” on page 144.

    If you provide a **Cancel** button in the message dialog, the installation is aborted on a target computer if a user clicks **Cancel**.

    Note: If a message has been specified, this is indicated by a diamond in the dialog’s **Message** *tab.*

16. Click **Execute**.

LANrev erases the specified disks of the target macOS computers and copies the software from the disk image. Any errors are noted in the command history.

Using a previously specified disk image

To reinstall a computer using a disk image specification that is already in the Software Distribution Center, proceed as described above but start with step 10.

Reinstalling a Windows computer

Using the software distribution system, LANrev can remotely reinstall the operating system (including additional software, if desired) on client computers, provided an additional server has been set up as described in “Installing support for reinstalling Windows computers” on page 22.

No manual steps beyond initiating the process are needed, let alone physically visiting the computer. All that is required is that a LANrev agent is already installed on the computer.

Windows computers can be reinstalled, provided that the computer is set to boot from the network first. This is possible even if no agent is installed on them.

IMPORTANT This process completely reinstalls a target computer's hard disk. It is in its nature to irrecoverably delete the target volume's previous contents. Before going ahead, you should therefore make absolutely sure that no important data is lost.

Reinstalling a Windows computer involves these main steps:

1. Create a disk image with the desired hard disk contents and save it on a distribution point. The distribution point must run on Windows, not on macOS.

   The details of this step differ depending on which PXE server you use. See the appropriate section for details:

   - **Preparing a disk image using the LANrev PXE server** (page 341)
   - **Preparing a disk image using FOG** (page 344)

2. Schedule the computer for reinstallation and restart it.

   For details, see "Reinstalling Windows client computers" on page 345.

When you tell LANrev to reinstall a client computer, it reboots the computer from the PXE server. It then erases the computer's boot disk and installs the content of the specified disk image on it. After that, the computer is rebooted from the reinstalled hard disk.

For details, see:

- **Preparing a disk image using the LANrev PXE server** (page 341)
- **Preparing a disk image using FOG** (page 344)
- **Reinstalling Windows client computers** (page 345)

Preparing a disk image using the LANrev PXE server

Preparing disk images using the procedure below requires that an LANrev PXE server is properly set up in your network, as described in "Setting up the LANrev PXE solution" on page 22.

To create a disk image:

1. Install the operating system on a Windows computer.

2. Create an empty file `C:\AMFOGImage` or `C:\AMImage`.

3. Install and configure the LANrev agent.

In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

Note: If you do not include LANrev Agent on the disk image, reinstallation is still possible but LANrev will be unable to administer the reinstalled client computers until LANrev Agent is installed on them once more. Also, the computer cannot automatically join a domain and the computer name is not set.

4. Install any additional software that you want to be present on the client computers.

5. Stop the LANrev Agent service and delete the registry value "HKLM\Software\Pole Position Software\LANrev Agent\AgentSerialno".

   Note: This is an optional but recommended step that provides a safety measure against duplicate agent IDs. LANrev can reassign new IDs when it detects a duplicate, but deleting the ID from the registry in the first place makes this process unnecessary.

6. Run the Microsoft Sysprep utility on the computer:

   - Windows Server 2003: The utility is found on the Windows installation disk in \Support\Tools\Deploy.cab. Create the directory C:\sysprep, copy Sysprep to it, and execute Sysprep using:

   ```
   C:\sysprep\sysprep.exe -reseal -mini -quiet -noreboot
   ```

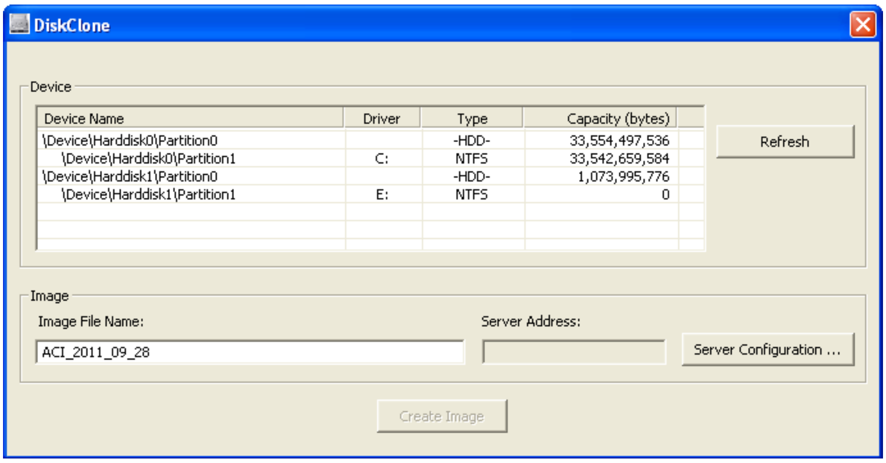
   - Windows 7 and up: The utility is installed on the boot disk by default. Execute it with the following command (all in one line):

   ```
   C:\windows\system32\sysprep\sysprep.exe
   /generalize /oobe /quiet /quit
   /unattend:C:\windows\system32\sysprep\sysprep.xml
   ```

   See the Sysprep documentation for details, including creating an answer file.

7. Restart the computer, enter the BIOS configuration, and set it to boot from the network.

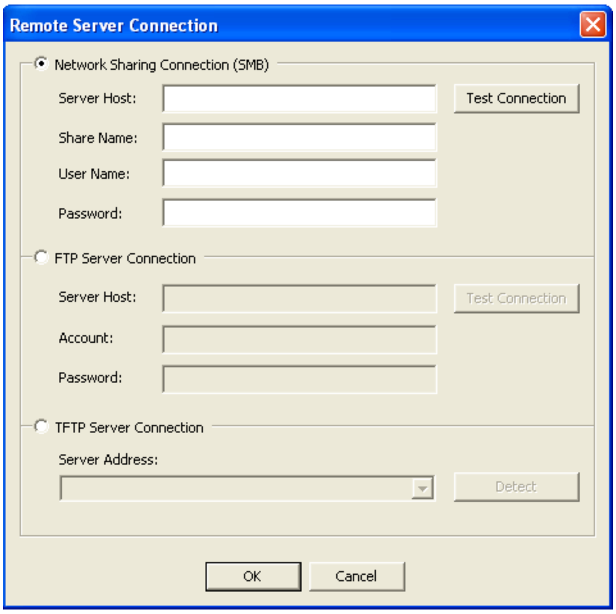
8. After a short delay, the DiskClone tool is displayed:



Device Name	Driver	Type	Capacity (bytes)
\Device\Harddisk0\Partition0		-HDD-	33,554,497,536
\Device\Harddisk0\Partition1	C:	NTFS	33,542,659,584
\Device\Harddisk1\Partition0		-HDD-	1,073,995,776
\Device\Harddisk1\Partition1	E:	NTFS	0

Image File Name: ACI_2011_09_28

9. Click **Server Configuration** to open the **Remote Server Connection** dialog:



● Network Sharing Connection (SMB)

10. Enter the address and access information for an SMB share or an FTP server on which you want the image file to be created.

    We do not recommend using TFTP because it does not support any kind of authentication.

11. Click **Test Connection** to verify that the connection is working. When it is, click **OK**.

12. In the device list, select the hard disk from which you want to create the installation image.

    We recommend that you choose a complete hard disk (a row with “HDD” in the **Type** column), not a partition (a row with a file system name in the **Type** column).

13. Enter the desired name for the image file in the **Image File Name** field.

14. Click **Create Image**.

    The disk contents is transferred to the specified server share.

When the transfer is complete, you can use this disk image to reinstall client computers, as described in “Reinstalling Windows client computers” on page 345.

Preparing a disk image using FOG

Preparing disk images using the procedure below requires that an FOG server is properly set up in your network, as described in “Setting up the FOG solution” on page 24.

To create a disk image:

1. Install the operating system on a Windows computer.

2. Create an empty file `C:\AMFOGImage`

3. Install and configure the LANrev agent.

   In particular, set the inventory server and, if you employ them, the software distribution server and the license monitoring server.

   Note: If you do not include LANrev Agent on the disk image, reinstallation is still possible but LANrev will be unable to administer the reinstalled client computers until LANrev Agent is installed on them once more. Also, the computer cannot automatically join a domain and the computer name is not set.

4. Install any additional software that you want to be present on the client computers.

5. Stop the LANrev Agent service and delete the registry value “HKLM\Software\Pole Position Software\LANrev Agent\AgentSerialno”.

   Note: This is an optional but recommended step that provides a safety measure against duplicate agent IDs. LANrev can reassign new IDs when it detects a duplicate, but deleting the ID from the registry in the first place makes this process unnecessary.

6. Run the Microsoft Sysprep utility on the computer:

   - Windows Server 2003: The utility is found on the Windows installation disk in \Support\Tools\Deploy.cab. Create the directory C:\sysprep, copy Sysprep to it, and execute Sysprep using:

```
C:\sysprep\sysprep.exe -reseal -mini -quiet -noreboot
```

   - Windows 7 and up: The utility is installed on the boot disk by default. Execute it with the following command (all in one line):

```
C:\windows\system32\sysprep\sysprep.exe
/generalize /oobe /quiet /quit
/unattend:C:\windows\system32\sysprep\sysprep.xml
```

See the Sysprep documentation for details, including creating an answer file.

7. Using FOG, create a disk image of the computer as described in the FOG documentation.

   Choose an image type depending on the operating system and partitioning scheme:

   - For Windows Server 2003 with a single partition, choose **Single Partition (NTFS only, Resizable)**.
   - For Windows Server 2003 with multiple partitions (for example, when there is a recovery partition), choose **Multiple Partition Image - Single Disk (Not Resizable)**.
   - For Windows 7 and up, choose **Multiple Partition Image - Single Disk (Not Resizable)**.

You can now use this disk image to reinstall client computers, as described below.

Reinstalling Windows client computers

When a PXE server is properly set up (as described in “Installing support for reinstalling Windows computers” on page 22) and a suitable disk image has been created (as described in “Preparing a disk image using the LANrev PXE server” on page 341 and “Preparing a disk image using FOG” on page 344), you can reinstall administered Windows computers:

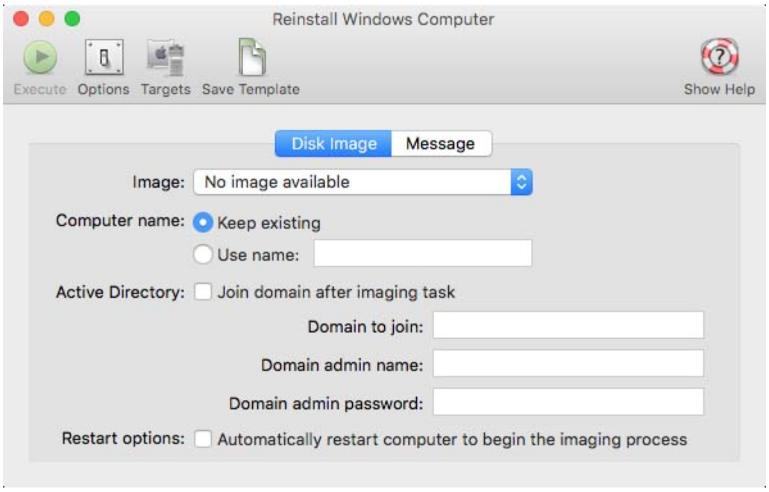
1. In any browser window, choose the computers you want to reinstall.

   All selected computers will receive the same disk image.

   You can also select computers on which no agent is installed if you have created placeholder records for them, as described in “Creating placeholder records for computers” on page 90.

2. From the **Commands** menu, choose **Reinstall Windows Computer**.

The **Reinstall Windows Computer** dialog opens:



Reinstall Windows Computer

Image: No image available

Computer name: ● Keep existing

○ Use name:

Active Directory: □ Join domain after imaging task

Domain to join:

Domain admin name:

Domain admin password:

Restart options: □ Automatically restart computer to begin the imaging process

3. From the **Image** pop-up menu, choose the desired disk image to be used for reinstalling the computers.

4. In the Computer name section, specify a new name for the selected computers or choose **Keep existing** to not change them.

5. In the **Active Directory** section, specify whether the reinstalled computers are to join a domain.

   If they are to join a domain, provide the name of the domain and administrator credentials for the domain.

6. If you want the reinstallation to proceed automatically when you send the command, check the **Automatically restart computer to begin imaging process** option.

   If this option is not checked, the target computers must be restarted manually before they will be reinstalled.

   The option has no effect for target computers on which no agent is installed; that is, such computers must always be manually restarted.

7. If you want to send a message to the user before the installation begins, click the **Message** tab. Using this tab is similar to using the **Send Message** command as described in “Sending messages” on page 144.

   If you provide a **Cancel** button in the message dialog, the installation is aborted on a target computer if a user clicks **Cancel**.

   Note: If a message has been specified, this is indicated by a diamond in the dialog’s ***Message*** *tab.*

8. Click **Execute**.

LANrev sends instructions to the PXE server to reinstall the computers after their next restart. If you have checked the **Automatically restart computer to begin imaging process** option, LANrev also instructs the agents to restart the target computers.

Note that the target computers must be set to boot from the network first in order for the reinstallation to be possible.

9. If no agent is installed on the target computers or you have not checked the **Automatically restart computer to begin imaging process** option, restart the target computers manually.

   Make sure that they boot from the network first. Many BIOSes allow you to specify the boot order on the fly by pressing the F10 or F12 key during the boot process.

The target computer reboot from the network. The PXE server provides them with the specified disk image and controls the reinstallation process.

The reinstallation task is displayed in the **Window Reinstallation Tasks** window.

Chapter 9 Monitoring licenses

LANrev allows you to monitor the installation and use of licensed software on the computers in your network, record purchasing and maintenance agreement details, and create reports on historic usage, ensuring compliance with licensing limits.

You can also specify software that is prohibited in your network and have all instances of this software be reported and optionally terminated automatically.

The various aspects of license monitoring are explained in:

- “Overview” on page 348
- “Setting up license specifications” on page 349
- “Exporting and importing license specifications” on page 353
- “Tracking purchasing information” on page 354
- “Setting up computer groups” on page 358
- “Configuring agents” on page 358
- “Checking licenses” on page 361
- “Reports” on page 362

Overview

The License Monitoring Center is a module of LANrev Server that provides constant automated monitoring of both per-installation and concurrent-use licenses as well as prohibited software. It also provides a repository for information related to license purchases and maintenance agreements.

This section discusses the basics of license monitoring and provides an overview of setting it up.

Prerequisites

Some functions of the License Monitoring Center can be used only by administrators whose accounts have certain rights enabled.

Configuring administrator accounts is described in “Administrator accounts” on page 72.

Setup

Setting up license monitoring involves defining license specifications – which define the software to be monitored and the licensing parameters and optionally include purchasing and maintenance agreement information – and computer groups – groups of computers that are considered together for purposes of license monitoring. This is described in “Setting up license specifications” on page 349 and “Setting up computer groups” on page 358.

Optionally, you can configure on the agents the servers to which they send reports. (If you do not configure this setting, reports are sent to the default inventory server.) This is described in “Configuring agents” on page 358.

You can also configure the times and intervals for checking for licensed software as well as the intervals for sending information to the server. This is described in “Configuring agents” on page 358.

If everything has been set up, license specifications are assigned to groups. The compliance with these specifications is then monitored and recorded by LANrev Server. This is described in “Checking licenses” on page 361; the available reports are discussed in “Reports” on page 362.

Prohibited software

If there is software the use of which is prohibited in your network, you can use LANrev to check for the presence of such software. This is done in exactly the same way as license monitoring; all that is required is to mark the software “prohibited” in the license specification.

Setting up license specifications

License specifications combine a definition of an application with information on the available licenses and status (prohibited or not).

License specifications can describe per-use (concurrent) licenses, per-seat (per-installation) licenses, or prohibited software. All three types are defined in the same way; the differences are in step 5 only.

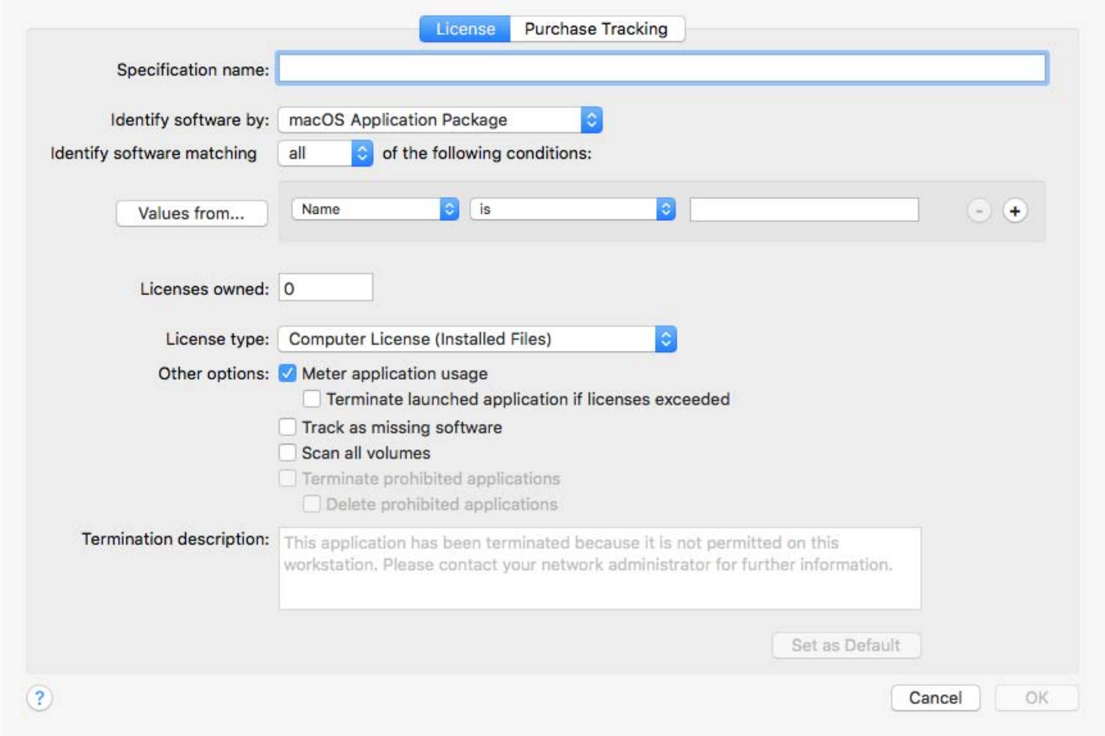
License specifications combine a definition of an application with information on the available licenses and status (prohibited or not).

NOTE License specifications can be created, edited, or deleted only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 758 for details.

To create a license specification:

1. From the action menu of the **Server Center**, choose **License Monitoring** > **New License Specification**.

The **Software License Specification** dialog opens:



Specification name:

Identify software by: macOS Application Package

Identify software matching all of the following conditions:

Name is

Licenses owned: 0

License type: Computer License (Installed Files)

Other options: ☑ Meter application usage

□ Terminate launched application if licenses exceeded

□ Track as missing software

□ Scan all volumes

□ Terminate prohibited applications

□ Delete prohibited applications

Termination description: This application has been terminated because it is not permitted on this workstation. Please contact your network administrator for further information.

2. Enter the desired name in the **Specification name** field.

   You can choose any desired name.

3. Choose the type of software that is to be monitored. Your choice in this menu determines, what kind of data LANrev considers when checking whether the licensed software is installed on an administered computer:

   - **macOS Application Package**: macOS packages (a folder appearing as a file) are checked.
   - **macOS Application File**: macOS files are checked. Files are only considered to match if they are executable applications.
   - **macOS File**: macOS files are checked.
   - **macOS Installer Receipt**: Installer receipts are checked. Installer receipts are descriptions of installed software in the form of an installer package that some macOS installers create.
   - **Windows Application File**: Windows files are checked. Files are only considered to match if they are executable applications.
   - **Windows File**: Windows files are checked.
   - **Windows Installer Receipt**: The reports on installed software that MSI installers create are checked.
   - **Windows Installed Software**: Software that is installed on the computer (as listed in the “Add/Remove Programs” or ”Programs and Features” control panel) is checked.

- **Windows Registry**: The contents of the Windows registry is checked.

4. Specify the conditions that an object must match to be identified as the licensed software.

   You can click the **Values from** button to insert default comparison value from a file on your computer.

   The available conditions are explained in “Files” on page 867 or “New License Specification” on page 732, depending on the software type selected.

   When you specify a path or registry location, you can include environment variables, as described in “Environment variables” on page 176.

   Note: When you specify a license by Windows registry data, you should use the **Key Name** *and* **Value Name** *conditions only when there is no other way to specify the desired software. Checking either condition requires the entire registry to be parsed, which generates significant local processor load on the client computer and also takes a while. If you do require either condition, specify it after any other conditions that may apply because that causes LANrev to apply it only to the part of the registry that meets those other conditions.*

   Note: When specifying a file version, make sure to use the right format (three numbers for macOS files, four for Windows files), as described in “Gathering information on files” on page 102.

5. Enter the number of available licenses.

   Note that this field is disabled if you have chosen to have LANrev calculate the number of available licenses automatically from the purchase records, as described in “Tracking purchasing information” on page 354.

6. Choose the type of the license:

   - **Computer License (Installed Files):** The license governs how many copies of the software may be installed in your network.
   - **Floating License (Running Processes):** The license governs how many copies of the software may be in use at the same time.
   - **Site License:** This type is for software that may be used without restriction throughout your network. You can also choose it when you want to use the license specification purely for monitoring purposes.
   - **Prohibited Application**: Software that is not allowed in your network. This is not really a license type; however, this setting allows you to use the license-checking mechanism to watch for the presence of undesirable software.

7. Set the other options:

   - Check **Meter application usage** if you want LANrev to not only scan the hard disks but also monitor the running processes for the licensed software and store the numbers for later reports.
     Note: Only applications on administered computers that have a working network connection to the server are included in the count.
     If you want LANrev agents to automatically terminate any applications launching which exceeds the available license count, check **Terminate launched applications if licenses exceeded**.
     When an application is automatically terminated, a message informs the local user about the reason; you can specify the text for this message in the **Termination description** field.
   - If you want LANrev agents to automatically terminate any prohibited application on their computers, check **Terminate prohibited applications**. (This option is available only when you have set the license type to "Prohibited Application".)
     To also delete the offending application, check the **Delete prohibited applications** option.
     When an application is automatically terminated, a message informs the local user about the reason; you can specify the text for this message in the **Termination description** field.
   - If LANrev is to provide an overview of the computers on which this software is not available, check **Track as missing software**.
     Note: Usually, you will want to activate this option only for software that should be installed on all or most of the administered computers. Tracking applications intended only for a few computers can clutter up the display of missing applications.
   - If you want LANrev to look for the licensed software on all local volumes of administered computers, check **Scan all volumes**. Otherwise, only the boot volume is scanned.

8. If desired, you can enter details of license purchases and maintenance agreements, as described in "Tracking purchasing information" on page 354.

9. Click **OK** to close the dialog.

10. To store the license specification on the LANrev server, choose **Save Distribution and Licensing Info** from the **Server** menu.

    You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but the new license specification becomes available to the License Monitoring Center only after you have done so.

Editing license specifications

To edit an existing license specification, select it in the sidebar of the **Server Center** window and choose **Edit License Specification** from the action menu.

The **Software License Specification** dialog opens that is described above.

After you have completed editing the specification, click **OK** and choose **Save Distribution and Licensing Info** from the **Server** menu to save the changes to LANrev Server.

Deleting license specifications

To delete an existing license specification, select it in the sidebar of the **Server Center** window and choose **Remove License Specification** from the action menu.

The license specification is deleted.

Choose **Save Distribution and Licensing Info** from the **Server** menu to save the changes to LANrev Server.

Exporting and importing license specifications

You can export license specifications from LANrev for importing into another installation.

NOTE Exporting and importing license specification is possible only for administrators with the **Modify License Specification** right. See “New Administrator” on page 758 for details.

Exporting license specifications

To export license specifications:

1. In the **Server Center** window, select the license specifications you want to export.
2. Right-click and choose **Export License Specification** from the context menu.

   A standard Save dialog is displayed.
3. Specify the name and location for the exported specifications and click **Save**.

The packages are exported as a file.

Importing license specifications

To import license specifications:

1. Choose **File** > **Import** > **License Specifications**.

   A standard Open dialog is displayed.

2. Select the exported license specification file you want to import and click **Open**.

The specifications are imported into your installation of LANrev Server and are thereafter available to all administrators.

Tracking purchasing information

As part of a license specification, you can also record details of purchases of the software in question, including updates and maintenance agreements.

NOTE Purchase tracking information can be entered and edited only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 758 for details.

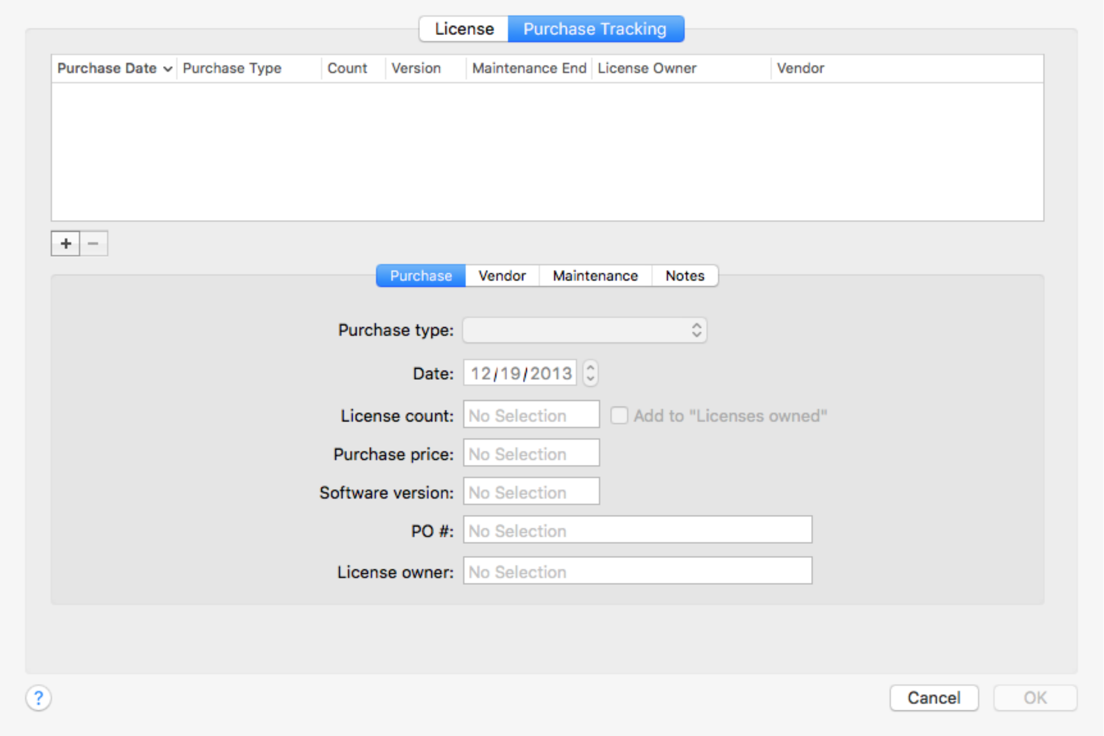
Entering new purchasing information

To enter purchasing or maintenance agreement information for a software:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

   The **Software License Specification** dialog opens.

2. Click the dialog’s **Purchase Tracking** tab:



Purchase Date	Purchase Type	Count	Version	Maintenance End	License Owner	Vendor

Purchase type:

Date: 12/19/2013

License count: No Selection □ Add to "Licenses owned"

Purchase price: No Selection

Software version: No Selection

PO #: No Selection

License owner: No Selection

3. To enter details of a new purchase – of any type: new software, software update, maintenance agreement, or maintenance extension – click the **+** button below the list.

4. Enter the information in the four subpanes. These subpanes’ fields are described in “Purchase Tracking” on page 736.

   Note that checking the **Add to “Licenses owned”** option in the **Purchase** subpane makes LANrev add up all your license purchases to automatically fill the license specification’s **Licenses owned** field. Manual entry into that field is disabled in this case.

5. Click **OK** to close the dialog.

6. To store the new information on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

   You do not need to save the changes to LANrev Server immediately (you can perform additional setup steps before doing so), but you must do so before quitting LANrev Admin – otherwise the changes will be lost.

Editing purchasing information

To edit existing information on license purchases or maintenance agreements:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

   The **Software License Specification** dialog opens.

2. Click the dialog’s **Purchase Tracking** tab.

3. In the list in the upper part of the tab, select the entry that you want to edit.

4. The entry’s information is displayed in the subtabs in the lower half of the dialog.

5. Edit the information as desired.

6. Click **OK** to close the dialog.

7. To store the new information on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

Importing purchasing information

You can import existing purchasing information from a different system as tabular data. If data belongs to a purchase that is already tracked in LANrev, that purchase’s information is updated. Otherwise, a new purchase record is created.

The process below describes transferring the data using a template supplied by HEAT Software. You can also create the required tabular import file in other ways as long as it has the same structure (see “License purchase data import file” on page 388 for details). If you do, begin the procedure with step 5.

To import purchase data using the template file:

1. Transfer your existing purchase data into a copy of the “License Purchase Data Template.xlsx” file that is available from the Resource Center.

   The details for doing so depend on how your data is currently stored and are beyond the scope of this manual.

   The individual columns of the template are described in “License purchase data import file” on page 388.

2. Make sure that the first four columns are filled for each record you want to import.

These columns are used to match imported data with existing records: If all four are the same as the corresponding values of an existing record, that record is updated with the imported values. If no matching record is found, a new record is created from the import data.

3. Make sure that all date formats are correct in the Purchase Date, Maintenance Start, and Maintenance End columns.

   Dates must be in the format set in the operating system on the computer where you import the file – specifically the medium format on macOS and the short format on Windows. For example, if US English formats are chosen, the date format would have to be “12/25/2014”; for German, it would have to be “25.12.2014”.

4. Export the table as a tab-delimited text file.

   If required, see the Excel documentation for details on doing so.

5. In LANrev Admin, choose **File** > **Import** > **License Purchase Data**.

   An Open dialog is displayed.

6. Select the tab-delimited file and click **OK**.

   LANrev imports the information from the file, updating and adding records as described above. When the import is complete, a summary of the imported data is displayed.

7. Choose **Server** > **Save Distribution and Licensing Info**.

Deleting purchasing information

To delete existing information on license purchases or maintenance agreements:

1. In the **Server Center** window, right-click the license specification of the software in question and choose **Edit License Specification**.

   The **Software License Specification** dialog opens.

2. Click the dialog’s **Purchase Tracking** tab.

3. In the list in the upper part of the tab, select the entry that you want to delete.

4. Click the **–** button below the list.

   The selected purchasing or maintenance agreement record is removed.

5. Click **OK** to close the dialog.

6. To store the new information on LANrev Server, choose **Save Distribution and Licensing Info** from the **Server** menu.

Setting up computer groups

Computer groups are collections of computers that can use the available licenses or that are otherwise to be considered together for software monitoring purposes. One computer can belong to multiple computer groups, allowing great flexibility through overlapping groups.

NOTE Computer groups can be set up only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 758 for details.

The same computer groups are used for license monitoring and software distribution. Creating and maintaining these groups is described in “Setting up computer groups” on page 324.

Configuring agents

The details of license monitoring can be configured individually on each LANrev agent:

- The intervals in which the agents check the hard disks for licensed software and the times of the day and the week in which they are doing so. (If the License Monitoring Center is configured to monitor running processes for licensed software, it does so constantly.)
- The LANrev server to which they send license monitoring information and the interval in which they do so.

Configuring the checking intervals and times will often be unnecessary as the defaults serve most organizations well.

Configuring agents

To configure LANrev agents for license monitoring:

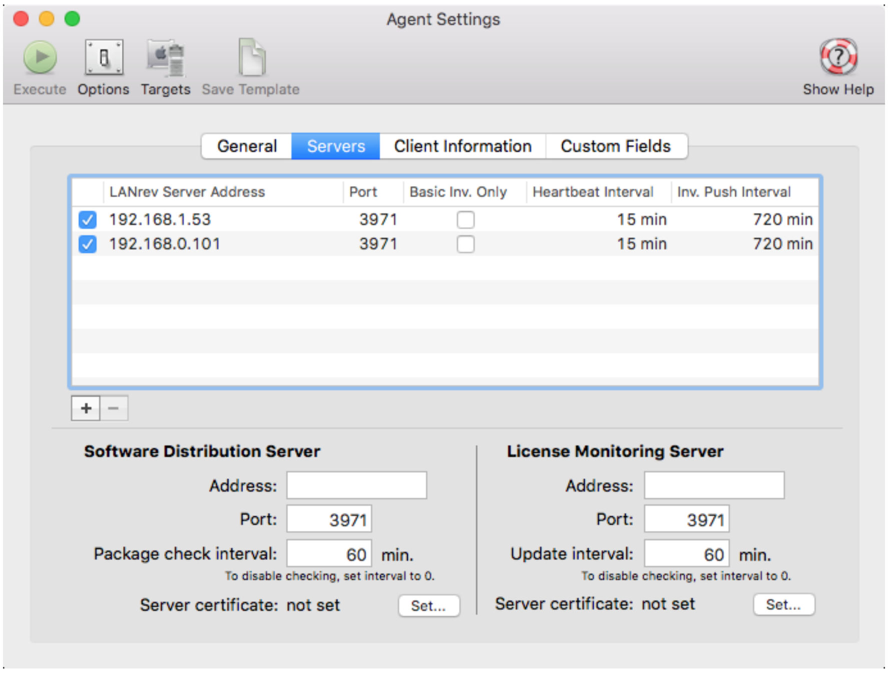
1. In any browser window, select the computers on which you want to configure the agents.

   Note: For information on specifying groups as targets, see “Targets” on page 404.

2. From the **Commands** menu, choose **Agent Settings**.

   The **Agent Settings** dialog opens.

3. Click the **Servers** tab:



	LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval
☑	192.168.1.53	3971	□	15 min	720 min
☑	192.168.0.101	3971	□	15 min	720 min

Software Distribution Server

Address:

Port: 3971

Package check interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set

License Monitoring Server

Address:

Port: 3971

Update interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set

4. In the **License Monitoring Server** section of the dialog, enter the IP address or DNS name of the LANrev server that is to be the selected agents' license monitoring contact, the port on which the server listens to traffic from the agents, and the desired interval in which agents check the server for new licensing information.

   Note: If you enter an abbreviated DNS name (that is, a partial name that is completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).

5. If the **Server certificate** field does not display "valid", click the **Set** button and choose the certificate for the server.

   Creating server certificates is described in "Exporting a server certificate" on page 21.

   Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

6. Click **Execute**.

Configuring intervals

You can configure the interval in which Agents scan the hard disks for installed licensed software and the interval in which they send reports to the server. These intervals are the same for all Agents connected to a particular license monitoring server.

NOTE The interval for scanning for running applications is not set. In contrast to scans of hard disks, such scans consume only negligible processor power and so are always performed frequently – usually about once per minute.

Configuring these intervals and times will often be unnecessary as the defaults serve most organizations well.

To set the intervals:

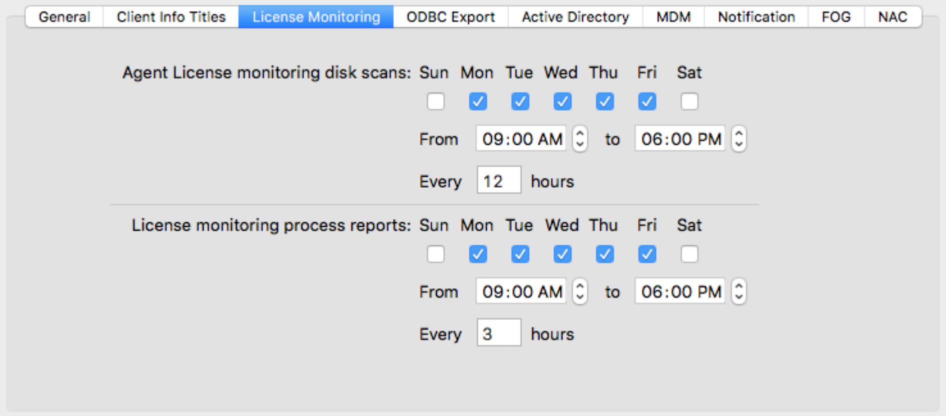
1. Make sure that you are connected to the license monitoring server that you want to configure.

2. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

3. In the **Server Center** windows sidebar, click **Server**.

   The **Server Settings** dialog is displayed in the **Server Center** window.

4. Click the **License Monitoring** tab:



Agent License monitoring disk scans: Sun Mon Tue Wed Thu Fri Sat
□ ☑ ☑ ☑ ☑ ☑ □
From 09:00 AM to 06:00 PM
Every 12 hours

License monitoring process reports: Sun Mon Tue Wed Thu Fri Sat
□ ☑ ☑ ☑ ☑ ☑ □
From 09:00 AM to 06:00 PM
Every 3 hours

5. In the **Agent License monitoring disk scans** section, specify the days of the week and the period during the day when license scans are to be performed and the interval of such scans.

   These settings are provided to avoid sending meaningless data to the server. For example, nothing happens in a normal office at 3 am, so there is no need to monitor license compliance when this has happened at 6 pm and will happen again at 9 am.

Note: Because of a limitation in the operating system, midnight at the end of the day cannot be specified as "24:00" when using a 24-hour clock. Enter "0:00" instead.

6. In the **License monitoring disk scans** section, specify the period during which Agents are to send licensing reports to the server and the interval for sending these reports.

   These reports also include results of scans for running software (if any license specifications include such scans), which are performed about once per minute.

7. Click **OK**.

The updated settings are sent to the server with the regular license monitoring updates. (The interval for these updates is specified in the **Servers** tab of the **Agent Settings** command window.)

Checking licenses

Once licenses and computer groups are set up, checking licensing compliance requires assigning licenses to groups.

LANrev Server then automatically transmits the information about what to look for to all relevant LANrev agents. These agents check their hard disks and, if so configured, running processes according to their individual settings for the specified software and return the results to the server.

Automatic and manual scans

Normally, both the local scans for licensed or prohibited software happen in regular intervals, as specified in the **Agent Settings** dialog. If you want to check for software immediately, outside the normal schedule, you can do so:

1. In any browser window, select the computers on which you want to check for software.

   Note: For information on specifying groups as targets, see "Targets" on page 404.

2. From the **Commands** menu, choose **Run License Monitoring Scan**.

3. Click **Execute**.

LANrev Server instructs the agents on the selected computers to scan immediately for all licenses that have been assigned to computer groups to which they belong. The agents send the results to the server immediately after they have completed their scans, irrespective of the schedule set in the **Servers** tab of the **Agent Settings** dialog for doing so.

Scan results

The results of all scans – manual or automatic – are collected by LANrev Server and presented to connected admins as a series of reports. These reports are discussed below.

Reports

The results of the license monitoring are presented by LANrev in a number of reports.

There are predefined reports; you can also define custom reports that also take the form of groups of database records.

Both predefined and custom reports are described below.

Understanding predefined reports

The predefined reports included with LANrev answer the issues that are most commonly considered in relation with license monitoring:

- **Fully compliant**: A list of all software for which the license numbers are observed.
  This report includes all license specifications where the total number of copies of the software found in all computer groups to which the specification was assigned does not exceed the number of available licenses.
  Note: New licenses may be included in the category even though they are exceeded because not all relevant agents have yet reported on them.
- **Licenses exceeded**: A list of all software that is currently used more often than permitted.
  This report includes all license specifications where the total number of copies of the software found in all computer groups to which the specification was assigned is higher than the number of available licenses.
- **Prohibited software**: A list of all copies of prohibited software in the network.
  This report includes all pairs of license specifications for prohibited software and computers that have been found, that is, if software declared prohibited in its license specification has been found on a computer, there is an entry stating the license, the computer, and the number of copies found.
- **Undetermined licenses**: Licenses for which no information has been returned from any agents.
  This report includes new licenses for which no agent has yet reported finding or not finding the specified software. If licenses remain in this report for an extended period of time, they may not have been assigned to any computer group.
- **Software usage**: A list of all copies of licensed or prohibited software.

This report includes all pairs of license specifications and computers that have been found, that is, if the software of a license specification has been found on a computer, there is an entry stating the license, the computer, and the number of copies found.

- **Missing software**: A list of all software that should be installed on a computer but is not.
  This report includes all pairs of license specifications and computers that have not been found. Any computer is checked for all licenses that have been assigned to a computer group to which it belongs, except prohibited software.
  If any of the software is not found on the computer, an entry in this report is generated stating the license and the computer.
- **History**: A trail of license numbers.
  This report includes time-stamped entries of license summaries. Each entry includes the license specification and the number of copies of the specified software found throughout the network.

Creating custom reports

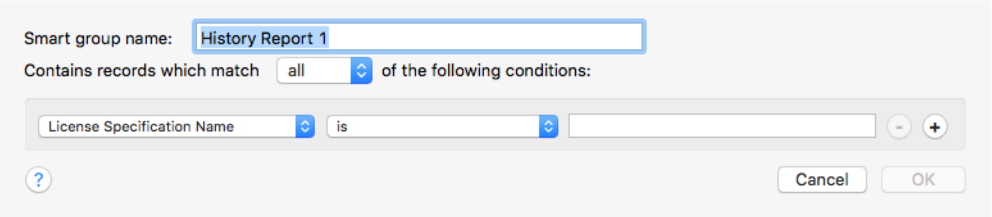
You can create custom reports to complement the predefined ones:

1. Open the **Server Center** window by choosing **Server Center** from the **Window** menu.

2. From the action menu’s **License Monitoring** section, choose one of these commands:

   - **New License Status Report** to create a report on the status of license specifications, similar to the **Fully compliant**, **Licenses exceeded**, or **Prohibited software** reports.
   - **New Software Usage Report** to create a report on the usage of licensed software on individual computers, similar to the **Software usage** report.
   - **New History Report** to create a report on past counts of licensed software, similar to the **History** report.
   - **New History Summary Report** to create a statistical report on the usage levels of licensed software in a selectable period, similar to the **History summary** report.
   - **New Missing Software Report** to create a report on the computers lacking a particular piece of licensed software, similar to the **Missing software** report.

   In each case, the **Smart Group** dialog opens:



Smart group name: History Report 1

Contains records which match all of the following conditions:

License Specification Name is

All five dialogs are similar; they differ only in the contents of the left-hand pop-up menu.

3. Enter a name for the report.

4. Specify the conditions that a license specification, software usage information, or history entry must match to be included in the report.

   To do so, choose an information from the left-hand pop-up menu, a relation from the pop-up in the middle, and enter a comparison value in the text field.

   You can add and remove conditions using the **+** and **–** buttons.

   When using multiple conditions, use the top pop-up menu to specify whether records must match all conditions (logical AND) or any condition (logical OR) to be included in the report.

5. Click **OK** to create the report.

Editing reports

To edit an existing custom report, select it in the sidebar of the **Server Center** window and choose **Edit <Report Type>** from the action menu.

The **Smart Group** dialog opens that is described above.

You cannot edit predefined reports.

Deleting reports

To delete an existing custom report, select it in the sidebar of the **Server Center** window and choose **Remove <Report Type>** from the action menu.

The report is deleted.

You cannot delete predefined reports.

Part 3: Reference

The Reference part of the manual describes the menus, dialogs, windows, and information items of LANrev. Dialogs and windows are described together with the menu commands that open them. Complex windows are described in their own chapters.

Menus:

- “LANrev Admin menu” on page 366
- “File menu” on page 375
- “Edit menu” on page 391
- “View menu” on page 396
- “Commands menu” on page 399
- “Server menu” on page 480
- “Window menu” on page 498
- “Help menu” on page 515

Windows:

- “Browser windows” on page 517
- “Compliance Report window” on page 531
- “Mobile Devices” on page 538
- “Classroom Management” on page 649
- “Configuration profile editor” on page 666
- “Home screen layout editor” on page 679
- “Server Center” on page 684
- “Agent Deployment Center” on page 803
- “Commands window” on page 822

Information items:

- “Information items” on page 831

External tools and client software:

- “LANrev Remote” on page 939
- “LANrev Agent” on page 970
- “Mobile Apps” on page 950

Chapter 10 *LANrev Admin menu*

The **LANrev Admin** menu contains commands that apply to the entire application and its configuration:

- **About LANrev Admin** (page 366)
- **Preferences** (page 366)
- **Switch Administrator and Server** (page 372)
- **Change Administrator Password** (page 373)
- **InstallEase Key** (page 373)
- **Services submenu** (page 373)
- **Hide LANrev Admin** (page 374)
- **Hide Others** (page 374)
- **Show All** (page 374)
- **Quit LANrev Admin** (page 374)

About LANrev Admin

The **About LANrev Admin** command opens the application's About dialog. The dialog contains the application version, information on the server platform, developer credits, registration information, and copyright information. It also displays the server to which the LANrev Admin application is currently connected.

Preferences

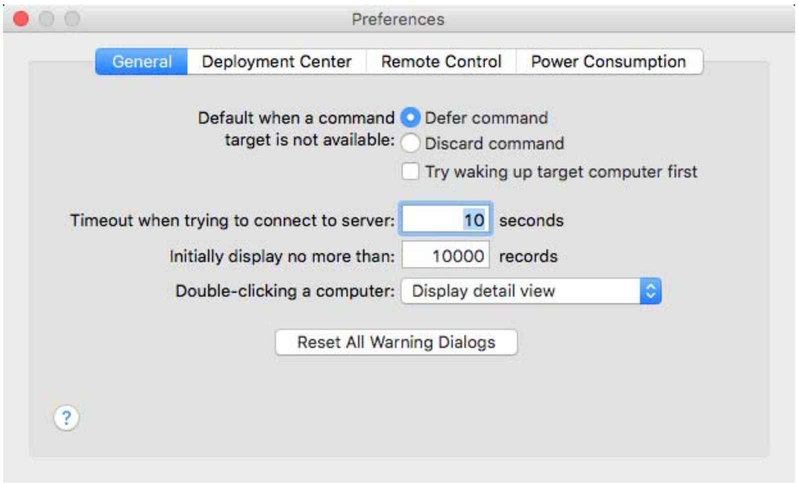
The **Preferences** command opens the **Preferences** dialog that lets you specify settings for the application:

The **Preferences** dialog has four tabs:

- **General**
- **Deployment Center**
- **Remote Control**
- **Power Consumption**

General

The **General** tab of the **Preferences** dialog lets you specify various preferences settings for LANrev Admin:



Default when a command target is not available: ● Defer command ○ Discard command

□ Try waking up target computer first

Timeout when trying to connect to server: 10 seconds

Initially display no more than: 10000 records

Double-clicking a computer: Display detail view

The tab contains these elements:

- **Default when a command target is not available**: The default behavior for cases where a target computer for a command is not available when the command is executed.
  - If you choose **Defer command**, the **Defer task if target computer is not available** option in the options dialog is checked for each new command.
  - If you choose **Discard command**, the option in the command options dialog is unchecked by default.
  - If **Try waking up target computer first** is checked, the **Wake up computer if not available** option in the command options dialog is checked by default.

  You can still change the options' settings for each command that you issue.
- **Timeout when trying to connect to server**: The time that LANrev Admin waits for responses from LANrev Server before it considers a connection attempt to have failed.
- **Initially display no more than**: This option lets you limit the number of records that LANrev Admin displays when opening a new browser window or group in a browser window.

  If a database table on the server contains more records than are displayed by LANrev Admin, there is an indication – "more…" – in the window's status bar. The additional records can be displayed by choosing **Display All Records** from the **View** menu or clicking the **more…** indicator.

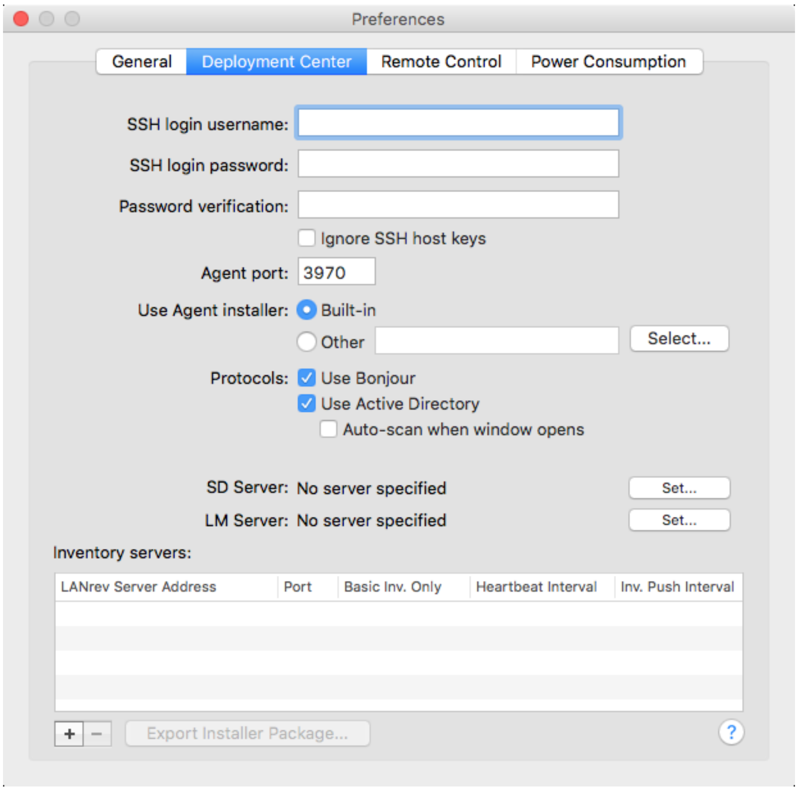
  This option is intended primarily for networks with very large database tables.
- **Double-clicking a computer**: The action that LANrev Admin takes when you double-click a computer record in a browser window.
- **Reset All Warning Dialogs**: Some of LANrev's warning alerts offer the option of turning this type of warning off for the future via a "do not show this dialog again" option. Clicking this button resets all such alerts, showing them again. (Of course,

you can turn any of these alerts off again by checking the option once more.)

Deployment Center

The **Deployment Center** tab of the **Preferences** dialog lets you specify defaults for installing LANrev Agent on administered computers or removing it.

NOTE You can override all settings when you perform an actual installation using the **Install Agent** command described on page 814 or remove LANrev Agent using the **Remove Agent** command described on page 816.



SSH login username:

SSH login password:

Password verification:

□ Ignore SSH host keys

Agent port: 3970

Use Agent installer: ● Built-in ○ Other

Protocols: ☑ Use Bonjour ☑ Use Active Directory □ Auto-scan when window opens

SD Server: No server specified

LM Server: No server specified

Inventory servers:

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

The tab contains these elements:

- **SSH login username**: The username that is to be used for SSH login on the selected computers. The account names (as well as the passwords) are case-sensitive. You must use the abbreviated username.
- **SSH login password**: The password for the SSH account.
- **Password verification**: Re-enter the password to guard against typos.
- **Ignore SSH host keys**: Checking this option skips verification of deployment target computers by their SSH host keys. This prevents error messages if the operating system of a known client is altered (for example, after reimaging). It may also allow illegitimate devices to pose as legitimate clients, particularly if physical access to your network is possible.

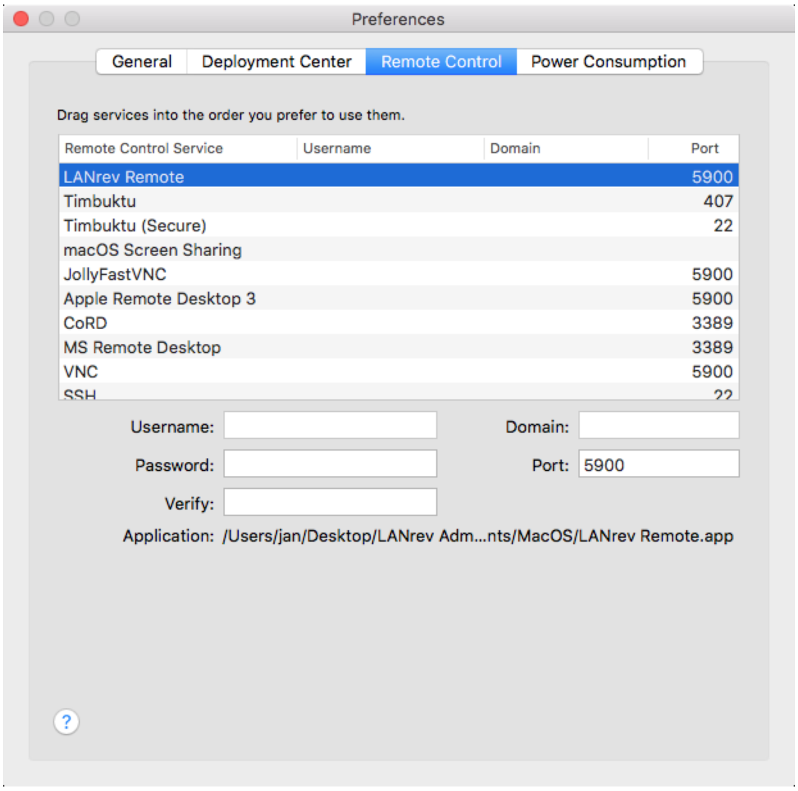
- **Agent port**: The TCP port on which the agent is to communicate with the server.
  Note: We recommend not to change the port unless you have a specific reason for doing so.
- **Use Agent installer**: Choose whether the installer embedded in LANrev Agent or a custom installer that you provide is to be used for installing the Agent.
  You can create a custom installer using the **Export Installer Package** button described below.
- **Select**: Clicking this button lets you select a custom installer.
- **Protocols**: These options let you choose which network protocols LANrev Admin is to use to detect computers on which LANrev Agent could be installed.
  For the Active Directory protocol, you can specify that LANrev automatically scans the network using that protocol. (With Bonjour, automatic scanning always happens when the protocol is activated.)
- **SD Server**: The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in "Server Properties dialog" on page 810.
- **LM Server**: The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in "Server Properties dialog" on page 810.
- **Inventory servers**: This table lists all known LANrev inventory servers.
  The list contains these columns:
  - **LANrev Server Address**: The IP address or DNS name of the server.
    Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).
  - **Port**: The port over which the server communicates with agents.
  - **Basic Inv. Only**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
  - **Heartbeat Interval**: The interval in which the agents are to contact the server to let it know that they are still available.
    Note: This interval should not be longer than the Agent Offline Threshold setting of LANrev Server. (See "Server Settings" on page 780 for details.)
  - **Inv. Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

Double-clicking a server displays a dialog for editing its settings. The dialog is described in “Inventory Server Properties dialog” on page 819.

- Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described in “Inventory Server Properties dialog” on page 819. Clicking the **–** button removes the selected server.
- **Export Installer Package**: Clicking this button lets you save a custom installer package that includes both the server settings you have specified in this dialog as well as the required certificates.
  You can use this installer package in the **Use Agent installer** section of this dialog.

Remote Control

The **Remote Control** tab of the **Preferences** dialog lets you configure the remote control software that LANrev is to use for viewing the screens of client computers.



Drag services into the order you prefer to use them.

Remote Control Service	Username	Domain	Port
LANrev Remote			5900
Timbuktu			407
Timbuktu (Secure)			22
macOS Screen Sharing			
JollyFastVNC			5900
Apple Remote Desktop 3			5900
CoRD			3389
MS Remote Desktop			3389
VNC			5900
SSH			22

Username:

Domain:

Password:

Port: 5900

Verify:

Application: /Users/jan/Desktop/LANrev Adm...nts/MacOS/LANrev Remote.app

The tab contains these elements. Depending on the selected service, inappropriate fields may be disabled:

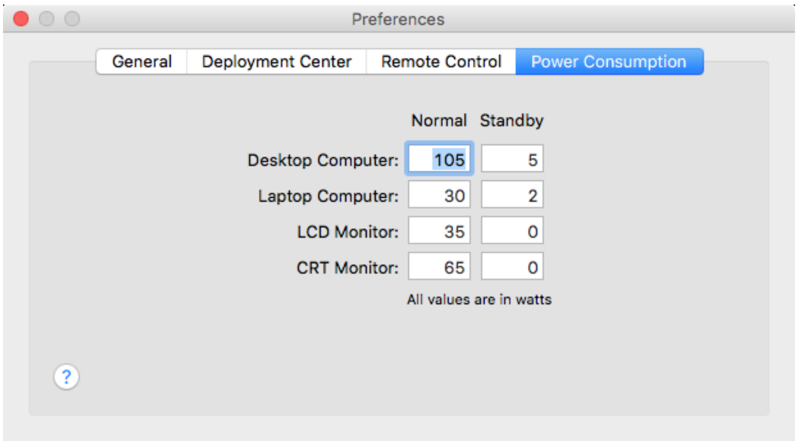
- List of supported remote control services: The list contains the remote control services that LANrev supports, along with important parameters.
  You can drag the entries to reflect the order of your preference; LANrev always tries from the top of the list before lower ones to remotely control a client.

You can edit the parameters that appear in the list in place (by double-clicking their cells) or – when the service is selected – in the fields below the list.

- **Username**: The user account for the remote control software on the client computers.
- **Password** and **Verify**: The password for the specified account. *Note: Some VNC applications do not support being supplied with a username and password when they are launched; when you are using these applications, you must enter a username and password within the application, even if you have already supplied both in LANrev. This is a limitation of these applications, not of LANrev.*
- **Application**: The local application that will be used to connect to the client. If "n/a" is displayed, no application for the selected protocol was found.
- **Domain**: The Window networking domain to be used for accessing client computers. *Note: Some VNC applications do not support domains.*
- **Port**: The network port on which to contact the remote control software on the client computers.

Power Consumption

The **Power Consumption** tab of the **Preferences** dialog lets you configure the power consumption levels of various types of devices. LANrev uses these rates in calculating the power usage reports.



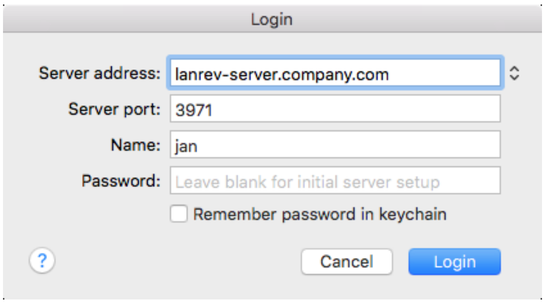
	Normal	Standby
Desktop Computer:	105	5
Laptop Computer:	30	2
LCD Monitor:	35	0
CRT Monitor:	65	0

All values are in watts

The tab contains **Normal** and a **Standby** fields for computers (stationary and portable) and monitors (LCD and CRT). They contain the typical amounts of power (measured in watts) that a device of that type consumes in your organization.

Switch Administrator and Server

The **Switch Administrator and Server** command opens the **Login** dialog, letting you log on to a different server, as a different user, or both:



Login

Server address: lanrev-server.company.com

Server port: 3971

Name: jan

Password: Leave blank for initial server setup

□ Remember password in keychain

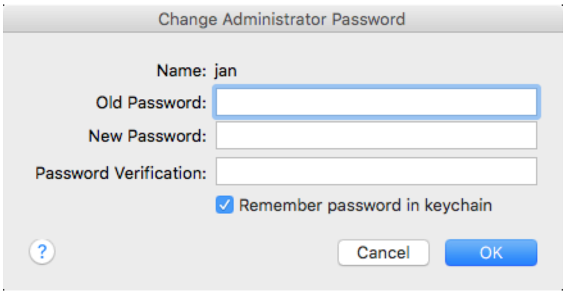
The dialog contains these text fields:

- **Server address**: The IP address or DNS name of the computer on which the desired LANrev Server is running. The pop-up menu beside the field provides access to the most recently used servers.
- **Server port**: The port number on which LANrev Server is listening.
  The server is preconfigured to use port 3791; we strongly recommend against changing this value unless you experience conflicts.
- **Name**: The username as defined in LANrev's **Administrator Center** window.
- **Password**: The account's password as defined in LANrev's **Administrator Center** window.
  If the account is based on an Active Directory user account, you can use the display name, the account name, or the login name to log in.
  Note: When you set up a server for the first time, you leave the **Password** *field empty. Details on setting up a server are available in "Installing LANrev Server" on page 16.*
- **Remember password in keychain**: If this option is checked, the password is stored in the keychain of the current macOS user account. On future launches of LANrev, you will automatically be logged in with the current account.
  Note: This gives everybody with access to your user account on the Macintosh automatic access to LANrev. If you cannot be sure that unauthorized persons will not gain access to your account on the Mac, you may want to disable this option.
  Note: To remove the password from the keychain, either delete it with the Keychain utility or choose **Change Administrator Password** *and uncheck the "***Remember password in keychain***" option.*

Clicking **Login** terminates the current session and connects you to the specified server and account in a new session.

Change Administrator Password

The **Change Administrator Password** command opens the **Change Administrator Password** dialog that lets you change the password for your LANrev account:



Change Administrator Password

Name: jan

Old Password:

New Password:

Password Verification:

☑ Remember password in keychain

NOTE This command is not available when the currently active account is based on an Active Directory user account.

The dialog contains these fields:

- **Name**: The name of the user account.
- **Old Password**: The existing password.
- **Password**: The new password. A password may contain any Unicode character.
- **Verify**: Retype the new password in this field. If the contents of the **Password** and **Verify** fields do not match, an error message is displayed and the password change is rejected.
- **Remember password in keychain**: If this option is checked, the new password is stored in the keychain of the current macOS user account.

InstallEase Key

The **InstallEase Key** command opens an alert in which an activation key for LANrev InstallEase is displayed:

You can use this key to activate copies of InstallEase 1.x; later versions of InstallEase no longer require an activation key.

Services submenu

This submenu contains services provided by other applications and utilities. It is managed by the operating system. For details on the commands in this submenu, see the macOS documentation and the documentation of the applications and utilities providing the services.

Hide LANrev Admin

The **Hide LANrev Admin** command hides all LANrev Admin windows, bringing the next open application to the front.

Hide Others

The **Hide Others** command hides all open applications except LANrev Admin.

Show All

The **Show All** command displays all running applications. It is dimmed when no application is currently hidden.

Quit LANrev Admin

The **Quit LANrev Admin** command quits LANrev Admin. If there are unsaved changes in any open window, you are prompted to save them.

NOTE This excludes changes to the Software Distribution Center and License Monitoring Center. Such changes are automatically saved locally but not sent to the server. They will thus be available to you when you next open LANrev Admin but will not take effect before you manually send them to LANrev Server.

Chapter 11 File menu

The **File** menu contains commands related to working with documents. LANrev offers the usual range of commands in this menu:

- **New** (page 375)
- **New Tab** (page 375)
- **Open** (page 376)
- **Open Recent submenu** (page 376)
- **Close** (page 376)
- **Close Window** (page 377)
- **Close Tab** (page 377)
- **Close Tab** (page 377)
- **Rename Tab** (page 378)
- **Save** (page 378)
- **Save As** (page 378)
- **Export** (page 379)
- **Export Groups** (page 380)
- **Import submenu** (page 380)
- **Groups** (page 381)
- **Custom Field Data for Desktop Devices** (page 381)
- **Custom Field Data for Mobile Devices** (page 383)
- **Enrollment Users for Desktop Devices** (page 383)
- **Enrollment Users for Mobile Devices** (page 385)
- **Device Users** (page 386)
- **Software Packages** (page 387)
- **License Specifications** (page 388)
- **License Purchase Data** (page 388)
- **Page Setup** (page 390)
- **Print** (page 390)

New

The **New** command creates a new browser window.

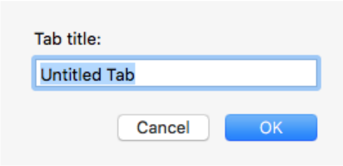
Browser windows display information from the Computers table in LANrev’s internal database and can display related information from other tables, for example, the Fonts or Files table.

A detailed description of browser windows is available in “Browser windows” on page 517.

New Tab

The **New Tab** command creates a new tab in the frontmost window.

Choosing the command opens the **New Tab** dialog:



The command is available only if the frontmost window is a browser window.

Open

The **Open** command lets you open saved LANrev documents.

Choosing the command brings up a standard Open dialog from the operating system. For details on this dialog, see the macOS documentation.

When you open a document, the browser window structure is recreated as it had been saved. The window is automatically populated with the current data.

A detailed description of browser windows is available in “Browser windows” on page 517.

Open Recent submenu

The **Open Recent** submenu lists the last ten files that you have opened in LANrev Admin. (The method by which the files were opened – using the **Open** command, by drag and drop, by double-clicking, etc. – is immaterial.)

Choosing any file from the submenu opens it.

Choosing the **Clear Menu** command resets the submenu to an empty state, removing all files from it.

Close

The **Close** command closes the frontmost window, just like clicking the window’s close box.

If the window contains unsaved changes, LANrev asks you whether you want to save the changes.

NOTE This excludes changes to the Software Distribution Center and License Monitoring Center. Such changes are automatically saved locally but not sent to the server. They will thus be available to you when you next open LANrev Admin but will not take effect before you manually send them to LANrev Server.

In macOS 10.12 and above, this command has been replaced by the **Close Window** command.

Close Window

The **Close Window** command closes the frontmost window, just like clicking the window's close box.

If the window contains unsaved changes, LANrev asks you whether you want to save the changes.

NOTE This excludes changes to the Software Distribution Center and License Monitoring Center. Such changes are automatically saved locally but not sent to the server. They will thus be available to you when you next open LANrev Admin but will not take effect before you manually send them to LANrev Server.

This command replaces the **Close** command in macOS 10.12 and above.

Close Tab

The **Close Tab** command closes the frontmost tab in the window, just like clicking the tab's close box.

Note that this command applies to operating system tabs, not tabs created by LANrev's **New Tab** command. The command is only available in macOS 10.12 and above, and is different from the **Close Tab…** command.

Close Tab

The **Close Tab** command closes the active tab.

Note that this command applies to tabs created by LANrev's **New Tab** command. Operating system tabs, available in macOS 10.12 and above, are closed by the **Close Tab** command directly above this command in the **File** menu.

Choosing the command closes the active tab after displaying a confirmation message.

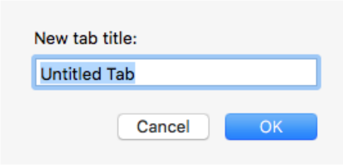
NOTE If you hold down the Option key while choosing **Close Tab**, no confirmation message is displayed.

The command is available only if the frontmost window contains more than one tab.

Rename Tab

The **Rename Tab** command lets you rename the active tab.

Choosing the command opens the **Rename Tab** dialog:



New tab title: Untitled Tab

The command is available only if the frontmost window contains more than one tab.

Save

The **Save** command saves the current state of the frontmost window in a file on disk. If the window is untitled, that is, if no document has yet been assigned to it, choosing **Save** has the same effect as choosing **Save As** (see below).

When the frontmost window cannot be saved to a file, the **Save** command is disabled.

When the frontmost window is a command window, choosing **Save** opens the **Save Template** dialog that is described in "Command window toolbar" on page 402.

NOTE **Save** is not available for the **Agent Settings** command.

When the frontmost window is the **Agent Deployment Center** window, choosing **Save** saves any changes to custom zones.

Save As

The **Save As** command lets you save the state of the frontmost window under a different name than before.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, see the macOS documentation.

The saved file contains the window’s entire structure information – groups and smart groups, columns, etc. – but none of the actual contents. The contents can be stored in a local file by means of the **Export** command.

NOTE To save the contents of a browser window, use the **Export** command.

When the frontmost window cannot be saved to a file, the **Save As** command is disabled.

Command window

When the frontmost window is a command window, choosing **Save As** opens the **Save Template** dialog that is described in “Command window toolbar” on page 402.

Text file

When the frontmost window is a text file display window, choosing **Save As** lets you save the window’s contents as a text file on your computer.

Export

The **Export** command lets you export the contents of the frontmost window as a file.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, see the macOS documentation.

The command supports these export formats:

- **HTML**: The data is saved as an HTML page.
The data is saved as a single HTML page according to the HTML 4.01 Transitional standard.

- **Text (CSV, UTF-8)**: The data is saved as comma-separated values in a text file.
Fields’ contents are enclosed in quotes and separated by commas; records are separated by line-feed characters.
The first record contains the column names.
Dates and times are formatted as short dates and times, respectively, according to the system’s current region settings.
Numbers are exported ‘raw’, that is, without any kind of formatting. Bytes are not converted to megabytes or other multiples.
Text is encoded as UTF-8 (Unicode).
- **Text (CSV)**: As **Text (CSV, UTF-8)** but with the current system encoding used instead of UTF-8.

- **Text (localized CSV)**: As **Text (CSV)**, but with localized list dividers as separators between fields, for example, semicolons instead of commas.
- **Text (tab-delimited, UTF-8)**: The data is saved as tab-delimited text, encoded as UTF-8.
  Fields' contents are separated by tab characters; records are separated by line-feed characters.
  The first record contains the column names.
  Fields are formatted as in the browser window being exported.
- **TheftTrack Report (HTML)**: An HTML file providing an overview of the theft-tracking information on the computers in the window.
- **TheftTrack Report (XML)**: The theft-tracking information on the computers in the window in XML format.
- **XML**: The data in the window is saved in XML format for processing in other applications or automated workflows.
  The data is saved in a simple structure that contains information about the document, about the columns exported, and the data for the individual records.

Clicking **Save** exports the data from the window.

When the frontmost window cannot be exported, the **Export** command is disabled.

Export Groups

The **Export Groups** command lets you export the selected groups and smart groups of the frontmost window to a file.

Choosing the command opens the Save dialog from the operating system. For details on this dialog, see the macOS documentation.

The **Export Groups** command is available only if the frontmost window contains groups or smart groups.

NOTE You can also export groups by dragging them to the desktop.

Import submenu

The **Import** submenu groups commands for importing various kinds of data and settings into LANrev.

For details, see the descriptions of the individual commands:

- **Groups** (page 381)
- **Custom Field Data for Desktop Devices** (page 381)
- **Custom Field Data for Mobile Devices** (page 383)
- **Enrollment Users for Desktop Devices** (page 383)
- **Enrollment Users for Mobile Devices** (page 385)
- **Device Users** (page 386)

- **Software Packages** (page 387)
- **License Specifications** (page 388)
- **License Purchase Data** (page 388)

Groups

The **Groups** command lets you import groups and smart groups from a file into the frontmost window.

Choosing the command opens the Open dialog from the operating system. For details on this dialog, see the macOS documentation.

In the dialog, you can choose any group file that has been previously saved from LANrev. Opening the file adds all groups that are specified in it to the frontmost window.

The **Groups** command is available only if the frontmost window can contain groups or smart groups.

NOTE You can also import groups by dragging them to the window’s sidebar from the desktop.

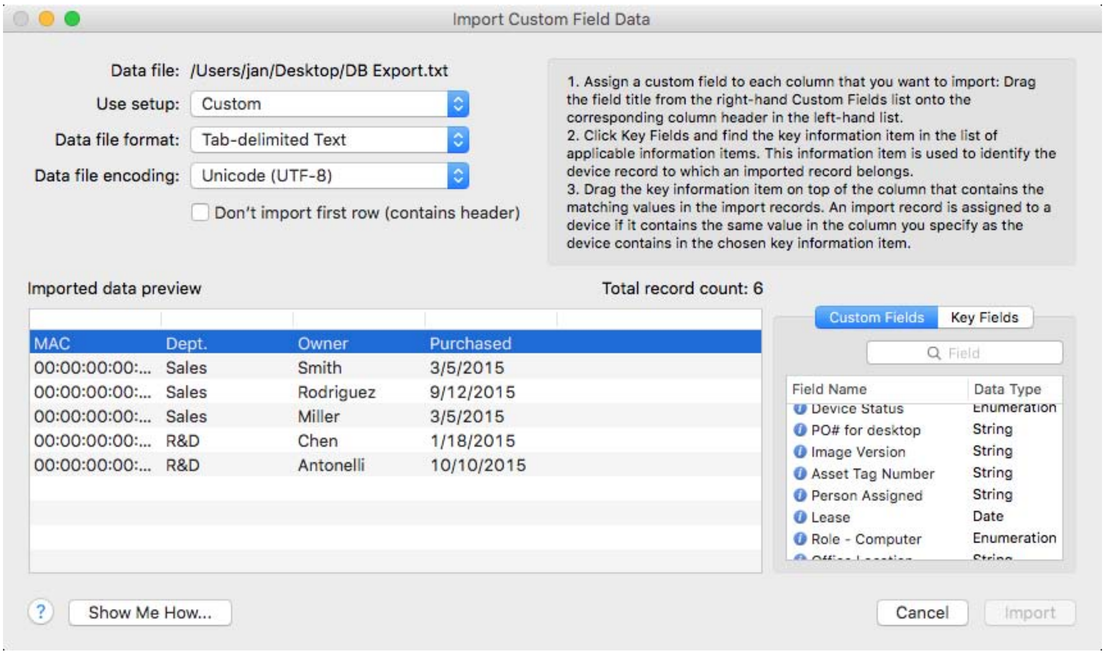
Custom Field Data for Desktop Devices

The **Custom Field Data for Desktop Devices** command lets you import data from text files into manual (that is, non-dynamic) custom information fields that have been defined for desktop devices.

(Note that you can also automate the import of this information, as described in “Automatically importing information” on page 122.)

Choosing the command opens the Open dialog from the operating system. (For details on this dialog, see the macOS documentation.)

When you open a text file in this dialog (in which fields are delimited with tabs, commas, or semicolons and records are delimited with returns), the **Import Custom Field Data** dialog is displayed.



Data file: /Users/jan/Desktop/DB Export.txt

Use setup: Custom

Data file format: Tab-delimited Text

Data file encoding: Unicode (UTF-8)

□ Don't import first row (contains header)

1. Assign a custom field to each column that you want to import: Drag the field title from the right-hand Custom Fields list onto the corresponding column header in the left-hand list.
2. Click Key Fields and find the key information item in the list of applicable information items. This information item is used to identify the device record to which an imported record belongs.
3. Drag the key information item on top of the column that contains the matching values in the import records. An import record is assigned to a device if it contains the same value in the column you specify as the device contains in the chosen key information item.

Imported data preview

Total record count: 6

MAC	Dept.	Owner	Purchased
00:00:00:00:...	Sales	Smith	3/5/2015
00:00:00:00:...	Sales	Rodriguez	9/12/2015
00:00:00:00:...	Sales	Miller	3/5/2015
00:00:00:00:...	R&D	Chen	1/18/2015
00:00:00:00:...	R&D	Antonelli	10/10/2015

Field Name	Data Type
Device Status	Enumeration
PO# for desktop	String
Image Version	String
Asset Tag Number	String
Person Assigned	String
Lease	Date
Role - Computer	Enumeration
Office Location	String

The dialog includes these elements:

- **Data file**: The file you have chosen to import.
- **Use setup**: This pop-up menu lets you save particular configurations of this dialog under a name and reopen saved configurations.
  In addition to all saved setups, it includes these commands:
  - **Save As**: Save the current settings in the dialog as a new named setup. All settings from the dialog are saved, except the import file chosen
  - **Rename**: Rename the currently chosen setup.
  - **Delete**: Delete the currently chosen setup. This does not affect the current settings in the dialog.
- **Data file format**: This menu lets you specify the field delimiter in the import file. LANrev tries to identify the delimiter automatically and presets this menu accordingly.
- **Data file encoding**: The text encoding of the import file. Again, LANrev tries to determine the encoding before displaying the dialog.
- **Don't import first row**: If this option is checked, LANrev starts importing the file with the second row. This is useful if the first row contains the field names.
- **Import data preview**: This table shows the first few lines of the import file according to the current settings in the dialog. It also lets you assign custom information fields to columns in the import file by dragging a field from the **Custom Fields** list to a column.
  Dragging a field from the **Key Fields** list to a column makes that column the column by which import records are matched to LANrev's database records.

Clicking the small badge ⊗ in the column title removes the assigned field.

- **Custom Fields**: This list contains all manual custom information fields for desktop devices that can be assigned to columns of the import file.
  Fields are assigned by dragging them on top of columns. Assigning a field to a column causes that column's data to be imported into the field.
  Entering text into the search field filters the list of custom information fields.
- **Key Fields**: This list contains all information items that can be assigned to columns of the import file.
  Fields are assigned by dragging them on top of columns. Assigning a key field to a column causes LANrev to store the data from each import record in that database record for which the key field matches the assigned column in the import record.
  Entering text into the search field filters the list of key fields.
- **Show Me How**: Clicking this button displays a brief tutorial on importing custom information field data.
- **Cancel**: Clicking this button cancels the import process. No data is imported.
- **Import**: Clicking this button imports the chosen file according to the specified settings.

Custom Field Data for Mobile Devices

The **Custom Field Data for Mobile Devices** command lets you import data from text files into manual (that is, non-dynamic) custom information fields that have been defined for mobile devices.

The command works exactly like **Custom Field Data for Desktop Devices**, described above, except that you can choose custom information fields for mobile devices into which to import the data.

Note that you can also automate the import of this information, as described in "Automatically importing information" on page 122.

Enrollment Users for Desktop Devices

The **Enrollment Users for Desktop Devices** command lets administrators with the "Modify Enrollment Users" privilege import data from text files that include Active Directory information for users of computers that you manage through LANrev.

Choosing the command opens the Open dialog from the operating system. (For details on this dialog, see the macOS documentation.)

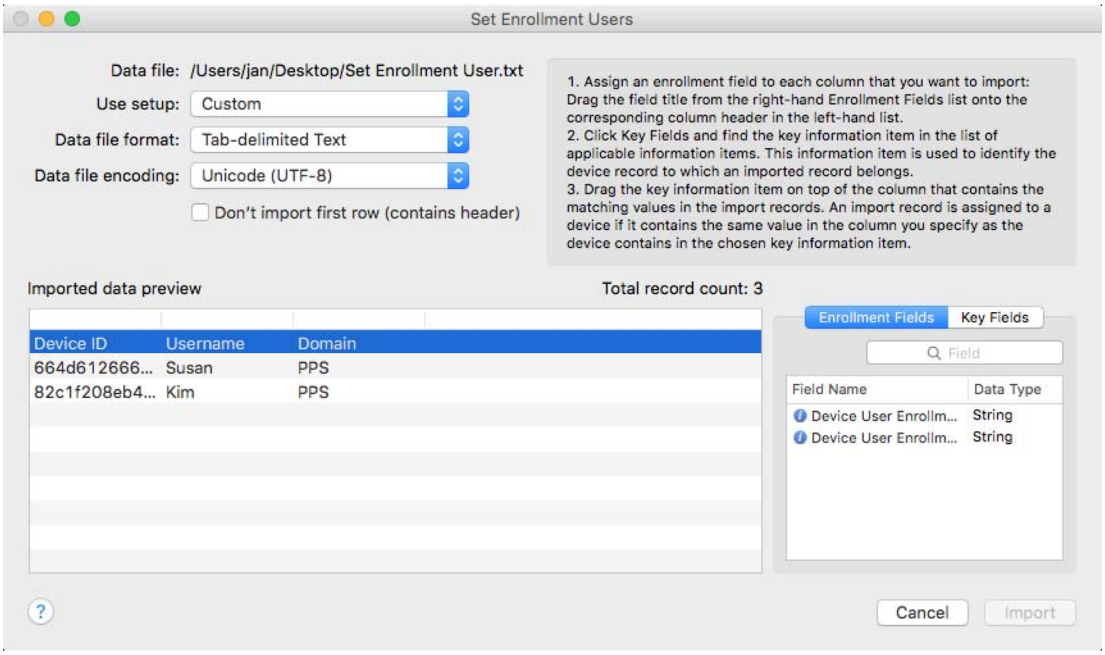
In this dialog, you can choose a text file in which fields are delimited with tabs, commas, or semicolons and records are delimited with returns. The file must contain one column with device identifiers, one column with user names, and one column with domains.

Clicking **OK** in the Open dialog opens the **Set Enrollment Users** dialog described below.

Note that you can also automate the import of this information, as described in "Automatically importing information" on page 122.

Set Enrollment Users

The **Set Enrollment Users** dialog is displayed when you import a text file with the **Enrollment Users for Desktop Devices** or **Enrollment Users for Mobile Devices** commands. It lets you specify the details of the import operation.



Data file: /Users/jan/Desktop/Set Enrollment User.txt

Use setup: Custom

Data file format: Tab-delimited Text

Data file encoding: Unicode (UTF-8)

☐ Don't import first row (contains header)

1. Assign an enrollment field to each column that you want to import: Drag the field title from the right-hand Enrollment Fields list onto the corresponding column header in the left-hand list.
2. Click Key Fields and find the key information item in the list of applicable information items. This information item is used to identify the device record to which an imported record belongs.
3. Drag the key information item on top of the column that contains the matching values in the import records. An import record is assigned to a device if it contains the same value in the column you specify as the device contains in the chosen key information item.

Imported data preview

Total record count: 3

Device ID	Username	Domain
664d612666...	Susan	PPS
82c1f208eb4...	Kim	PPS

Field Name	Data Type
Device User Enrollm...	String
Device User Enrollm...	String

The dialog includes these elements:

- **Data file**: The file you have chosen to import.
- **Use setup**: This pop-up menu lets you save particular configurations of this dialog under a name and reopen saved configurations.
  In addition to all saved setups, it includes these commands:
  - **Save As**: Save the current settings in the dialog as a new named setup. All settings from the dialog are saved, except the import file chosen
  - **Rename**: Rename the currently chosen setup.
  - **Delete**: Delete the currently chosen setup. This does not affect the current settings in the dialog.
- **Data file format**: This menu lets you specify the field delimiter in the import file. LANrev tries to identify the delimiter automatically and presets this menu accordingly.
- **Data file encoding**: The text encoding of the import file. Again, LANrev tries to determine the encoding before displaying the dialog.
- **Don't import first row**: If this option is checked, LANrev starts importing the file with the second row. This is useful if the first row contains the field names.

- **Imported data preview**: This table shows the first few lines of the import file according to the current settings in the dialog. It also lets you assign information fields to columns in the import file by dragging a field from the **Custom Fields** list to a column.
  Dragging a field from the **Key Fields** list to a column makes that column the column by which import records are matched to LANrev's database records.
  Clicking the small badge ⊗ in the column title removes the assigned field.
- **Custom Fields**: This list contains the information items for the user name and domain.
  Fields are assigned by dragging them on top of columns. Assigning a field to a column causes that column's data to be imported into the field.
  Entering text into the search field filters the list of custom information fields.
- **Key Fields**: This list contains all information items that can be assigned to the column of the import file that identifies the devices.
  The matching information item must be assigned to the device ID column by dragging it on top of the column. For example, if devices are identified by IMEI, drag the "Mobile Device IMEI" information item on top of the column.
  For information on the available information items, see the appropriate section in "Information items" on page 831.
  Entering text into the search field filters the list of key fields.
- **Show Me How**: Clicking this button displays a brief tutorial on importing custom field information (which is a very similar process to importing enrollment user data).
- **Cancel**: Clicking this button cancels the import process. No data is imported.
- **Import**: Clicking this button imports the chosen file according to the specified settings.

Enrollment Users for Mobile Devices

The **Enrollment Users for Mobile Devices** command lets you import data from text files that include Active Directory information for users of mobile devices that you manage through LANrev.

Choosing the command opens the Open dialog from the operating system. (For details on this dialog, see the macOS documentation.)

In this dialog, you can choose a text file in which fields are delimited with tabs, commas, or semicolons and records are delimited with returns. The file must contain one column with device identifiers, one column with user names, and one column with domains.

Clicking **OK** in the Open dialog opens the **Set Enrollment Users** dialog described above.

Note that you can also automate the import of this information, as described in "Automatically importing information" on page 122.

Device Users

The **Device Users** command lets you import user data from text files. LANrev uses this information if no Active Directory service is available.

Choosing the command opens the Open dialog from the operating system. (For details on this dialog, see the macOS documentation.)

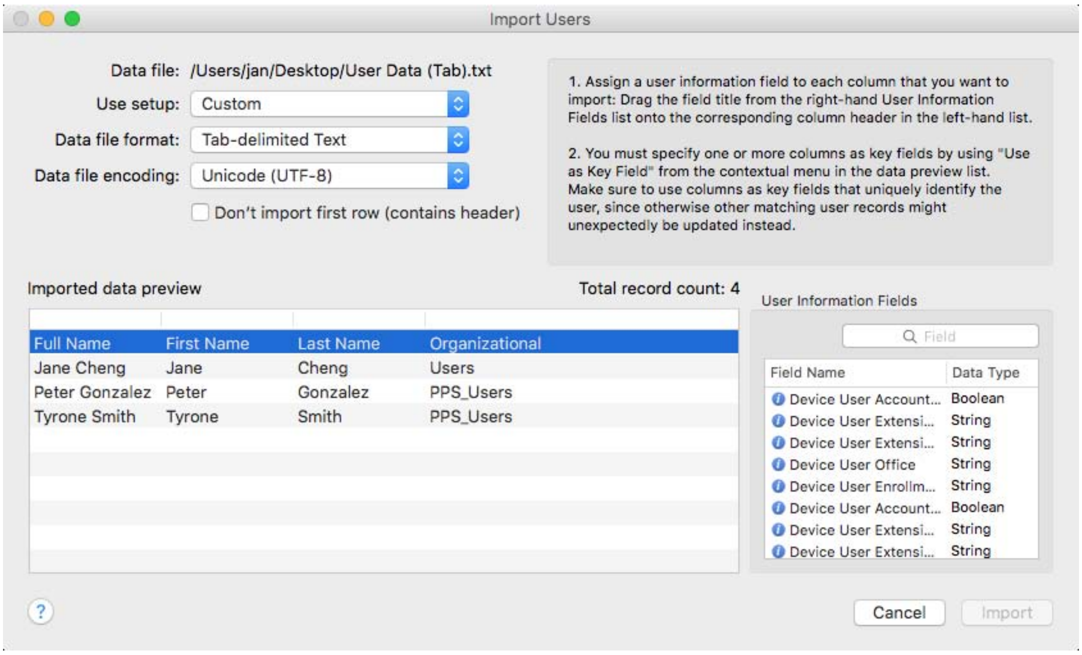
In this dialog, you can choose a text file in which fields are delimited with tabs, commas, or semicolons and records are delimited with returns. The file must contain at least one column a combination of columns that can contains unique identifiers for the users.

Clicking **OK** in the Open dialog opens the **Import Users** dialog described below.

Note that you can also automate the import of this information, as described in “Automatically importing information” on page 122.

Import Users

The **Import Users** dialog is displayed when you import a text file with the **Device Users** command. It lets you specify the details of the import operation.



Data file: /Users/jan/Desktop/User Data (Tab).txt

Use setup: Custom

Data file format: Tab-delimited Text

Data file encoding: Unicode (UTF-8)

☐ Don’t import first row (contains header)

1. Assign a user information field to each column that you want to import: Drag the field title from the right-hand User Information Fields list onto the corresponding column header in the left-hand list.

2. You must specify one or more columns as key fields by using "Use as Key Field" from the contextual menu in the data preview list. Make sure to use columns as key fields that uniquely identify the user, since otherwise other matching user records might unexpectedly be updated instead.

Imported data preview

Total record count: 4

Full Name	First Name	Last Name	Organizational
Jane Cheng	Jane	Cheng	Users
Peter Gonzalez	Peter	Gonzalez	PPS_Users
Tyrone Smith	Tyrone	Smith	PPS_Users

User Information Fields

Field Name	Data Type
Device User Account...	Boolean
Device User Extensi...	String
Device User Extensi...	String
Device User Office	String
Device User Enrollm...	String
Device User Account...	Boolean
Device User Extensi...	String
Device User Extensi...	String

The dialog includes these elements:

- **Data file**: The file you have chosen to import.
- **Use setup**: This pop-up menu lets you save particular configurations of this dialog under a name and reopen saved configurations.
  In addition to all saved setups, it includes these commands:

  - **Save As**: Save the current settings in the dialog as a new named setup. All settings from the dialog are saved, except the import file chosen
  - **Rename**: Rename the currently chosen setup.
  - **Delete**: Delete the currently chosen setup. This does not affect the current settings in the dialog.
- **Data file format**: This menu lets you specify the field delimiter in the import file. LANrev tries to identify the delimiter automatically and presets this menu accordingly.
- **Data file encoding**: The text encoding of the import file. Again, LANrev tries to determine the encoding before displaying the dialog.
- **Don't import first row**: If this option is checked, LANrev starts importing the file with the second row. This is useful if the first row contains the field names.
- **Imported data preview**: This table shows the first few lines of the import file according to the current settings in the dialog. It also lets you assign information fields to columns in the import file by dragging a field from the **User Information Fields** list to a column or by right-clicking the column and choosing the desired field from the context menu.
  When a column has been associated with a field, you can specify it as a key column by choosing **Use as Key Field** from the context menu. To take the key field status away from a column, choose **Use as Key Field** again.
  Clicking the small badge ⊗ in the column title or choosing **Remove Field** from the context menu removes the assigned field from the column.
- **User Information Fields**: This list contains the information items for the device user.
  Fields are assigned by dragging them on top of columns. Assigning a field to a column causes that column's data to be imported into the field.
  Entering text into the search field filters the list of custom information fields.
- **Cancel**: Clicking this button cancels the import process. No data is imported.
- **Import**: Clicking this button imports the chosen file according to the specified settings. The imported data is used to populate user information fields that normally display Active Directory data. When Active Directory data becomes available for a user, it automatically overwrites the imported data for that user.

Software Packages

The **Software Packages** command lets you import software packages into LANrev that have previously been exported with the **Export Package** command.

Choosing the command opens the Open dialog from the operating system. For details on this dialog, see the macOS documentation.

In the dialog, you can choose any software package file that has been previously exported from LANrev.

License Specifications

The **License Specifications** command lets you import license specifications into LANrev that have previously been exported with the **Export License Specification** command.

Choosing the command opens the Open dialog from the operating system. For details on this dialog, see the macOS documentation.

In the dialog, you can choose any license specification file that has been previously exported from LANrev.

License Purchase Data

The **License Purchase Data** command lets you import information about license purchases into LANrev. This is intended for situation where you have previously managed your license purchases in a different system and want to switch to LANrev.

Choosing the command opens the Open dialog from the operating system. For details on this dialog, see the macOS documentation.

In the dialog, you can choose a tab-delimited file containing your purchase data. See "License purchase data import file", below, for information on this file.

LANrev parses the file and updates existing purchase information records or creates new ones from the content:

- If the values in the first four columns of a row (License Specification, Purchase Type, Purchase Date, Purchase Count) match the values of an existing purchase records, that record is updated with the values from the row.
  If a row contains empty cells, any corresponding data in an updated record is overwritten.
- If no existing record matches, a new record with the values from the row is created.

After the import is complete, a summary dialog is displayed.

License purchase data import file

The file must contain the same columns as the "License Purchase Data Template.xlsx" file that is available in the Resource Center's Power Tools section. The easiest way to achieve this is to import or copy your data into the tablet file and then export is as a tab-delimited file.

The file can contain the columns listed below. The first four columns must be filled for any row, the rest are optional. The columns correspond to the fields in the **Purchase Tracking** pane of the **Software License Specification** dialog:

- **License Specification**: The name for this license specification in LANrev.
  LANrev uses this information (together with the next three fields) to match a row with an existing license specification. If no such match is found, LANrev creates a new record with this field as the license specification name.
- **Purchase Type**: A code for the type of purchase made:
  - 1: New software
  - 2: Software update
  - 3: New maintenance contract
  - 4: Maintenance renewal
- **Purchase Date**: The date when the purchase was made.
  The date format must be the same as the format set in the operating system on the computer where you import the file – specifically the medium date format on macOS and the short date format on Windows. For example, if US English formats are set, the date format would have to be "12/25/2014"; for German, it would have to be "25.12.2014".
- **Purchase Count**: The number of licenses purchased (or affected, in the case of updates and renewals).
- **Add to Licenses Owned**: If column contains "Yes" or 1, the number of licenses purchased is added to the number of licenses available for this software in LANrev's license monitoring.
  If the purchase type (see above) is 3 or 4, the licenses are not added, irrespective of the content of this column.
- **Purchase Price**: The cost of the purchase.
  This information is imported as a string, so you can include formatting (such as thousands separators or currency symbols) as desired.
- **Software Version**: The version of the software purchased, if any.
- **Purchase Order Number**: The identifier that the purchase order has in your bookkeeping system.
- **License Owner**: The person or organization that is registered as the owner of this license.
- **Vendor Name**: The company or person where you made the purchase.
- **Vendor Contact**: The name of the person who is your contact at the vendor company.
- **Vendor Support**: The contact address (for example, phone number or e-mail address) for technical support for this license.
- **Maintenance Begin**: The start date of the purchased maintenance coverage.
  See **Purchase Date**, above, for information on the date format requirements.
- **Maintenance End**: The end date of the purchased maintenance coverage.
  See **Purchase Date**, above, for information on the date format requirements.
- **Maintenance Price**: The cost of the maintenance coverage.
  This information is imported as a string, so you can include formatting (such as thousands separators or currency symbols) as desired.

- **Maintenance Reference**: The contract number or similar information for identifying the maintenance agreement.
- **Notes**: A free-form field for any additional information you would like to record for this purchase.
  Any occurrence of "/n" in the imported note text is replaced by a line break during the import.

If the first row of the table contains the column titles, it is skipped. If it contains other data, it is considered to contain a purchase record and is imported.

Page Setup

The **Page Setup** command is not currently supported by LANrev.

Print

The **Print** command is not currently supported by LANrev.

Chapter 12 Edit menu

The **Edit** menu contains commands related to editing and finding text and objects. LANrev offers the usual range of commands in this menu:

Undo

The **Undo** command reverses the effects of the last action. Whenever an undoable action has been performed, it is added to the name of the **Undo** command, for example, "Undo Typing".

LANrev supports unlimited undo levels. Not all actions are undoable.

Redo

The **Redo** command takes back the last **Undo** command you issued, restoring the action that was reversed by the undo.

Whenever an undo action has been performed, it is added to the name of the **Redo** command, for example, "Redo Typing".

Cut

The **Cut** command removes the selected text from its window and places it on the clipboard.

Copy

The **Copy** command places a copy of the selected text or object on the clipboard.

Besides selected text and objects such as groups, you can also copy selected records. They are converted to text in the clipboard and can be pasted in other applications that accept text.

Paste

The **Paste** command inserts the text or objects on the clipboard into the frontmost window.

The command is dimmed when the clipboard does not contain information that can be pasted at the current location.

Delete

The **Delete** command removes the currently selected text or records.

If the record is deleted of a device to which licenses are still assigned, you are asked whether you want to revoke those licenses first. If you chose to revoke them and the revocation fails, the devices are not deleted.

The command is dimmed when no deletable item is selected.

Select All

The **Select All** commands selects all text or records in the current context.

The command is dimmed when the keyboard focus is on an area where there are no selectable objects, for example, an empty list, or where only one object can be selected at a time, for example, the **Groups & Machines** list.

Find submenu

The **Find** submenu contains commands for finding text. Its use in LANrev is limited to windows displaying text files from administered computers.

The commands in this submenu are available only when the frontmost window is a text file window.

Find

The **Find** command opens the **Find** dialog that lets you specify the text you are searching for and control the searching process.

The **Find** dialog is provided by macOS. See the operating system documentation for details.

This command is available only when the frontmost window is a text file display window.

Find Next

The **Find Next** command finds the next instance of the specified search text.

This command is available only when the frontmost window is a text file display window and you have specified a search string in the **Find** dialog.

Find Previous

The **Find Previous** command finds the previous instance of the specified search text.

This command is available only when the frontmost window is a text file display window and you have specified a search string in the **Find** dialog.

Use Selection for Find

The **Use Selection for Find** command enters the currently selected text as the search string in the **Find** dialog. It does not, however, open the dialog or initiate a search.

This command is available only when the frontmost window is a text file display window and text is selected in that window.

Jump to Selection

The **Jump to Selection** command scrolls the frontmost window so as to display the selected text.

This command is available only when the frontmost window is a text file display window and text is selected in that window.

Spelling and Grammar submenu

The **Spelling and Grammar** submenu contains commands to control spell-checking. LANrev uses the spell-checking feature of macOS. This means, for example, that spellings that have been learned are shared with other applications.

The commands in this submenu are available only when the text insertion mark is located in a text field.

Show Spelling and Grammar

The **Spelling and Grammar** command opens the **Spelling and Grammar** dialog that lets you check the spelling of your text; accept, revise, or turn down suggestions; and choose a spell-checking dictionary.

The **Spelling** dialog is provided by macOS. See the operating system documentation for details.

This command is available only when the text insertion mark is located in a text field.

Check Spelling

The **Check Spelling** command checks the spelling of your text, marking words that may be misspelled.

This function is provided by macOS. See the operating system documentation for details.

Check Spelling as You Type

The **Check Spelling as You Type** toggles constant spell-checking on or off:

- If the command is checked, LANrev checks the spelling of each word as you type it.
- If the command is unchecked, you must manually initiate spell-checking by choosing the **Check Spelling** command.

This function is provided by macOS. See the operating system documentation for details.

Start Dictation

The **Start Dictation** command allows you to enter text by spoken voice.

This command is provided by the operating system; see the macOS documentation for details.

Emoji & Symbols

The **Emoji & Symbols** command opens the **Characters** Palette of macOS that lets you enter characters that are not available on the keyboard.

This palette is provided by the operating system; see the macOS documentation for details.

Chapter 13 View menu

The **View** menu contains commands related to displaying and configuring toolbars.

Show Tab Bar

The **Show Tab Bar** command displays or hides the tab bar in the front-most window. (Note that this tab bar displays operating system tabs, not tabs created using LANrev's **New Tab** command.)

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Details

The **Details** command displays details for a selected computer, software package, or license specification.

Choosing the command for a computer selects it in the browser window's sidebar and displays in the sidebar all information categories that are available for the computer.

Choosing the command for a software package or license specification displays the package's or specification's details in the table area of the browser window.

Select Container

The **Select Container** command selects (in a browser window's sidebar) the container of a selected item.

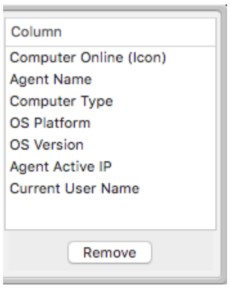
Choosing the command selects the next-higher container (that is, expandable item) in the browser window's sidebar.

NOTE You can also press Command-Up Arrow on the keyboard for the same effect.

Configure Columns

The **Configure Columns** command lets you add, rearrange, or remove columns from the frontmost window.

Choosing the command opens the columns drawer:



Column

Computer Online (Icon)
Agent Name
Computer Type
OS Platform
OS Version
Agent Active IP
Current User Name

If the drawer is already open, choosing **Configure Columns** closes it.

The drawer contains the titles of all columns that appear in the window, in the order in which the columns appear.

Rearranging the column titles in the drawer rearranges the columns in the window.

Dragging an information item from the **Information Items** window to the drawer adds a corresponding column to the windows.

Clicking **Remove** removes the selected column from the window.

Choosing **Configure Columns** again closes the drawer

Display All Records

The **Display All Records** command loads records from the server into the frontmost window in cases where not all records have been loaded because that would have exceeded the limit set in the **Preferences** dialog’s **General** tab.

Choosing the command loads all records from the server that are not yet displayed in the frontmost window.

The command is available only if the frontmost window does not display all records (which is indicated in the status bar).

Hide Toolbar

The **Hide Toolbar** command hides the toolbar of the frontmost window. It is available only if the toolbar of the frontmost window is currently visible.

Show Toolbar

The **Show Toolbar** command displays the toolbar of the frontmost window. It is available only if the toolbar of the frontmost window is currently hidden.

Customize Toolbar

The **Customize Toolbar** command lets you customize the contents of the toolbar of the frontmost window. It is available only if the frontmost window has a toolbar (visible or hidden).

Choosing the command displays a customization dialog that contains these elements:

- Buttons and other items: These buttons and additional items like spaces and dividers can be dragged into the toolbar to be displayed there. Items already in the toolbar can be dragged out of it, in which case they will no longer be displayed.
  The exact range of items available in the dialog depends on the type of window to which the toolbar belongs.
- **Show**: This pop-up menu lets you choose the style in which the toolbar contents is displayed.
- **Use Small Size**: If this option is checked, the size of the items in the toolbar is reduced.
- **Done**: Clicking **Done** closes the dialog and sets the toolbar of all windows of this type to the specifications you made.

Enter Full Screen

Choosing **Enter Full Screen** displays the frontmost window in full-screen mode, as if the green button in the upper left-hand corner of the window had been clicked.

Exit Full Screen

Choosing **Exit Full Screen** displays the frontmost window in normal mode. The command is only available if the window currently is in full-screen mode.

Chapter 14 Commands menu

The **Commands** menu contains commands that let you perform actions related to the managed computers.

There are two different command lists in the menu, one when the frontmost window shows information related to desktop computers and another when the window shows information related to mobile devices.

Both versions are listed below.

Commands and command options for computers

- **Execute Command Now** (page 457)
- **Edit Command** (page 457)
- **Reapply Command** (page 458)
- **Show/Hide Target List** (page 458)

Commands and command options for mobile devices

- **Variables for mobile devices** (page 458)
- **Install Configuration Profile** (page 459)
- **Install Provisioning Profile** (page 460)
- **Install Application** (page 461)
- **Install Media File** (page 463)
- **Change Application Configuration** (page 464)
- **Issue Device Lock** (page 464)
- **Issue Clear Passcode** (page 465)
- **Issue Clear Restrictions Passcode** (page 466)
- **Erase Device** (page 466)
- **Set Roaming Options** (page 467)
- **Send Message to Device** (page 468)
- **Set Wallpaper** (page 468)
- **Install iOS Update** (page 469)
- **Request AirPlay Mirroring** (page 470)
- **Stop AirPlay Mirroring** (page 471)
- **Change Personal HotSpot State** (page 471)
- **Set Activation Lock Options** (page 471)
- **Enable Activation Lock** (page 472)
- **Remove Activation Lock** (page 472)
- **Show Activation Lock Bypass Code** (page 472)
- **Enable Attention Mode** (page 473)
- **Disable Attention Mode** (page 473)
- **Set Lost Mode** (page 474)
- **Set Organization Information** (page 475)
- **Update Device Information** (page 475)
- **Create KNOX Workspace** (page 476)
- **Remove KNOX Workspace** (page 476)
- **Lock KNOX Workspace** (page 477)
- **Unlock KNOX Workspace** (page 477)
- **Reset KNOX Workspace Password** (page 477)
- **Track Device** (page 477)
- **Get Device Geolocation** (page 479)
- **Reset Tracking Passphrase** (page 479)

Favorites

The **Favorites** submenu contains command templates that you want to have quickly available.

The menu contains all command templates that have been saved with the **Include in favorites** option in the **Save Template** dialog or that have been checked in the **Command Templates** window’s **Favorites** column.

Variables for computers

LANrev supports a range of variables that you can use in commands and similar circumstances when specifying text that is sent to or displayed on the device (such as the body of an e-mail). This is described in “Information variables” on page 175.

To use a variable in a text field, enclose it in curly brackets and prefix a dollar sign, for example, `${MDU_Company}`.

For computers, you can use all variables listed below. In addition, you can use any custom information fields for computers that you have given a variable name. (See “Defining custom information fields” on page 108 for more information.)

Predefined variables for computers

- MDU_AccountDisabled (Device User Account Disabled)
- MDU_AccountLocked (Device User Account Locked)
- MDU_AccountLockoutTime (Device User Account Lockout Time)
- MDU_AccountPasswordExpirationDate (Device User Account Password Expiration Date)
- MDU_AccountPasswordExpired (Device User Account Password Expired)
- MDU_BusinessCategory (Device User Business Category)
- MDU_City (Device User City)
- MDU_Company (Device User Company)
- MDU_Country (Device User Country)
- MDU_Department (Device User Department)
- MDU_DepartmentNumber (Device User Department Number)
- MDU_DisplayName (Device User Display Name)
- MDU_EMail (Device User E-Mail)
- MDU_EmployeeID (Device User Employee ID)
- MDU_EmployeeNumber (Device User Employee Number)
- MDU_EnrollmentDomain (Device User Enrollment Domain)
- MDU_EnrollmentUsername (Device User Enrollment Username)
- MDU_ExtensionAttribute1 through MDU_ExtensionAttribute15 (Device User Extension Attribute 1 through 15 information items.
- MDU_FirstName (Device User First Name)
- MDU_JobTitle (Device User Job Title)
- MDU_LastName (Device User Last Name)
- MDU_LogOnName (Device User Log-on Name)
- MDU_ManagedBy (Device User Managed By)
- MDU_MemberOf (Device User Is Member Of)
- MDU_MobilePhone (Device User Mobile Phone Number)
- MDU_Office (Device User Office)
- MDU_OrganizationalUnit (Device User Organizational Unit)
- MDU_OrganizationalUnitPath (Device User Organizational Unit Path)
- MDU_PhoneNumber (Device User Phone Number)
- MDU_State (Device User State)

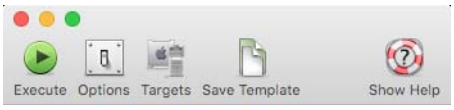
- MDU_Street (Device User Street)
- MDU_ZIPCode (Device User ZIP Code)
- DD_ComputerName (Computer Name)
- DD_ComputerModel (Computer Model)
- DD_ComputerManufacturer (Computer Manufacturer)
- DD_CurrentLoginUserName (Current User Name)
- DD_OSPlatform (OS Platform)
- DD_IPAddress (Agent Active IP)
- DD_PrimaryMACAddress (Primary MAC Address)
- DD_LastHeartbeat (Last Heartbeat)
- DD_OSVersion (OS Version)
- DD_OSBuildNumber (OS Build Number)
- DD_OSServicePack (OS Service Pack)
- DD_SerialNumber (Computer Serial Number)
- DD_UDID (Computer Device Identifier (UDID))
- DD_CurrentUser (Current User Name)
- DD_MissingPatchesCount (Missing Patch Stat Count)
- DD_VPPInviteURL (Device User VPP Invite URL)
- DD_ADComputerName (AD Computer Name)
- DD_ADComputerOU (AD Computer Organizational Unit)
- DD_ADComputerOUPath (AD Computer Organizational Unit Path)
- DD_ADComputerIsMemberOf (AD Computer Is Member Of)
- DD_ADUserOU (AD User Organizational Unit)
- DD_ADUserOUPath (AD Computer Organizational Unit Path)
- DD_ADUserIsMemberOf (AD User Is Member Of)
- DD_ClientInfo1 through DD_ClientInfo10 (Client Information 1 … 10 information items.

Command window toolbar

All command windows share a common toolbar. It contains buttons that let you specify options for the timing and scope of the command execution as well as saving command templates and getting help.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar contains these buttons by default:



These buttons are described in:

- “Execute” on page 403
- “Options” on page 403
- “Targets” on page 404
- “Save Template” on page 405
- “Show Help” on page 405

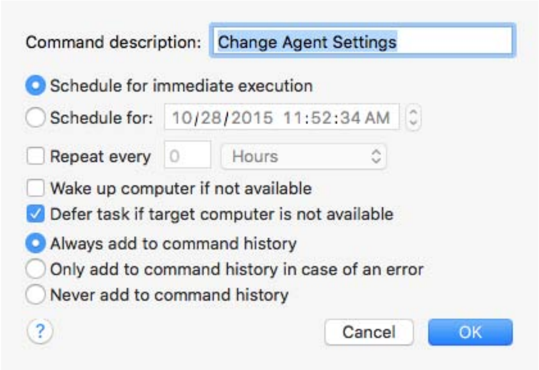
Execute

The **Execute** button executes the command with the currently specified options and closes the command window.

Depending on the scheduling settings (see below), clicking **Execute** executes the command immediately or enters it in the command queue for later execution.

Options

Clicking the **Options** button opens the **Command Options** dialog:



Command description: Change Agent Settings

● Schedule for immediate execution

○ Schedule for: 10/28/2015 11:52:34 AM

□ Repeat every 0 Hours

□ Wake up computer if not available

☑ Defer task if target computer is not available

● Always add to command history

○ Only add to command history in case of an error

○ Never add to command history

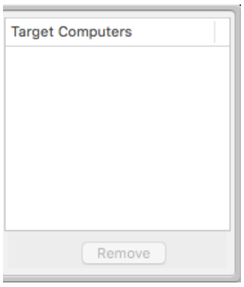
The dialog contains these elements:

- **Command description**: The title under which the command will appear in the **Commands** window.
- **Schedule for immediate execution**: The command will be executed immediately when the **Execute** button in the command window is clicked.
- **Schedule for**: When the **Execute** button in the command window is clicked, the command will not be executed immediately but entered in the command queue to be executed at the specified date.
- **Repeat every**: If this option is checked, the command is executed in the specified intervals after its first execution.
- **Wake up computer if not available**: If this option is checked, LANrev tries to wake up any target computer that is not available before considering it unavailable.
  Note: The default for this setting is specified in the Preferences dialog.
- **Defer task if target computer is not available**: This option determines what happens with the command if a target computer is not available. If it is checked, the command is entered in the command queue to be executed when the target computer becomes available. If the option is unchecked, the command is considered to have failed and no attempt is made to execute it at a later date.
  Note: The default for this setting is specified in the Preferences dialog.
- **History options**: These options let you specify in which this command will be entered into the command history:
  - **Always add to command history**: After the command has been completed, it is added to the command history in all cases, no matter the outcome.

  - **Only add to command history in case of an error**: The command is only added to the command history when it could not be executed successfully.
  - **Never add to command history**: After the command has been completed, it is removed from the command window. In no case is it added to the command history.

Targets

Clicking the **Targets** button opens or closes the **Target Computers** drawer, toggling its state.



Dragging a computer from a browser window into this list adds it to the target list, causing the command to be executed on that computer as well.

You can include computer groups and smart groups as targets. This has the following effects:

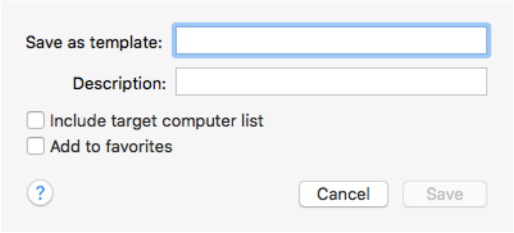
- Specifying a (non-smart) computer group as a target has exactly the same effect as specifying all their members as targets individually.
- The effect of specifying a smart computer group as a target varies according to the type of command execution:
  - When the command is executed immediately or at a specified time or when it is saved as a template and later re-used, all computers that are members of the specified smart group at the moment of execution are the command targets. (That is, it does not matter which computers belong to the smart group at the moment when the command is saved.)
  - When the command is a repeating command, the membership of the smart group is evaluated anew each time the command is executed. All computers that meet the smart group criteria at that time are command targets, and all computers that do not meet these criteria are not targets.
    This means that a computer can be sometimes but not always a target of a repeating command with a smart group as its target.
    Note: For performance reasons, the membership in the smart groups for purposes of determining targets of repeating commands is evaluated only periodically. Therefore, computers may be erroneously included in or excluded from the list of targets when their status with

respect to the smart group criteria changes very shortly before the execution of the repeating command.

Clicking the **Remove** button removes the selected computers from the target list.

Save Template

Clicking the **Save Template** button opens the **Save Template** dialog:



The dialog lets you save the command in its currents state – including all settings – as a template for future reuse. It contains these elements:

- **Save as template**: The name for the command template.
- **Description**: The description for the command template that will be displayed in the **Command Templates** window. When the dialog is opened, this field contains the text from the **Options** dialog's **Command description** field.
- **Include target computer list**: If this option is checked, the current list of target computers for the command is included in the template. If the option is unchecked, the template is saved with an empty target list.
- **Add to favorites**: If this option is checked, the saved template is listed in the **Favorites** submenu.
- **Save**: Clicking the **Save** button stores the command as a command template that can be reused via the **Command Templates** window.

Show Help

Clicking the **Show Help** button displays the help for the command to which the command dialog belongs.

Agent Settings

The **Agent Settings** command lets you specify various settings for the LANrev agents on the selected computers.

Choosing the command opens the **Agent Settings** dialog. The dialog has four panes:

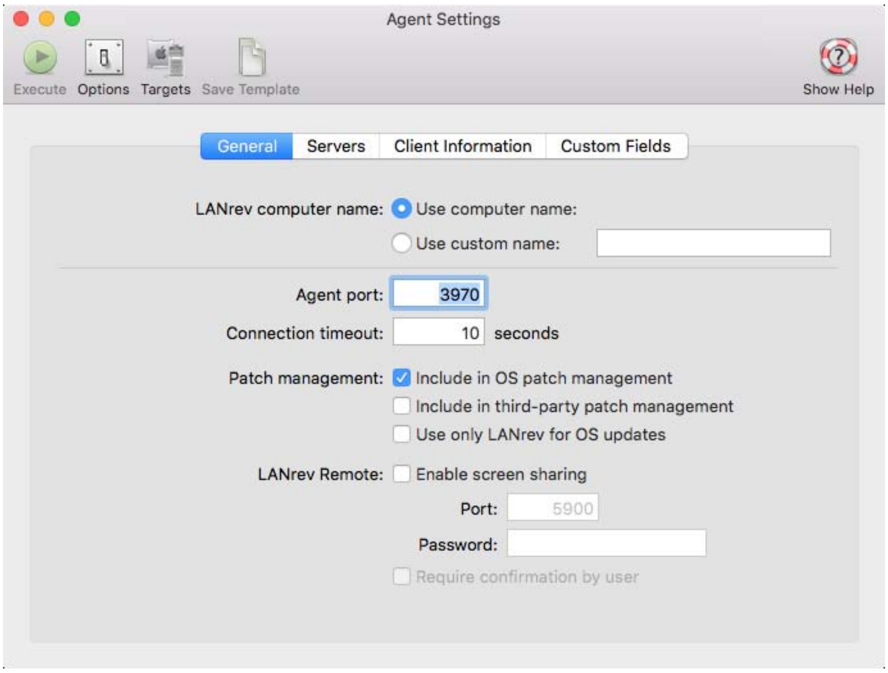
- **General**
- **Servers**
- **Client Information**
- **Custom Fields**

All three are described below.

The toolbar of command windows is described in “Command window toolbar” on page 402. Note, however, that it is not possible to save the **Agent Settings** command as a command template; both the **Save Template** button in the toolbar and the **Save** command in the **File** menu are disabled.

General

The **General** pane of the **Agent Settings** dialog lets you configure various basic parameters for the agents’ operation:



LANrev computer name: ● Use computer name:
○ Use custom name:

Agent port: 3970

Connection timeout: 10 seconds

Patch management: ☑ Include in OS patch management
☐ Include in third-party patch management
☐ Use only LANrev for OS updates

LANrev Remote: ☐ Enable screen sharing
Port: 5900
Password:
☐ Require confirmation by user

- **LANrev computer name**: The name that is displayed for the computer in the LANrev system. You can choose to use the name specified for the computer in the local operating system or you can specify a custom name that is only used by LANrev. This option is not available when there is more than one computer in the commands target list.
  You can use the variables listed in “Variables for computers” on page 401.
  The computer name can also be set automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.
- **Agent port**: The TCP port over which the Agent communicates with LANrev Server. We recommend that you do not change this port unless there is a specific reason.
- **Connection timeout**: The interval before the Agent considers an attempt to contact a server to have failed. When the attempt was made to send a regular information report (such as the heartbeat or an inventory report), the Agent retries at the next scheduled time. Attempts to download software to be deployed or to report the success of a software installation are repeated at the next opportunity.
- **Include in OS patch management**: If this option is checked, any operating system patches that are assigned to groups to which this computer belongs will be installed on this computer.

If the option is unchecked, no operating system patches from the automatic patch management will be installed.
This is discussed in more detail in "Automated patch management" on page 333.

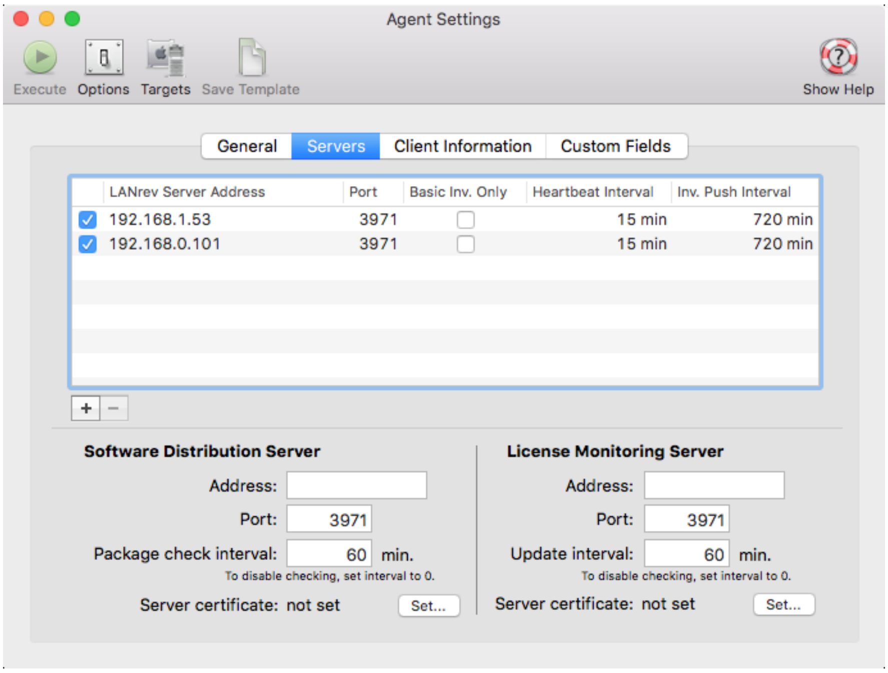
- **Include in third-party patch management**: This option is similar to **Include in OS patch management**, above, but controls the andling of third-party patches.
- **Use only LANrev for OS Updates**: When this option is checked, the Agent disables the local update mechanism of the operating system – that is, Software Update for macOS or Windows Update for Windows.
  Note that users can manually re-enable local software checks even if this setting is active. LANrev Agent will disable the local checks again the next time it starts. Also note that users can always perform manual checks for new software through the operating system mechanism.
- **Enable screen sharing**: When this option is checked, the computer allows its screen to be shared via the built-in LANrev Remote function of the Agent. (Note that disabling screen sharing here has no effect on third-party screen-sharing software.)
- **Port**: The port over which the Agent accepts screen-sharing requests.
- **Password**: The password required to authorize screen-sharing requests. If this field is left empty, no password is required.
- **Require confirmation by user**: If this option is checked, the local user of the computer has to approve all screen-sharing requests. If it is unchecked, all incoming connection requests are automatically accepted (as long as the correct password, if any, is provided).

When there is more than one target computer, checkboxes are displayed to the right of most options. Only checked options are updated in the Agents.

NOTE The options in this tab can be set only by administrators with the **Change Agent General Settings** right. See "New Administrator" on page 758 for details.

Servers

The **Servers** pane of the **Agent Settings** dialog lets you configure server addresses and communication intervals:



	LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval
☑	192.168.1.53	3971	□	15 min	720 min
☑	192.168.0.101	3971	□	15 min	720 min

Software Distribution Server

Address:

Port: 3971

Package check interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

License Monitoring Server

Address:

Port: 3971

Update interval: 60 min.

To disable checking, set interval to 0.

Server certificate: not set Set...

When there is more than one target computer, checkboxes are displayed to the right of all options outside the list. Only checked options are updated in the agents.

Main list

The main list contains the LANrev servers with which the selected agents can communicate:

- When a server is checked, all agents will be set to communicate with it.
- When a server is unchecked but present in the list, its current state on the agents will not be changed. (That is, agents that were set to communicate with it before will remain to be thus set. Agents who were not set to communicate with this server before will not be set to do so afterwards.)
- A server that is not in the list will be removed from the list of servers to communicate with on all agents; none of the target agents will communicate with this server after the command has been executed.
- A server which is checked in the **Basic Inv. Only** column will be sent only basic inventory information by the target agents. This useful for eliminating unnecessary network traffic to servers that are to act only as software distribution servers or license monitoring servers.
  The list columns contains parameters for the server that you can edit by double-clicking it opening the **Inventory Server Properties** dialog (see “Inventory Server Properties dialog” on page 819):

- **LANrev Server Address**: The IP address or DNS name of the server.
  Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).
- **Port**: The port over which the server communicates with agents.
- **Basic Inv. Only**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
- **Heartbeat Interval**: The interval in which the agents are to contact the server to let it know that they are still available.
  Note: This interval should not be longer than the Agent Offline Threshold setting of the LANrev server. (See "Server Settings" on page 780 for details.)
- **Inventory Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

You can drag the servers in the list up and down to change their order. The topmost server is the main inventory server, as described in "Assigning inventory servers to agents" on page 79.Clicking the **+** button opens a dialog that lets you add a new server to the list. The dialog is described in "Inventory Server Properties dialog" on page 819. Clicking the **–** button removes the selected server.

Software Distribution Server

- **Address**: The IP address or DNS name of the LANrev server that will be the software distribution server for the selected agents.
  Note: Here, too, we recommend using only fully qualified DNS names (or IP numbers).
- **Port**: The port over which the server communicates with agents.
- **Package check interval**: The interval in which the agents are to check the server for new or changed packages.
  Note: The same kind of check can be performed manually from the LANrev Agent control panel's **Software Updates** *pane.*
- The **Server certificate** field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
  Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

- The **Set** button lets you open a saved certificate file to validate the server.
  Saving certificate files is described in “Exporting a server certificate” on page 21.

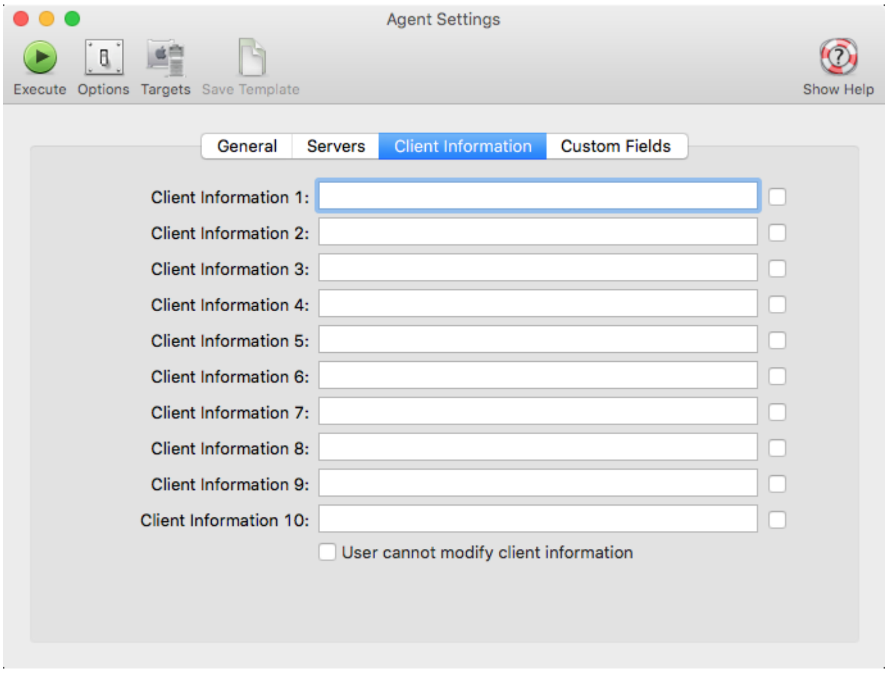
License Monitoring Server

- **Address**: The IP address or DNS name of the LANrev server that will be the license monitoring server for the selected agents.
  Note: Here, too, we recommend using only fully qualified DNS names (or IP numbers).
- **Port**: The port over which the server communicates with agents.
- **Update interval**: The interval in which the agents check the server for changes to the licensing specifications.
- The **Server certificate** field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
  Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.
- The **Set** button lets you open a saved certificate file to validate the server.
  Saving certificate files is described in “Exporting a server certificate” on page 21.

NOTE The options in this tab can be set only by administrators with the **Change Agent Server Settings** right. See “New Administrator” on page 758 for details.

Client Information

The **Client Information** pane of the **Agent Settings** dialog lets you specify the contents of the ten Client Information fields that allow, for example, locations or inventory numbers to be stored on the administered computers:



Client Information 1: □
Client Information 2: □
Client Information 3: □
Client Information 4: □
Client Information 5: □
Client Information 6: □
Client Information 7: □
Client Information 8: □
Client Information 9: □
Client Information 10: □

□ User cannot modify client information

When there is more than one target computer, checkboxes are displayed to the right of all fields. Only checked fields are updated in the agents.

You can use the variables listed in “Variables for computers” on page 401 for the specification of field values.

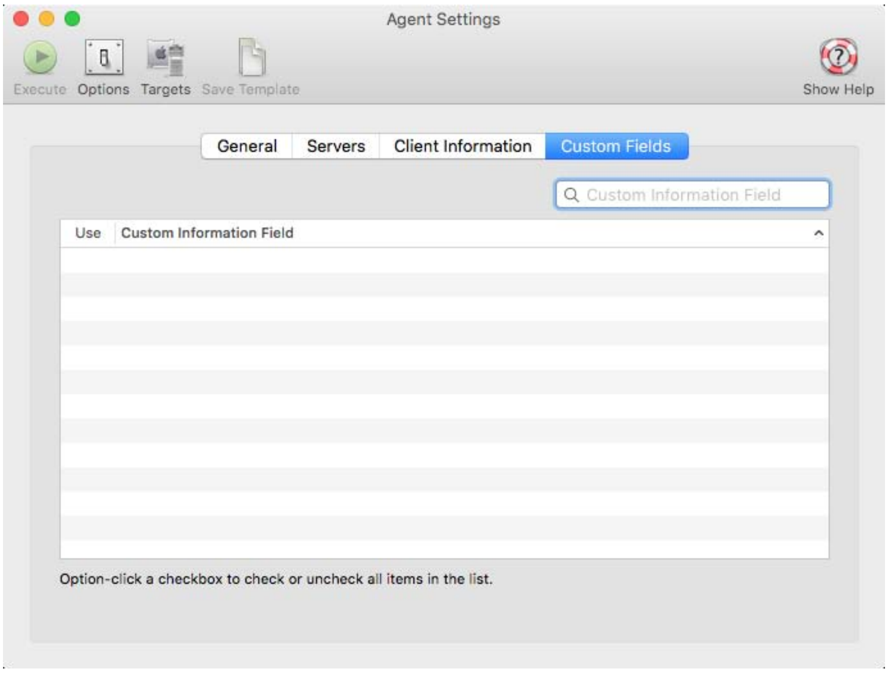
The **User cannot modify client information** option lets you prevent users from changing the fields’ contents locally or allow them to do so.

NOTE The names of the fields can be changed in the **Server Settings** dialog.

NOTE The options in this tab can be set only by administrators with the **Change Agent Client Info Settings** right. See “New Administrator” on page 758 for details.

Custom Fields

The **Custom Fields** pane of the **Agent Settings** dialog lets you assign existing custom information fields to selected agents:



Option-click a checkbox to check or uncheck all items in the list.

The dialog contains a list displaying all custom information fields that are defined on the LANrev server.

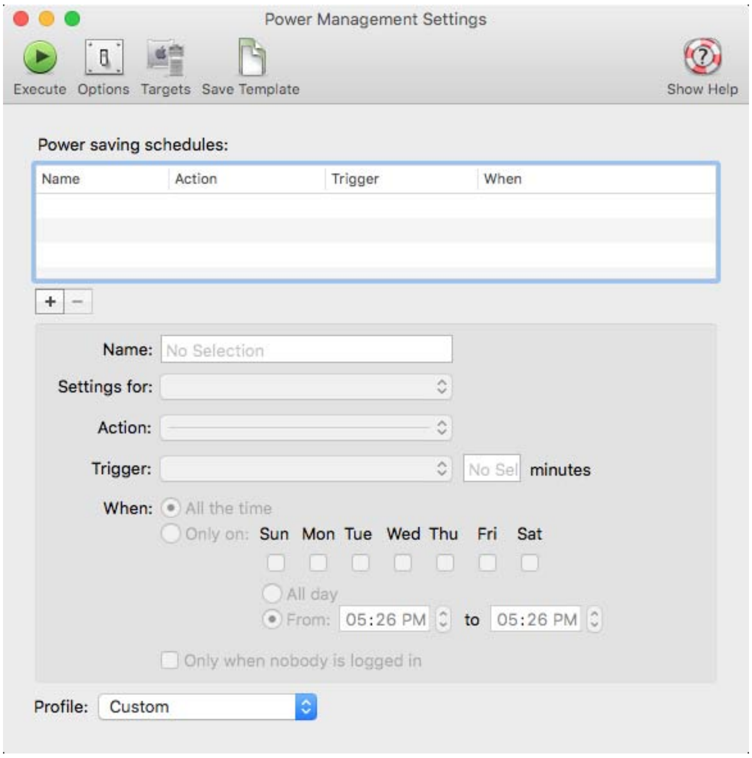
All fields that are checked in the **Use** column are assigned to the target computers; all fields that are not checked are unassigned. The status of fields whose checkbox is in the ‘neutral’ state (⊟) remains unchanged.

NOTE The options in this tab can be set only by administrators with the **Change Custom Info Fields Settings** right. See “New Administrator” on page 758 for details.

Power Management Settings

The **Power Management Settings** command lets you set the target computers’ automatic sleep and wake-up settings.

Choosing the command opens the **Power Management Settings** dialog:



Power saving schedules:

Name	Action	Trigger	When

Name: No Selection

Settings for:

Action:

Trigger: No Sel minutes

When: ● All the time

○ Only on: Sun Mon Tue Wed Thu Fri Sat

□ □ □ □ □ □ □

○ All day

● From: 05:26 PM to 05:26 PM

□ Only when nobody is logged in

Profile: Custom

The dialog contains these elements:

- **Power saving schedules**: This list contains all schedules that are to be applied to the target computers.
  You can define any number of schedules; all are applied to the targets and all are active at the same time on these computers.
  Click the **+** button to create another schedule.
  Click a schedule in the list to display its settings. You can change the settings of the selected schedule; all changes are saved automatically when you select another schedule.
  Click the **–** button to delete the selected schedule.
- **Name**: The name of the schedule.
- **Settings for**: The type of power supply to which this schedule applies. The schedule will only be active if the target computer runs on the specified type of power.
- **Action**: What is to happen when the conditions specified in this schedule are met. Available actions include:
  - **Start Up or Wake Up**: The computer is woken from sleep. If it is switched off, it is started. This option applies only to macOS clients.
  - **Wake Up**: The computer is woken from sleep. If it is switched off, nothing happens. This option applies only to macOS clients.
  - **Sleep**: The computer is put to sleep.
  - **Hibernate**: The computer is put into hibernation. This option applies only to Windows clients.
  - **Restart**: The computer is restarted. This is a ‘soft’ restart, that is, the user is prompted to save open documents that

contain unsaved changes. If these prompts are not answered, the restart fails.

- **Restart (Forced)**: The computer is restarted. This is a ‘hard’ restart, that is, there is no user prompt, all applications are terminated by force, and any unsaved changes in open documents are lost.
- **Shut Down**: The computer is shut down. This is a ‘soft’ shutdown, that is, the user is prompted to save open documents that contain unsaved changes. If these prompts are not answered, the shutdown fails.
- **Shut Down (Forced)**: The computer is shut down. This is a ‘hard’ shutdown, that is, there is no user prompt, all applications are terminated by force, and any unsaved changes in open documents are lost.
- **Log Out**: The active user is logged out. The user is prompted to save open documents that contain unsaved changes. If these prompts are not answered, the logout fails.
- **Display Sleep**: The display is dimmed to blackness.
- **Hard Disk Sleep**: The hard disks are spun down.

Before the **Sleep**, **Hibernate**, **Restart**, **Shut Down**, or **Log Out** actions are performed, an alert is displayed on the target computer that gives the user the chance to cancel the action.
Note: Individual client computers may lack the required hardware or operating system support for some options.

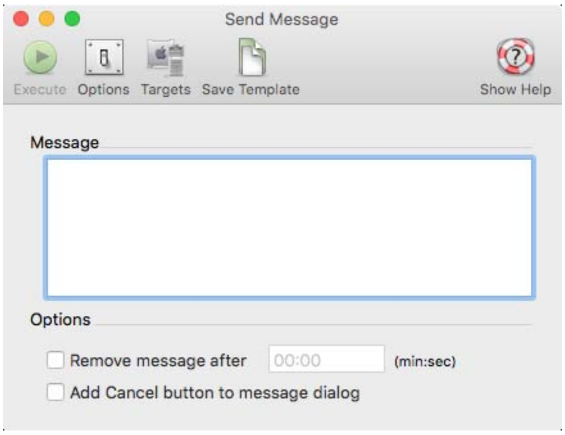
- **Trigger**: The kind of condition by which the action is triggered. You can specify that the action happens at particular times of the day or after a certain period of inactivity.
- **When**: The times of the day and the week when this schedule is to be active. You can either specify that it is active all the time or you can restrict it to certain days and times of the day. The time of the day is the same for all days. Note that the time is specified using a 24 hour clock.
- **Profile**: Using this menu, you can save the current settings for easy later recall.
  When the pop-up menu is closed, it displays the currently active profile. If no profile is active, it displays **Custom**.
  - **Save As**: Choosing this command lets you save all schedules currently listed in the list at the top of the command window under a name of your choice.
    All saved profiles are added to the pop-up menu.
  - **Rename**: Choosing this command lets you edit the name of the currently active profile. The command is unavailable if no profile is active.
  - **Delete**: Choosing this command removes the currently active profile from the **Profile** pop-up menu.
    Note: This does not remove the currently shown schedules from the command window.
- **Only when nobody is logged in**: If this option is checked, the schedule applies only as long as no user is logged in on the target computer. If it is unchecked, it applies regardless of whether a user is logged in.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Send Message

The **Send Message** command sends a message to selected client computers.

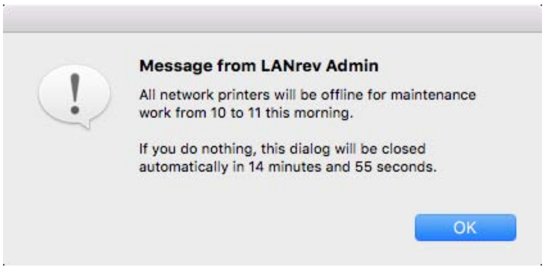
Choosing the command opens the **Send Message** dialog:



The dialog contains these elements:

- **Message**: The text that will appear on the client computers. You can use the variables listed in “Variables for computers” on page 401.
  Note: To insert a line break in the text, press Option-Return.
- **Remove message after**: If this option is chosen, you can enter a time in minutes and seconds after which the message dialog on the client computer is automatically closed.
  The dialog is closed as if the user had clicked **OK**. (The timeout is, however, noted in the command history.)
- **Add Cancel button to message dialog**: If this option is checked, the message dialog on the client computer has a **Cancel** button in addition to the **OK** button. You can see in the command history whether a user clicked the **Cancel** button.

When the command is executed, the message appears in a dialog on the screen of each selected target:


Message from LANrev Admin

All network printers will be offline for maintenance work from 10 to 11 this morning.

If you do nothing, this dialog will be closed automatically in 14 minutes and 55 seconds.

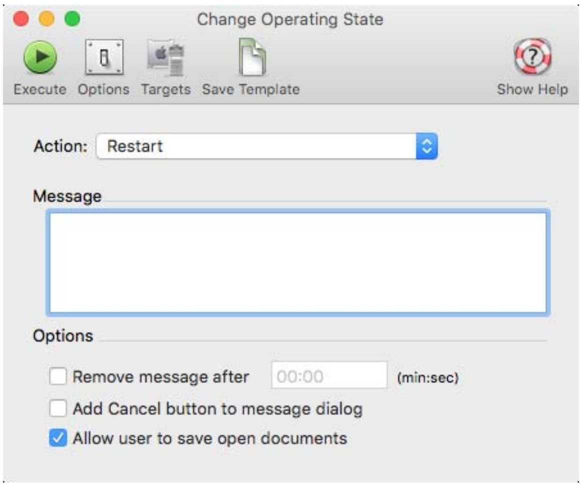
The toolbar of command windows is described in “Command window toolbar” on page 402.

Messages can also be sent automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

Change Operating State

The **Change Operating State** command restarts, shuts down, or puts to sleep remote computers or logs their users out.

Choosing the command opens the **Change Operating State** dialog:



Action: Restart

Message

Options

□ Remove message after 00:00 (min:sec)

□ Add Cancel button to message dialog

☑ Allow user to save open documents

The dialog contains these elements:

- **Action**: The desired change in the operating states of the target computers.
  The **Force restart (FileVault authenticated)** option is a forced restart that applies only to certain computers meeting all of these criteria:
  - macOS 10.8.2 and above.
  - MacBook Pro mid 2009 or newer, MacBook or iMac late 2009 or newer, Mac mini mid 2010 or newer, MacBook Air late 2010 or newer, Mac Pro late 2013 or newer.
  - The currently valid FileVault key has been stored in LANrev. (See "macOS profiles" on page 668 for more information.)

  Other computers will be simply force-restarted.
  Choosing this option lets you start the administered computer once without requiring the presence of the local user to enter the FileVault password.
  Note: This option leaves the target computers running and unlocked. Depending on the circumstances, this may present a security risk.
  Note: When you try to put to sleep a Windows computer, LANrev first tries to hibernate it. If that is not supported, it tries to put it into stand-by mode. If the computer does not support this mode either, the command fails with an error log entry.
- **Message**: An optional text that will appear on the target computers before the action is executed. Leave empty to display no message.

You can use the variables listed in “Variables for computers” on page 401.
Note: To insert a line break in the text, press Option-Return.

- **Remove message after**: If this option is chosen, you can enter a time in minutes and seconds after which the message dialog on the client computer is automatically closed.
- **Add Cancel button to message dialog**: If this option is checked, the message dialog on the client computer has a **Cancel** button in addition to the **OK** button. If a user clicks the **Cancel** button, the action is not executed on that computer.
- **Allow user to save open documents**: If this option is checked, quit events are sent to all running processes, allowing the user to save unsaved changes. If the option is unchecked, all processes are forcefully terminated and unsaved changes are lost.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Wake Up

The **Wake Up** command wakes up remote computers. There are no options for this command, but target computers must support Wake On LAN and the feature must be activated.

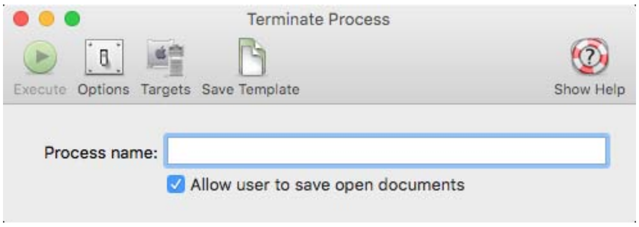
Waking up computers is possible across subnets as long as an LANrev server or agent is running (active) in the target subnet.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Terminate Process

The **Terminate Process** command stops processes running on target computers.

Choosing the command opens the **Terminate Process** dialog:



Process name:

☑ Allow user to save open documents

The dialog contains these elements:

- **Process name**: The name of the process that you want to terminate. You must enter the exact name. If you open the dialog while a process is selected in the frontmost window, the name is pre-entered. If you select more than one process, only the number of processes is shown.

- **Allow user to save open documents**: If this option is checked, quit events are sent to the target processes, allowing the user to save unsaved changes. If the option is unchecked, the processes are forcefully terminated and unsaved changes are lost.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Processes can also be terminated automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

Lock macOS Computer

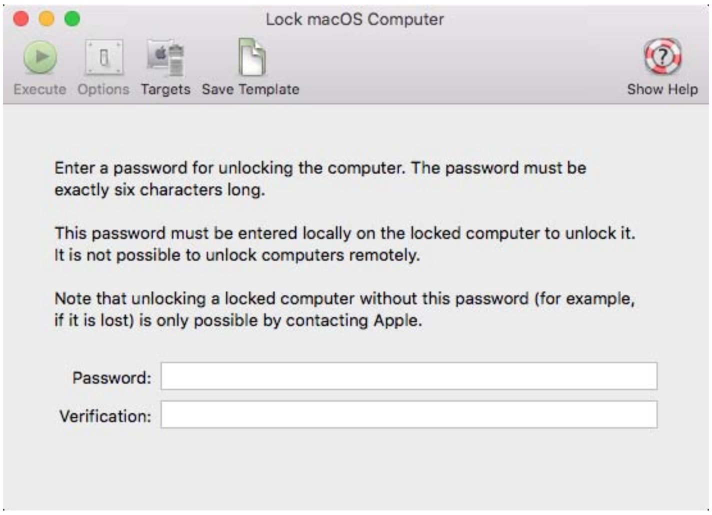
The **Lock macOS Computer** command lets you lock an MDM-managed macOS computer against any use.

This lock is not the same as requiring a login for using the computer: A lock prevents any user with an account as well as guests from using the computer until a specific unlocking password set by you is entered. This lock cannot be circumvented by using the recovery partition, booting from external volumes, or reinstalling the operating system.

The computer must be unlocked locally. It is not possible to unlock it remotely.

NOTE If you lose the unlock password, accessing the locked computers requires you to contact Apple for assistance.

Choosing the command opens the **Lock macOS Computer** dialog:



Enter a password for unlocking the computer. The password must be exactly six characters long.

This password must be entered locally on the locked computer to unlock it. It is not possible to unlock computers remotely.

Note that unlocking a locked computer without this password (for example, if it is lost) is only possible by contacting Apple.

Password:

Verification:

The dialog contains these elements:

- **Password**: The password that must be entered to unlock the computer. This password must be exactly six characters long. Repeat the password in the **Verification** field.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Erase macOS Computer

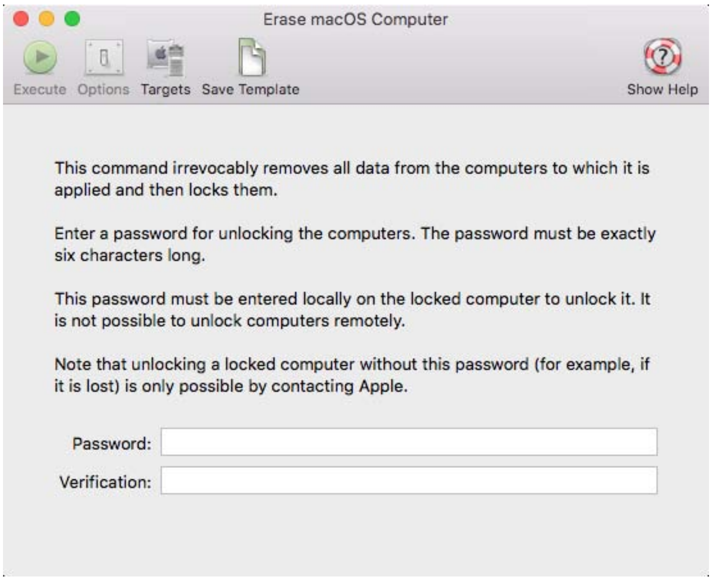
The **Erase macOS Computer** command deletes all data – operating system applications, and user data – on the selected computers, including any local external disks (but not mounted server volumes).

IMPORTANT Erasing a computer irretrievably deletes all information from all writable internal and external disks (although it might be possible to restore some of the information with specialized forensic tools). If your company is not the owner of that information, such as might be the case with BYOD computers, doing so without the owner’s consent may expose you to civil or criminal liability.

You also lock the computer against any use. This lock cannot be circumvented by using the recovery partition, booting from external volumes, or reinstalling the operating system. Using the computer again is only possible if a password specified by you is entered.

NOTE If you lose the unlock password, accessing the locked computers requires you to contact Apple for assistance.

Choosing the command opens the **Erase macOS Computer** dialog:



This command irrevocably removes all data from the computers to which it is applied and then locks them.

Enter a password for unlocking the computers. The password must be exactly six characters long.

This password must be entered locally on the locked computer to unlock it. It is not possible to unlock computers remotely.

Note that unlocking a locked computer without this password (for example, if it is lost) is only possible by contacting Apple.

Password:

Verification:

The dialog contains these elements:

- **Password**: The password that must be entered to unlock the computer. This password must be exactly six characters long. Repeat the password in the **Verification** field.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Reinstall macOS Computer

The **Reinstall macOS Computer** command lets you reinstall client computers from a specified disk image or Time Machine backup.

Choosing the command opens the **Reinstall macOS Computer** dialog. The dialog has two panes:

- **Disk Image**
- **Message**

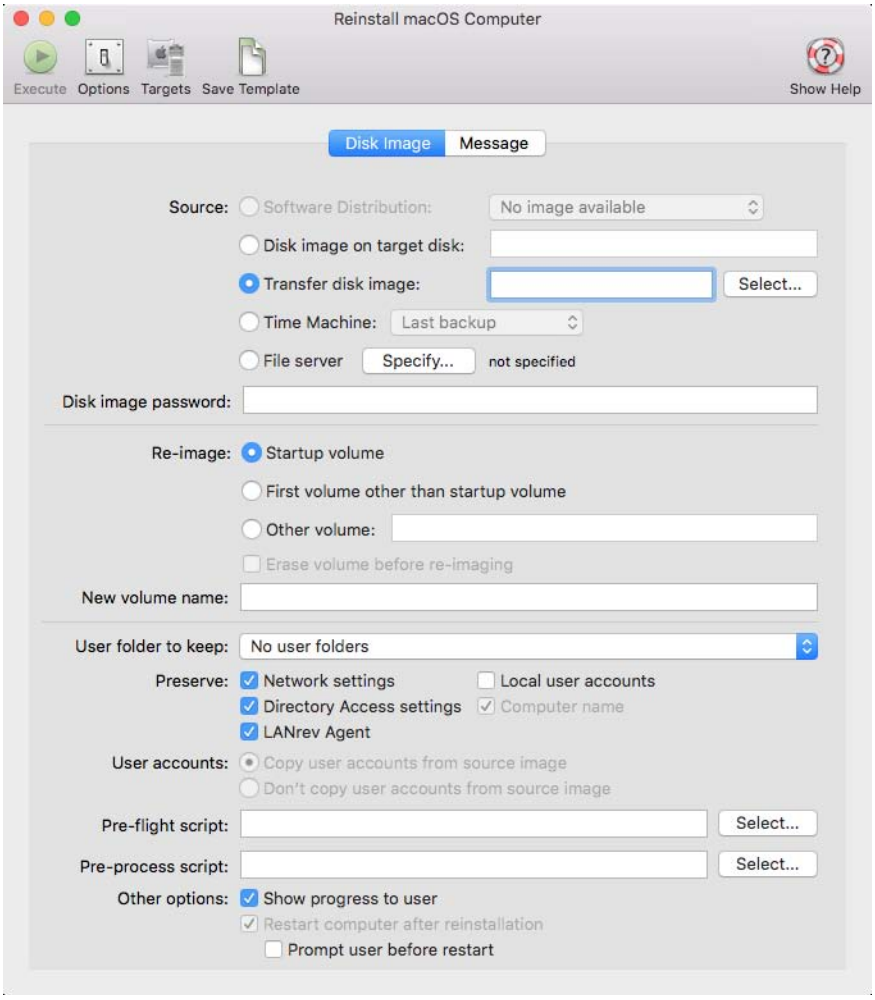
Both are described below.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Note that this command cannot be used on client computers running macOS 10.11 (El Capitan) and up when System Integrity Protection (SIP) is enabled on those computers.

Disk Image

The **Disk Image** pane of the **Reinstall macOS Computer** dialog lets you choose an image and set options for the reinstallation of the target computers.



Source: ○ Software Distribution: No image available
○ Disk image on target disk:
● Transfer disk image: Select...
○ Time Machine: Last backup
○ File server Specify... not specified

Disk image password:

Re-image: ● Startup volume
○ First volume other than startup volume
○ Other volume:
□ Erase volume before re-imaging

New volume name:

User folder to keep: No user folders

Preserve: ☑ Network settings □ Local user accounts
☑ Directory Access settings ☑ Computer name
☑ LANrev Agent

User accounts: ● Copy user accounts from source image
○ Don't copy user accounts from source image

Pre-flight script: Select...

Pre-process script: Select...

Other options: ☑ Show progress to user
☑ Restart computer after reinstallation
□ Prompt user before restart

The dialog contains the following elements:

- **Software Distribution**: When one of the disk images available in the Software Distribution Center is chosen from the pop-up menu, that image’s contents will be written to the boot volumes of the target computers.
- **Disk image on target disk**: Specify the path to a disk image that is already present on the intended target disk.
- **Transfer disk image**: Choosing **Transfer disk image** allows you to select a disk image file on your computer instead of one from the Software Distribution Center. Clicking **Select** opens an **Open** dialog for choosing the image.
- **Time Machine**: If the target computer runs macOS 10.5 or newer and Time Machine is active on it, you can specify that a Time Machine Backup be restored. The pop-up menu lets you specify a date; LANrev restores the last backup prior to that date.

- **File server**: Specify a disk image that is located on a file server. Clicking the **Specify** button opens a dialog in which you specify the server and the location of the disk image on it:
  - **Disk image source**: The path of the disk image on the server volume.
  - **Server address**: The file server's network address.
  - **Server volume**: The volume on which the disk image is located.
  - **User**: The user account which LANrev is to use for logging in to the server.
  - **Password**: The password for the account.
- **Disk image password**: If the image is password-protected, enter the password here.
- **Re-image**: The volume on which the disk image's contents is to be installed. Options include:
  - **Startup volume**: The selected client's current boot volume.
  - **First volume other than startup volume**: The second volume in the client's volume list, with the startup volume considered the first volume in the list.

IMPORTANT This option is primarily intended to allow you to reinstall the (sole) local volume of a computer that has been booted from a network volume. If there are more than two volumes on a client, there is no way to tell which of the non-startup volumes will be chosen. We strongly recommend against using this option on computers with more than two mounted volumes.

  - **Other volume**: The name of a local volume of the client. You can use the variables listed in “Variables for computers” on page 401.
- **New volume name**: The name that the target computers' boot volumes will have after the reinstallation.
  You can use the variables listed in “Variables for computers” on page 401.
- **User folder to keep**: Whether to keep any user folders (that is, subfolders of the **Users** folder belonging to individual users) during the reinstallation and, if so, which ones:
  - **No user folders**: All user folders will be deleted during the reinstallation.
  - **Folder of current user**: The user folder of the user who is currently logged in will be preserved; all others will be deleted.
  - **All user folders**: All user folders will be preserved.
- **Preserve**: Preserve the target computers' current network settings during the reinstallation:
  - **Network settings**: General network settings.
  - **Directory Access settings**: Settings related to accessing directory services such as Active Directory.
  - **LANrev Agent**: The LANrev agent with all its settings.
  - **Local user accounts**: Currently existing user accounts on the target computers.
  - **Computer name**: The name of the computer by which it is known in the network.

- **User accounts**: If **Copy user accounts from the source image** is chosen, all user accounts that have been defined on the source image, including their access privileges and data, are copied to the reinstalled computer. If **Don’t copy user accounts from the source image** is chosen, no accounts from the source image are added to the preserved accounts (if any) on the target computer.
- **Pre-flight script**: Clicking the **Select** button allows you to specify a shell script that is executed on the target computers after the disk has been mounted but before any files have been copied to the local hard disk.
  These parameters are supplied to the script:
  - $1: the disk image mount point
  - $2: the name of the specified target volume (**/** for the boot volume)
- **Pre-process script**: Clicking the **Select** button allows you to specify a shell script that is executed on the target computers before the reinstallation.
  These parameters are supplied to the script:
  - $1: the path to the folder where the installation files have been copied
- **Other options**: Additional settings for the reimaging process:
  - **Show progress to user**: A progress bar on the local computer keeps the user informed of the process state.
  - **Restart computer after reinstallation**: If this option is checked, the target computer is rebooted when the installation is complete. When the startup volume is reinstalled, this option cannot be deactivated.
  - **Prompt user before restart**: If this option is checked, a dialog is displayed on the target computer, allowing the user to postpone restarting. This gives local users additional time to save open documents, etc.

Message

The **Message** tab of the **Reinstall macOS Computer** dialog lets you send a message to target computers before their computers are reinstalled. A black diamond on the tab ◆ Message indicates that a message has been specified, even when you select another tab.

The elements of this pane are described in “Send Message” on page 415.

If a **Cancel** button is added to the dialog, any target computer on which the user clicks **Cancel** will not be reinstalled.

Reinstall Windows Computer

The **Reinstall Windows Computer** command lets you reinstall client Windows computers from a specified disk image on the FOG server.

In addition to administered computers with agents you can also specify placeholder records as targets. See “Creating placeholder records for computers” on page 90 for information on how to create placeholder records.

Using the command requires a FOG server or LANrev PXE server in addition to LANrev Server. The required installation procedure is described in “Installing support for reinstalling Windows computers” on page 22.

Choosing the command opens the **Reinstall Windows Computer** dialog. The dialog has two panes:

- **Disk Image**
- **Message**

Both are described below.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Disk Image

The **Disk Image** pane of the **Reinstall Windows Computer** dialog lets you choose an image and set options for the reinstallation of the target computers.

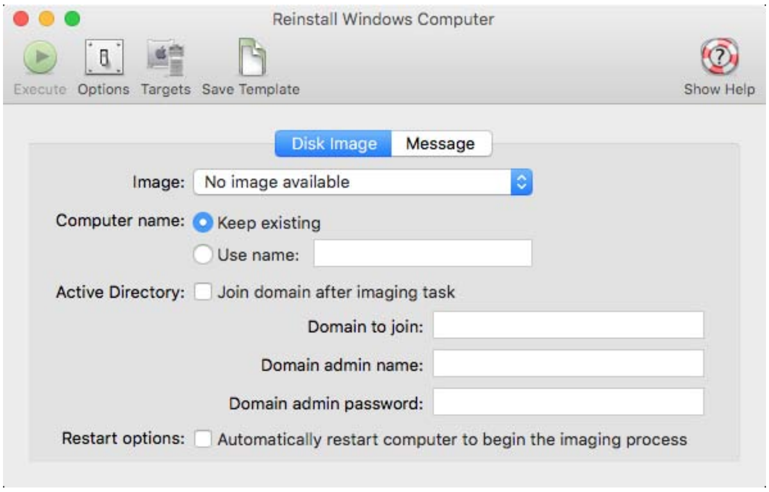


Image: No image available

Computer name: ● Keep existing

○ Use name:

Active Directory: □ Join domain after imaging task

Domain to join:

Domain admin name:

Domain admin password:

Restart options: □ Automatically restart computer to begin the imaging process

The dialog contains the following elements:

- **Image**: This pop-up menu includes all disk images that are stored on the FOG server (if you use FOG) or in LANrev Server under Windows Disk Images (if you use the LANrev PXE server).
- **Computer name**: The name to give the target computer:
  - **Keep existing**: After the reinstallation, the computer has the same name as now.
  - **Use name**: The name is changed to the specified name during reinstallation.
- **Join domain after imaging task**: If this option is checked, the computer joins the specified Active Directory domain after the reinstallation.
- **Domain name**: The name of the Active Directory domain to join.
  You can use the variables listed in “Variables for computers” on page 401.

- **Domain admin name**: The username of an administrator account for the domain controller. You can also enter the UPN (user principal name) for the account.
- **Domain admin password**: The password for the administrator account.
- **Automatically restart computer to begin the imaging process**: If this option is checked, the selected target computers are automatically restarted to begin the reinstallation.
  This option has no effect on target computers without an agent (that is, target computers that have been specified by means of placeholder records).

Message

The **Message** tab of the **Reinstall Windows Computer** dialog lets you send a message to target computers before their computers are reinstalled. A black diamond on the tab ◆ Message indicates that a message has been specified, even when you select another tab.

Messages cannot be sent to selected target computers without agents (that is, computers that are represented by placeholder records).

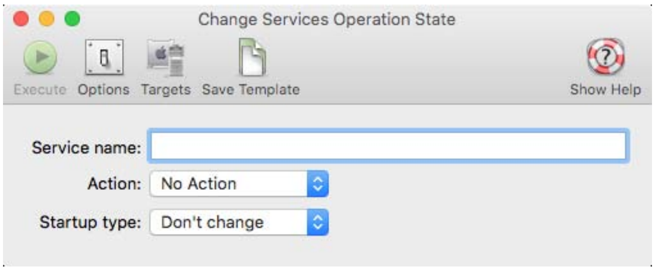
The elements of this pane are described in “Send Message” on page 415.

If a **Cancel** button is added to the dialog, any target computer on which the user clicks **Cancel** will not be reinstalled.

Change Services Operation State

The **Change Services Operation State** command allows you to start or stop services on Windows computers and set their startup states.

Choosing the command opens the **Change Services Operation State** dialog:



Service name:
Action: No Action
Startup type: Don't change

The dialog contains these elements:

- **Service name**: The name of the service you wish to affect, as displayed in the **Service Name** information item.
  If a single service is selected in a browser window when you open the command dialog, its name is pre-entered in the field. If more than one service is selected, the number of services is displayed in the field.

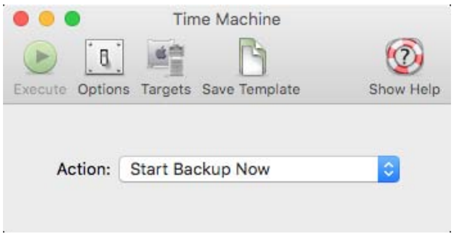
- **Action**: The change to the operating state that you want to affect.
- **Startup type**: The startup status to which you want to set the selected services:
  - **Automatic**: The service is automatically started whenever the operating system boots.
  - **Manual**: The service is not automatically started but may be started by users or other applications.
  - **Disabled**: The service cannot be started at all.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Time Machine

The **Time Machine** command lets you control the operation of Time Machine on target computers. The command can only be used on target computers running macOS 10.5 or later.

Choosing the command opens the **Time Machine** dialog:



Action: Start Backup Now

The dialog contains these elements:

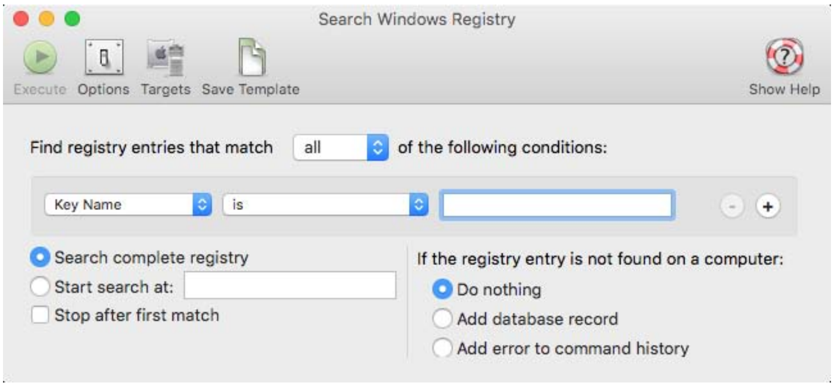
- **Action**: The action that you want Time Machine to perform.
  - **Start Backup Now**: The target computers immediately begin a Time Machine backup.
    Note: This command has an effect only on target computers where a Time Machine disk has already been specified.
  - **Stop Running Backup**: Any Time Machine backups in progress on the target computers are immediately stopped.
  - **Enable Automatic Backup**: On all target computers, automatic Time Machine backups are enabled. (This has the same effect as sliding the master switch in the Time Machine control panel to **On**.)
    Note: This command has an effect only on target computers where a Time Machine disk has already been specified.
  - **Disable Automatic Backup**: On all target computers, automatic Time Machine backups are disabled. (This has the same effect as sliding the master switch in the Time Machine control panel to **Off**.)

The toolbar of command windows is described in “Command window toolbar” on page 402.

Search Windows Registry

The **Search Windows Registry** command allows you search for keys and values in the registries of administered Windows computers.

Choosing the command opens the **Search Windows Registry** dialog:



Find registry entries that match all of the following conditions:

Key Name | is |

● Search complete registry
○ Start search at:
□ Stop after first match

If the registry entry is not found on a computer:
● Do nothing
○ Add database record
○ Add error to command history

The dialog contains these elements:

- **Find registry entries that match**: When **all** is chosen from this pop-up menu, registry entries are found that match all specified conditions (Boolean AND). If **any** is chosen, entries are found that match at least one of the specified conditions (Boolean OR).
- Condition area: The first pop-up menu lets you choose a condition to match registry entries. The second one contains the possible comparison operators. For most conditions, one or two text field lets you specify the value to compare entries against. The **+** and **–** buttons let you add new conditions or remove existing ones.
  These search criteria are available:
  - **Key At**: Enter a full path of a key to check whether the key exists (or does not exist) on the target computers.
  - **Value At**: As **Key at**, but for values.
  - **String At**: Enter the full path of a string type value and compare it against a fixed value.
  - **Number At**: As **String at**, but for numbers.
  - **Binary At**: As **Binary at**, but for binary values.
  - **Key Path**: Search for keys by partial paths – all keys are found whose paths contain the search string. The keys' names are not considered part of their paths.
  - **Value Path**: As **Key Path**, but for values.
  - **Key Name**: Search for keys by their names.
  - **Value Name**: As **Key Name**, but for values.
  - **String Value**: Search for string values by their contents.
  - **Number Value**: As **String Value**, but for numbers.

  When you specify a path, you can include environment variables, as described in “Environment variables” on page 176.
- **Search complete registry**: The entire registries of the target computers are searched.

- **Start search at**: When this option is checked and a path in the registry is specified, only keys and values below that path are searched.
- **Stop after first match**: If a matching file has been found on a target computer, the search is stopped on that computer.
- **If the registry entry is not found on a computer**: Specify what LANrev is to do when the registry search returns no hits on a particular target computer:
  - **Do nothing**: No particular action is taken; no entries from this computer appear in the **Registry Entries** window.
  - **Add database record**: A record is created in the Registry Entries database with a value of "No" in the **Registry Entry Found** information item.
  - **Add error to command history**: An error entry, stating that the key could not be found, is added to the **History** section of the **Commands** window.

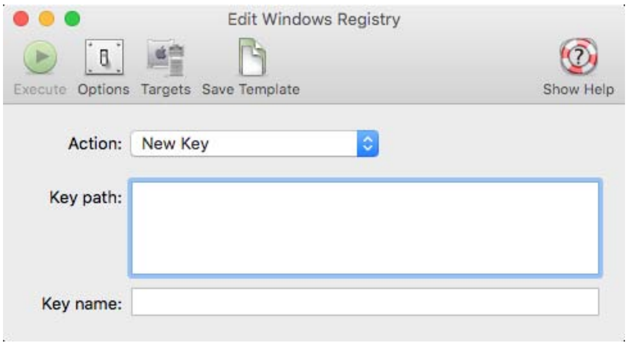
Any found registry entries are added to the Registry Entries database and displayed in the **Registry Entries** window.

The toolbar of command windows is described in "Command window toolbar" on page 402.

Edit Windows Registry

The **Edit Windows Registry** command allows you add, edit or delete keys and values in the registries of administered Windows computers.

Choosing the command opens the **Edit Windows Registry** dialog



Action: New Key

Key path:

Key name:

The dialog contains these elements:

- **Action**: This pop-up menu lets you specify the desired action that you want to perform in the target computers' registries. These actions are available:
  - **New Key**: Create a new key at a specified path.
  - **New Value**: Create a new value in a specified key.
  - **Change Value**: Alter a value at a specified location.
  - **Delete Key**: Delete a specified key and all its contents.
  - **Delete Value**: Delete a specified value.
  - **Rename Key**: Change the name of a specified key.
  - **Rename Value**: Change the name of a specified value.

Additional elements let you enter key and value specifications and data. Which of them are visible depends on the chosen action. In these fields, you can use the variables listed in “Variables for computers” on page 401.

This is a list of all elements; only a subset is visible in each case:

- **Key path**: The path of an existing key in which a new key or value is to be created.
- **Key name**: The name of the new key that you want to create.
- **Value path**: The path of a value that is to be changed.
- **Value type**: The data type of a new value or of a value that is to be changed.
- **Value**: The new data of a value.
- **Path**: The path of a key or value that is to be deleted or renamed.
- **New name**: The new name of a key or value.

When you specify a path, you can include environment variables, as described in “Environment variables” on page 176.

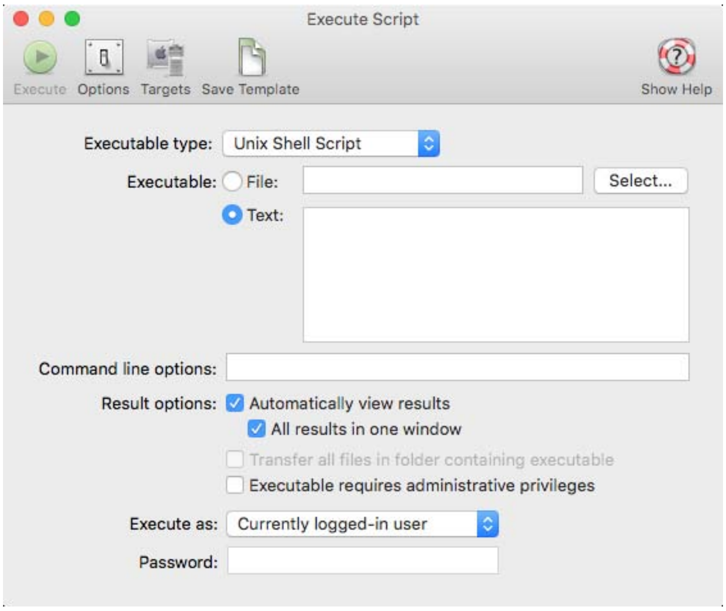
The toolbar of command windows is described in “Command window toolbar” on page 402.

The Windows registry can also be modified automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

Execute Script

The **Execute Script** command executes script files on the target computers.

Choosing the command opens the **Execute Script** dialog:



Executable type: Unix Shell Script

Executable: ○ File:

● Text:

Command line options:

Result options: ☑ Automatically view results

☑ All results in one window

□ Transfer all files in folder containing executable

□ Executable requires administrative privileges

Execute as: Currently logged-in user

Password:

The dialog contains these elements:

- **Executable type**: The type of program that is to run on the clients to gather the information for the field:
  - Unix shell script (macOS targets)
  - AppleScript (macOS targets)
  - DOS batch file (Windows targets)
  - Visual Basic script (Windows targets)
  - PowerShell script (Windows targets)

  Depending on the choice made in this pop-up menu, different fields become available in the dialog pane.
- **File**: The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for all executable types.)
  Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to LANrev Server.
- **Text**: The text of a script can be entered in this field. The entered script is executed on the target computers. (This option is available for all executable types.)
  You can use the variables listed in “Variables for computers” on page 401.
  Note: LANrev offers syntax verification functions only for AppleScript scripts; we strongly recommend that you test the scripts before entering them here.
- **Transfer all files in folder containing executable**: If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the script is executed. (This option is available for all executable types.)
  Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).
- **Command line options**: Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question).
  You can use shell variables in the options, as described in “Environment variables” on page 176.
- **Automatically view results**: If this option is checked, the results that the scripts return are automatically displayed in result windows on your computer. (By default, they are just entered in the command history.)
  If **All results in one window** is checked, all returned script results are displayed together in a single window. Clicking a computer in the window’s upper half scrolls the lower half to that computer’s results.
  If **All results in one window** is unchecked, a separate window is opened for each script result.
- **Executable requires administrative privileges**: If this option is checked, the specified script is executed with administrator privileges on the target computers. (This option is available for the **Unix Shell Script** executable type.)
- **Execute as**: This pop-up menu allows you to specify a user account on the target computers with the privileges of which

the script is executed. (This option is available for the **Unix Shell Script**, **DOS Batch File**, **Visual Basic Script**, and **PowerShell** executable types.)

NOTE The result of the script execution, if any, can be displayed via the **Show Command Result** context menu command in the **Commands** window.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Scripts can also be executed automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

Execute macOS File

The **Execute macOS File** command runs applications from the administrator’s computer on target macOS computers, providing special options for running installer applications.

These file types are supported:

- .pkg and .mpkg files for Apple’s Installer
- Installers based on MindVision’s InstallerVISE engine
- Other installers that contain the installer engine and all required installer files with a single application
- Other applications and AppleScript applets
- Shell scripts and other scripts (text files for which the executable bit is set and which begin with #!)

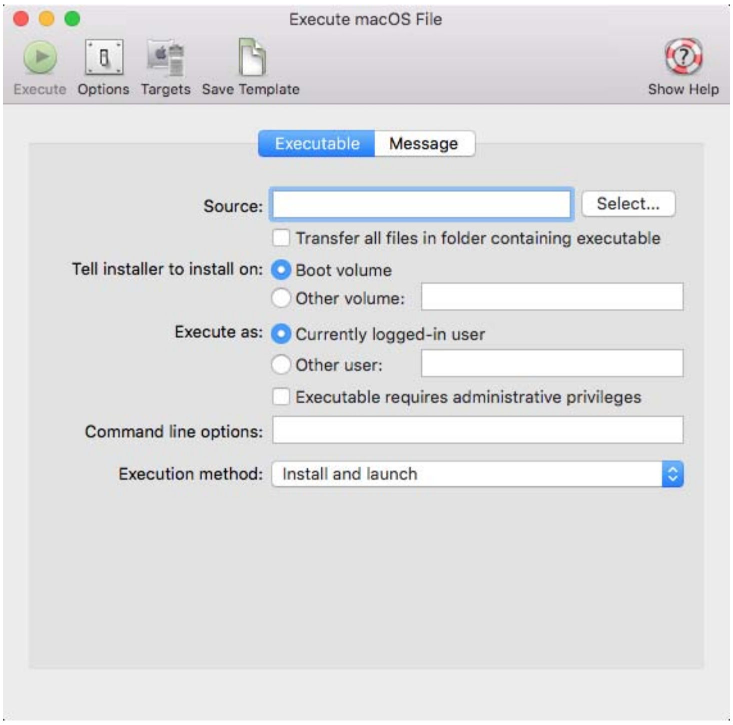
Choosing the command opens the **Execute macOS File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 402.

Executable

The **Executable** tab of the **Execute macOS File** dialog lets you specify the file to execute and the manner of its execution:



Source:

□ Transfer all files in folder containing executable

Tell installer to install on: ● Boot volume

○ Other volume:

Execute as: ● Currently logged-in user

○ Other user:

□ Executable requires administrative privileges

Command line options:

Execution method: Install and launch

The tab contains these elements:

- **Source**: The file on your computer or on the server that is to be executed.
- **Select**: Clicking this button opens a dialog in which the file to be executed can be selected.
- **Transfer all files in folder containing executable**: If this option is selected, LANrev transfers not only the executable itself to the target computer but also any other files that are located in the same folder.
- **Tell installer to install on**: The volume where the installer is to install the software.
  You can use the variables listed in “Variables for computers” on page 401.
  Note: Specifying a target volume may not be supported by all installers.
- **Execute as**: The user with whose privileges the application is to run.
  You can use the variables listed in “Variables for computers” on page 401.
- **Executable requires administrative privileges**: If this option is checked, the Agents run the script with system administrator privileges.
- **Command line options**: Any text entered in this field is passed as a parameter to the application.
  You can use shell variables in the options, as described in “Environment variables” on page 176.
- **Execution method**: Whether the installer is copied to the target computers or run from a server:

  - **Install and launch**: The specified file is copied from the administrator's computer to the target computers and run there.
  - **Launch from server**: The specified server volume (see below) is mounted, the file executed, and the server volume unmounted.
  - **Launch using server URL**: The specified file (see URL, below) on a server is executed.

  You can use the variables listed in "Variables for computers" on page 401 in the following fields.
- **Address**: The IP address or DNS name of the server.
  SMB server addresses must be prefixed by a double backslash, according to UNC notation.
  Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain), if you use DNS names.
- **Volume**: The volume of the server on which the file is located.
- **User**: The username to use to connect to the server.
- **Password**: The password to use to connect to the server.
- **URL**: The URL of the server volume. The URL is made up of several elements, some of which are optional, in this order:
  - The protocol (`afp` or `smb`), followed by `://`
  - Optionally a username followed by `@`
  - Optionally for AFP servers `;AUTH=` and an authentication type (see below)
  - Optionally `:` and a password
  - The server's IP address or DNS name
  - Optionally, `:` and a port number
  - The path of the server volume to use

  The following authentication methods are supported:
  - No User Authent
  - Cleartxt Passwrd
  - Randum Exchange
  - 2-Way Randnum
  - DHCAST128
  - DHX2
  - Client Krb v2
  - Microsoft V1.0

  These are two sample URLs:
  - afp://username:userpass@server.company.com/volumename/
  - afp://user:pass;AUTH=Cleartxt Passwrd@server.company.com/volumename/

  Note the space in the **AUTH** parameter in the second example.

Message

The **Message** tab of the **Execute macOS File** dialog lets you send a message to target computers before the file is executed. A black diamond on the tab ◆ Message indicates that a message has been specified, even when you select another tab.

The elements of this pane are described in “Send Message” on page 415.

If a **Cancel** button is added to the dialog, the file will not be executed on any target computer on which the user clicks **Cancel**.

Execute Windows File

The **Execute Windows File** command runs applications or .BAT files from the administrator’s computer on target Windows computers.

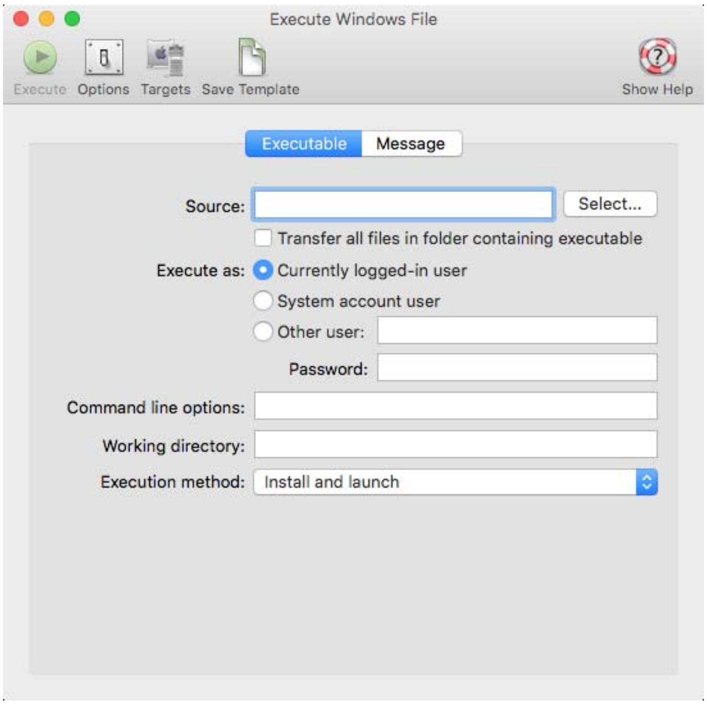
Choosing the command opens the **Execute Windows File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 402.

Executable

The **Executable** tab of the **Execute Windows File** dialog lets you specify the file to execute and the manner of its execution:



Source:

□ Transfer all files in folder containing executable

Execute as: ● Currently logged-in user
○ System account user
○ Other user:
Password:

Command line options:

Working directory:

Execution method: Install and launch

The tab contains these elements:

- **Source**: The file on your computer or on the server that is to be executed.
- **Select**: Clicking this button opens a dialog in which the file to be executed can be selected.

- **Transfer all files in folder containing executable**: If this option is selected, LANrev transfers not only the executable itself to the target computer but also any other files that are located in the same folder.
- **Execute as**: The user with whose privileges the application is to run.
- **Command line options**: The command line options with which the file is launched on the target computer.
  You can use shell variables in the options, as described in "Environment variables" on page 176.
  Note: When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options, LANrev adds the `/qn` *option (*`/quiet /norestart` *for MSU files) to run the installer silently.*
- **Working directory**: The working directory for the file's execution on the target computers.
  You can use the variables listed in "Variables for computers" on page 401.
- **Execution method**: Whether the installer is copied to the target computers or run from a server:
  - **Install and launch**: The specified file is copied to the target computers and run there.
  - **Launch from server**: The specified server volume (see below) is mounted, the file executed, and the server volume unmounted.
  - **Launch using server URL**: The specified file (see URL, below) on a server is executed.
- **Address**: The IP address or DNS name of the server.
  SMB server addresses must be prefixed by a double backslash, according to UNC notation.
  Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain), if you enter a DNS name.
- **Volume**: The volume of the server on which the file is located.
- **User**: The username to use to connect to the server.
  For Windows clients in networks with domains, the username must be specified as **domain\username**.
- **Password**: The password to use to connect to the server.
- **URL**: The URL of the server volume. The URL is made up of several elements, some of which are optional, in this order:
  - The protocol (`smb`), followed by `://`
  - Optionally a username followed by `@`
  - Optionally `:` and a password
  - The server's IP address or DNS name
  - Optionally, `:` and a port number
  - The path of the server volume to use

Message

The **Message** tab of the **Execute Windows File** dialog lets you send a message to target computers before the file is executed. A black diamond on the tab ◆ Message indicates that a message has been specified, even when you select another tab.

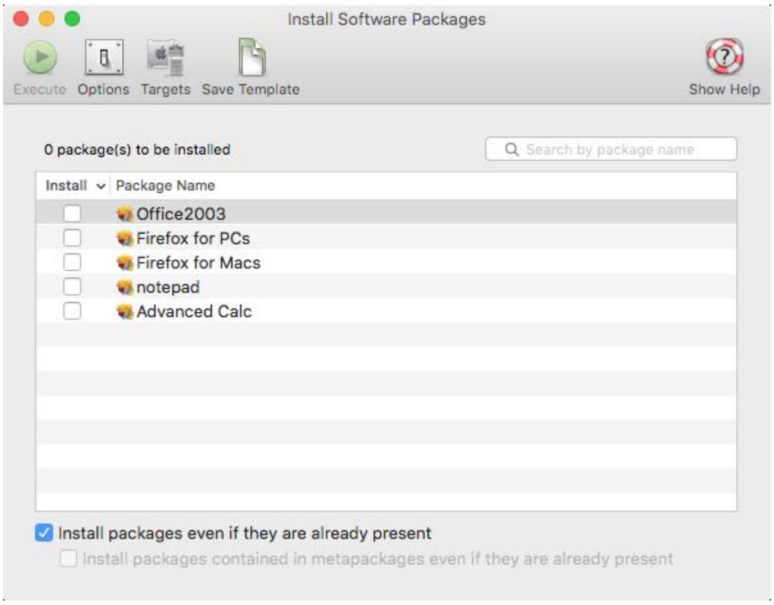
The elements of this pane are described in “Send Message” on page 415.

If a **Cancel** button is added to the dialog, the file will not be executed on any target computer on which the user clicks **Cancel**.

Install Software Packages

The **Install Software Packages** command lets you install a software package or metapackage on target computers without having to create a distribution group.

Choosing the command opens the **Install Software Packages File** dialog:



0 package(s) to be installed

Install	Package Name
□	Office2003
□	Firefox for PCs
□	Firefox for Macs
□	notepad
□	Advanced Calc

☑ Install packages even if they are already present

□ Install packages contained in metapackages even if they are already present

The dialog contains these elements:

- Search field: Enter part of the name of a software package here to restrict the display to packages with matching names.
- List of packages: Check all packages that you want to install.
- **Install packages even if they are already present**
  If this option is checked, packages are installed on the target computers even if they are already present.
  If the option is unchecked, the selected packages are installed only on those target computers that do not already have them.
- **Install packages contained in metapackages even if they are already present**
  If this option is checked, all packages contained in selected metapackages are installed on the target computers even if they are already present.

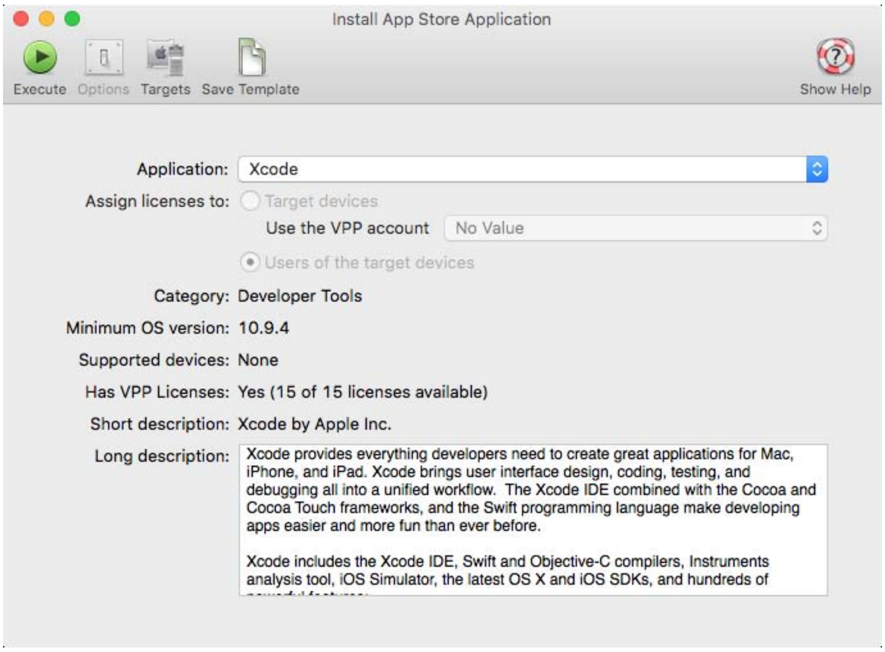
If the option is unchecked, packages in the selected metapackages are installed only on those target computers that do not already have them.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Install Mac App Store Application

The **Install Mac App Store Application** command lets you install an application from the app store on selected Macs.

Choosing the command opens the **Install App Store Application** dialog:



Application: Xcode

Assign licenses to: ○ Target devices

Use the VPP account: No Value

● Users of the target devices

Category: Developer Tools

Minimum OS version: 10.9.4

Supported devices: None

Has VPP Licenses: Yes (15 of 15 licenses available)

Short description: Xcode by Apple Inc.

Long description: Xcode provides everything developers need to create great applications for Mac, iPhone, and iPad. Xcode brings user interface design, coding, testing, and debugging all into a unified workflow. The Xcode IDE combined with the Cocoa and Cocoa Touch frameworks, and the Swift programming language make developing apps easier and more fun than ever before.

Xcode includes the Xcode IDE, Swift and Objective-C compilers, Instruments analysis tool, iOS Simulator, the latest OS X and iOS SDKs, and hundreds of

The dialog contains these elements:

- **Application**: This pop-up menu contains all App Store applications that have been imported into LANrev, as described in “Creating app packages for Mac App Store apps” on page 320.
- **Assign licenses to**: When installing compatible applications, you can choose whether to install the licenses to the devices or the users of the devices:
    - **Target devices**: If this option is chosen, the license is assigned to the selected devices. Choose the VPP account from which the license is to be taken.
      This option is available only for devices running macOS 10.11 (El Capitan) and up, and only for compatible applications.
    - **Users of target devices**: If this option is chosen, the license is assigned to the users of the selected devices.

- Information fields: Non-editable fields that display the information that was specified for the application in its application package. In addition, you can see whether this application was purchased as part of the VPP.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Transfer File/Folder

The **Transfer File/Folder** command copies files or folders from your hard disk to those of target computers.

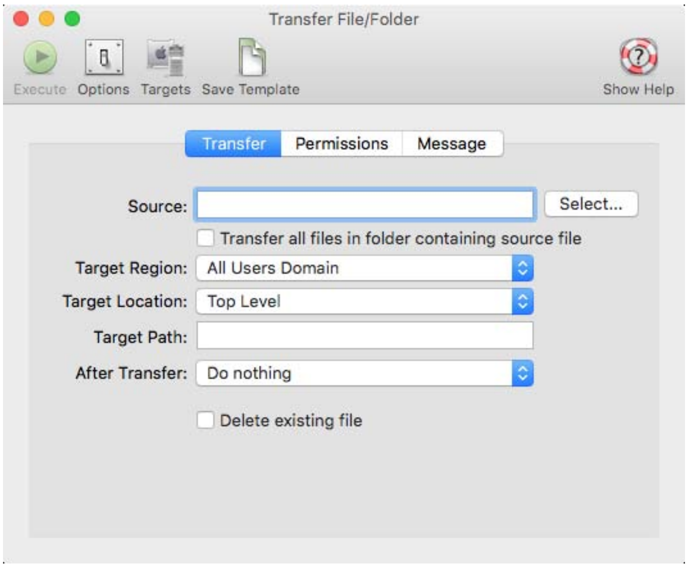
Choosing the command opens the **Transfer File/Folder File** dialog, which has three tabs:

- **Transfer**
- **Permissions**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 402.

Transfer

The **Transfer** tab of the **Transfer File/Folder** dialog lets you specify the files or folders to be transferred from your computer:



Transfer File/Folder

Source:

□ Transfer all files in folder containing source file

Target Region: All Users Domain

Target Location: Top Level

Target Path:

After Transfer: Do nothing

□ Delete existing file

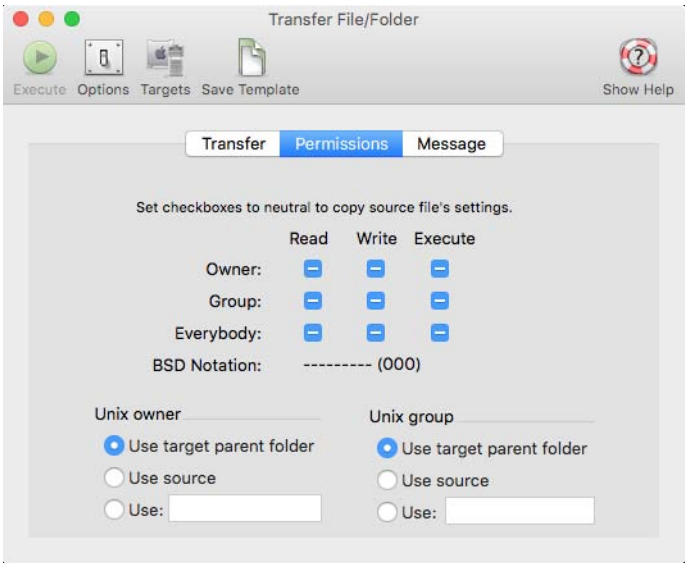
The tab contains these elements:

- **Source**: The file or folder on your computer or on the server that is to be transferred.
- **Select**: Clicking this button opens a dialog in which the file or folder to be transferred can be selected.
- **Transfer all files in folder containing source file**: If this option is selected, LANrev transfers not only the selected file itself to the target computer but also any other files that are located in the same folder.

- **Transfer contents of disk image**: When a disk image has been selected as the source file, the **Transfer all files in folder containing source file** option becomes this option. Checking it makes LANrev transfer not the disk image itself but its contents to the target computers' boot volumes. In this case, the **Target Region**, **Target Location**, and **Target Path** options are not available; the folder structure from the disk image is mirrored on the boot volumes.
- **Target Region**: The general domain where the files or folders are to be transferred to. The available regions are explained in "Copy File/Folder" on page 441.
- **Target Location**: The specific location within the target region where the files or folders are to be transferred to. The available locations are explained in "Copy File/Folder" on page 441.
- **Target Path**: The path of a folder within the specified target location where the files or folders are to be transferred to (optional).
  When **Use Path Only** is chosen as the location, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Music for the user's music folder.)
  For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in "Environment variables" on page 176.
  You can use the variables listed in "Variables for computers" on page 401.
- **After Transfer**: What LANrev is to do with a file or folder after having transferred it:
  - **Do nothing**: No action is taken beyond transferring the file or folder.
  - **Open file**: Open the file, same as using the **Open File** command (see "Open File" on page 449).
  - **Open file with admin privileges**: Open the file, same as using the **Open File** command. The file is opened with administrator privileges.
- **Delete existing file**: If this option is checked, a file at the target location with the same name as a transferred file or folder is replaced. If the option is unchecked, the transfer fails if a file with the same name already exists.

Permissions

The **Permissions** tab of the **Transfer File/Folder** dialog lets you specify the access permissions for the transferred files on macOS target computers:



Set checkboxes to neutral to copy source file's settings.

	Read	Write	Execute
Owner:	⊟	⊟	⊟
Group:	⊟	⊟	⊟
Everybody:	⊟	⊟	⊟

BSD Notation: --------- (000)

Unix owner
● Use target parent folder
○ Use source
○ Use:

Unix group
● Use target parent folder
○ Use source
○ Use:

The tab contains these elements:

- **macOS Permissions**: The access permissions:
  ☑ This permission is set for the transferred file or folder.
  ⊟ This permission is set to the same value for the transferred file or folder as for the source file on your computer.
  □ This permission is not set for the transferred file or folder.
  The permissions are displayed in standard BSD notation below the array for easy verification.
- **Unix owner**: When a file or folder is transferred to a macOS target, its owner can be set. The owner can either be the owner of the parent folder on the target computer, the owner of the source file on your computer, or a specified user of the target computer.
  You can use the variables listed in "Variables for computers" on page 401.
- **Unix group**: When a file or folder is transferred to a macOS target, its group can be set. The group can either be the group of the parent folder on the target computer, the group of the source file on your computer, or a specified group on the target computer.
  You can use the variables listed in "Variables for computers" on page 401.

Message

The **Message** tab of the **Transfer File/Folder** dialog lets you send a message to target computers before the files or folders are transferred. A black diamond on the tab ◆ Message indicates that a message has been specified, even when you select another tab.

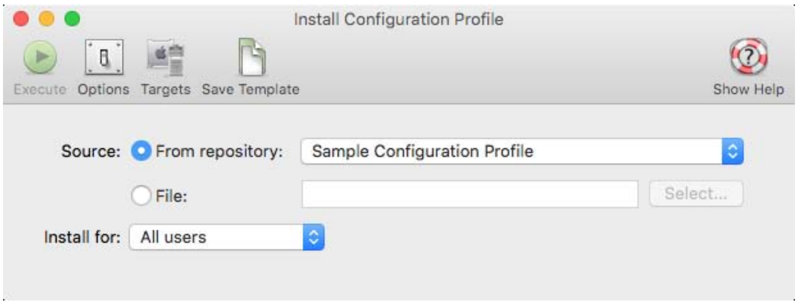
The elements of this pane are described in "Send Message" on page 415.

If a **Cancel** button is added to the dialog, the transfer will not take place to any target computer on which the user clicks **Cancel**.

Install Configuration Profile

Choosing this command displays the **Install Configuration Profile** dialog in which you can choose a configuration profile file to install on the selected computers.

Choosing the command opens the **Install Configuration Profile** window:



Source: ● From repository: Sample Configuration Profile

○ File:

Install for: All users

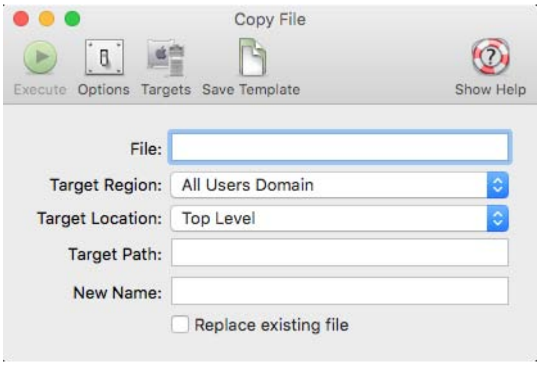
The dialog contains these elements:

- **From repository**: If this option is active, you can choose the configuration profile to install from the pop-up menu. The menu lists all applicable profiles that have been stored in LANrev, as described in “Creating or importing configuration profiles” on page 156.
- **File**: If this option is active, you can install a configuration profile that is available as a file on disk. You can drag a file into the field beside the option or click the **Select** button to choose a file.
- **Install for**: If the chosen profile is a user profile (as opposed to a device profile), you can choose from this menu the user or users for which the profile will be installed.

Copy File/Folder

The **Copy File/Folder** command copies files or folders on the target computers to another location on the same computers.

Choosing the command opens the **Copy File** dialog:



File:

Target Region: All Users Domain

Target Location: Top Level

Target Path:

New Name:

□ Replace existing file

The dialog contains these elements:

- **File**: The path of the file or folder that is to be copied. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
  To specify a file or folder manually, enter the entire path, with slashes as path dividers for macOS files and backslashes for Windows files.
  For files on Windows targets, you can use environment variables, as described in “Environment variables” on page 176.
- **Target Region**: On macOS target computers, the general domain to which the file or folder is to be copied. These target regions exist:
  - **System Domain**: /System and its subfolders
  - **All Users Domain**: /Library and its subfolders
  - **Current User Domain**: ~/ and its subfolders
  - **Classic Domain**: The Mac OS 9 system folder or one of its subfolders. (Requires the Classic environment to be configured on the target computer.)
  - **Network Domain**: The network resources folder defined by NetInfo and its subfolders.

  On Windows targets, only some domains are recognized:
  - **System Domain**: The operating system folder and its subfolders
  - **All Users Domain**: The **Users** folder (Vista and later) or **Documents and Settings** folder (XP and earlier) and their subfolders
  - **Current User Domain**: The current user’s folder and its subfolders

- **Target Location**: The specific location within the target region where the file or folder will be copied.

Location	macOS	Windows
Use Path Only	The target region is ignored and only the contents of the **Target Path** field is considered. (Using the contents as an absolute path.)	
Desktop	The desktop of the target computer.	
Top Level	The top level of the specified domain.	
Current User Folder	~/	Current user's folder (in Vista and later usually in **Users**, in XP and earlier usually in **Documents and Settings**)
Users	/Users	**Users** folder (Vista and later) or **Documents and Settings** folder (XP and earlier)
Applications	/Applications	**Program Files** folder
Documents	~/Documents	Current user's **My Documents** folder
Utilities	/Applications/ Utilities	n/a
Library	Library folder in the target region.	n/a
Frameworks	Library/ Frameworks folder in the target region.	n/a
Preferences	Library/ Preferences folder in the target region.	n/a
Preference Panes	Library/ PreferencePanes folder in the target region.	System directory for control panels (usually **c:\windows \system3**2)

Location	macOS	Windows
Kernel Extensions	Library/Extensions folder in the target region.	Active system folder (usually **c:\windows \system32**)
Fonts	Library/Fonts folder in the target region.	Windows fonts folder (usually **c:\windows\fonts**)
Scripting Additions	Library/Scripting-Additions folder in the target region.	n/a
Startup Items	Library/ StartupItems folder in the target region.	Startup program group
Applications Support	Library/Application Support folder in the target region.	Application Data folder
Contextual Menus	Library/Contextual Menu Items folder in the target region.	n/a

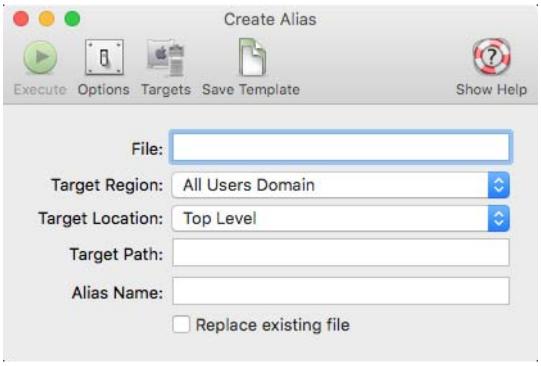
- **Target Path**: The path of a folder within the specified target location where the file or folder is to be copied (optional). When **Use Path Only** is chosen as the location, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Music for the user’s music folder.)
  For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in “Environment variables” on page 176.
- **New Name**: A name for the copied file or folder that is different from the original (optional).
- **Replace existing file**: If this option is checked, a file with the same name as the copied file or folder at the target location is replaced. If the option is unchecked, the copying process fails if a file with the same name already exists.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Create Alias

The **Create Alias** command creates an alias of the selected files or folders on the target computers in a specified location on the same computers. (On Windows targets, a shortcut is created.)

Choosing the command opens the **Create Alias** dialog:



File:

Target Region: All Users Domain

Target Location: Top Level

Target Path:

Alias Name:

□ Replace existing file

The dialog contains these elements:

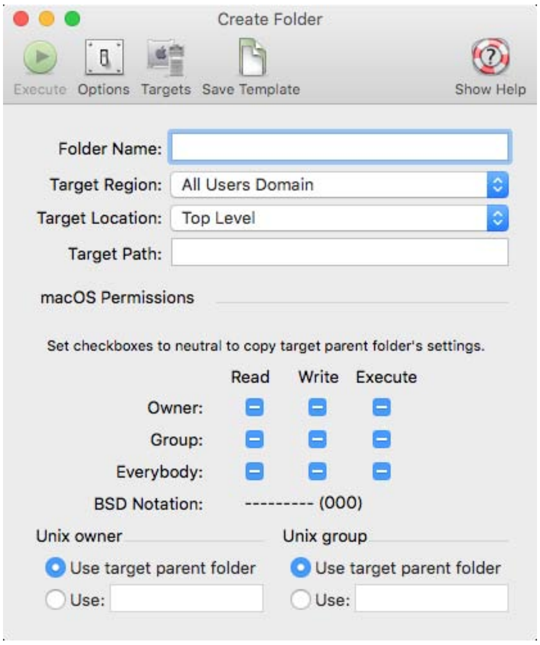
- **File**: The path of the file or folder from which an alias is to be created. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
  To specify a file or folder manually, enter the entire path, with slashes as path dividers for macOS files and backslashes for Windows files.
  For Windows targets, you can use environment variables, as described in "Environment variables" on page 176.
- **Target Region**: The general domain where the alias is to be created. The available regions are explained in "Copy File/ Folder" on page 441.
- **Target Location**: The specific location within the target region where the alias is to be created. The available locations are explained in "Copy File/Folder" on page 441.
- **Target Path**: The path of a folder within the specified target location where the alias is to be created (optional).
  When **Use Path** Only is chosen as the location, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Music for the user's music folder.)
  For Windows targets, you can use environment variables, as described in "Environment variables" on page 176.
- **New Name**: A name for the alias that is different from the default name (optional).
- **Replace existing file**: If this option is checked, a file with the same name as the alias at the target location is replaced. If the option is unchecked, the process fails if a file with the same name already exists.

The toolbar of command windows is described in "Command window toolbar" on page 402.

Create Folder

The **Create Folder** command creates a folder on the target computers in a specified location.

Choosing the command opens the **Create Folder** dialog:



Folder Name:

Target Region: All Users Domain

Target Location: Top Level

Target Path:

macOS Permissions

Set checkboxes to neutral to copy target parent folder's settings.

	Read	Write	Execute
Owner:	⊟	⊟	⊟
Group:	⊟	⊟	⊟
Everybody:	⊟	⊟	⊟

BSD Notation: --------- (000)

Unix owner

● Use target parent folder

○ Use:

Unix group

● Use target parent folder

○ Use:

The dialog contains these elements:

- **Folder Name**: The desired name of the folder.
- **Target Region**: The general domain where the folder is to be created. The available regions are explained in “Copy File/ Folder” on page 441.
- **Target Location**: The specific location within the target region where the folder is to be created. The available locations are explained in “Copy File/Folder” on page 441.
- **Target Path**: The path of a folder within the specified target location within which the folder is to be created (optional). Use slashes as path dividers for macOS targets and backslashes for Windows targets.
  Note: This is not the path of the folder that is to be created but the path of its parent folder.
  When **Use Path Only** is chosen as the location, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Music for the user’s music folder.)
  For Windows targets, you can use environment variables when **Use Path Only** is chosen, as described in “Environment variables” on page 176.
- **macOS Permissions**: When creating folders on macOS target computers, you can specify its permissions:
  ☑ This permission is set for the folder.
  ⊟ This permission is set to the same value for the folder as for the parent folder.
  □ This permission is not set for the folder.
  The permissions are displayed in standard BSD notation below the array for easy verification.

- **Unix owner**: When a folder is created on a macOS target, its owner can be set. The owner can either be the owner of the parent folder or a specified user of the target computer.
- **Unix group**: When a folder is created on a macOS target, its group can be set. The group can either be the group of the parent folder or a specified group on the target computer.

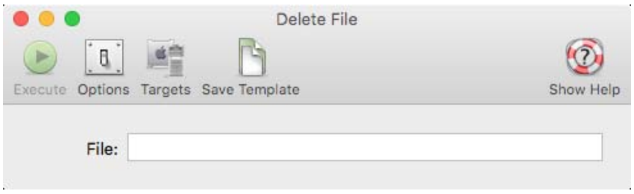
The toolbar of command windows is described in “Command window toolbar” on page 402.

Delete File/Folder

The **Delete File/Folder** removes a file or folder from the target computers.

IMPORTANT Once executed, this command is not reversible. The selected files and folders are not put into the trash but removed completely. They cannot be recovered, short of using specialized tools or from a backup.

Choosing the command opens the **Delete File** dialog:



File:

The dialog contains these elements:

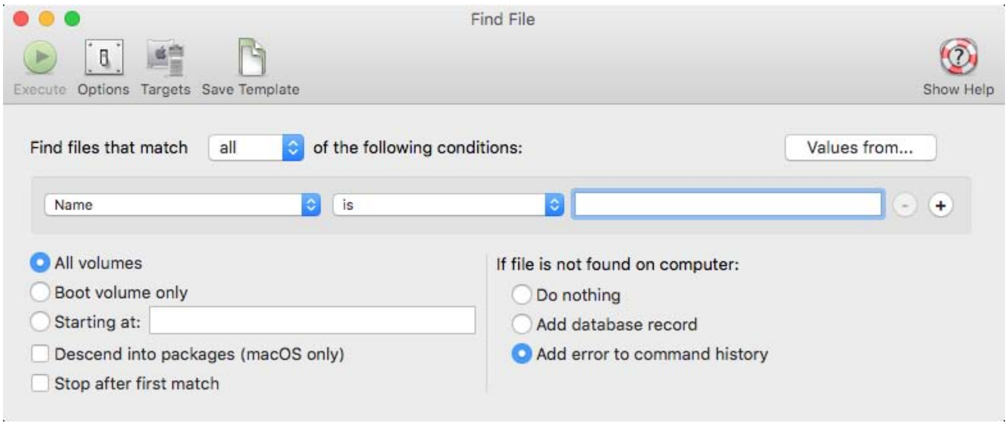
- **File**: The path of the file or folder that is to be deleted. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
  To specify a file or folder manually, enter the entire path, with slashes as path dividers for macOS files and backslashes for Windows files.
  For Windows targets, you can use environment variables, as described in “Environment variables” on page 176.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Find File

The **Find File** command searches target computers for files and enters found files into the Files table of the LANrev database.

Choosing the command opens the **Find File** dialog:



Find files that match all of the following conditions:

Name is

● All volumes
○ Boot volume only
○ Starting at:
□ Descend into packages (macOS only)
□ Stop after first match

If file is not found on computer:
○ Do nothing
○ Add database record
● Add error to command history

The dialog contains these elements:

- **Find files that match**: When **all** is chosen from this pop-up menu, files are found that match all specified conditions (Boolean AND). If **any** is chosen, files are found that match at least one of the specified conditions (Boolean OR).
- **Values from**: Clicking this button lets you select a file. All specified conditions are filled with the respective parameters from this file. If you later add new conditions, they initially also contain comparison values from this file.
- Condition area: The first pop-up menu lets you choose a condition to match files. The second one contains the possible comparison operators. For most conditions, a text field lets you specify the value to compare files against. The **+** and **–** buttons let you add new conditions or remove existing ones.
  The parameters available for specifying conditions are described in “Files” on page 867, except for **Checksum** and **Path**:
  - **Checksum** lets you select files by their MD5 checksums, making sure that files are really the desired version, without alterations. Note that the checksum has to be calculated dynamically; doing so for a large number of files requires a huge amount of processing power on the client computer and should therefore be avoided. Always combine the **Checksum** criterion with other criteria that make sure that the checksum needs to be calculated only for a small number of files.
    Checksums are not available for folders.
  - **Path** lets you select files and folders by their paths on the hard disk. It references the **File Path** information item. When this option is chosen, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Documents for the user’s documents folder.)
    For Windows targets, you can use the environment variables when this option is chosen, as described in “Environment variables” on page 176.
- **All volumes**: All volumes of the target computers are searched.

- **Boot volume only**: Only the boot volumes of the target computers are searched.
- **Starting at**: Only the directory specified in the text field and its subdirectories are searched.
  You can use macOS' ~/ notation for the user folder and Windows' environment variables as described above for the **Path** criterion.
- **Descend into packages**: If this option is checked, the contents of packages on macOS target computers are included in the search. If it is unchecked, the packages are treated as files and their contents are not searched.
- **Stop after first match**: If a matching file has been found on a target computer, the search is stopped on that computer.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Move File/Folder

The **Move File/Folder** command moves files or folders on the target computers to another location on the same computers.

The command is similar in all respects to the **Copy File/Folder** command (see “Copy File/Folder” on page 441), except that files and folders are moved instead of copied.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Open File

The **Open File** command opens a file on the target computers. The effect is the same as if the file had been double-clicked locally.

The file to be opened must already be present on each target computer. (Compare “Transfer File/Folder” on page 438.)

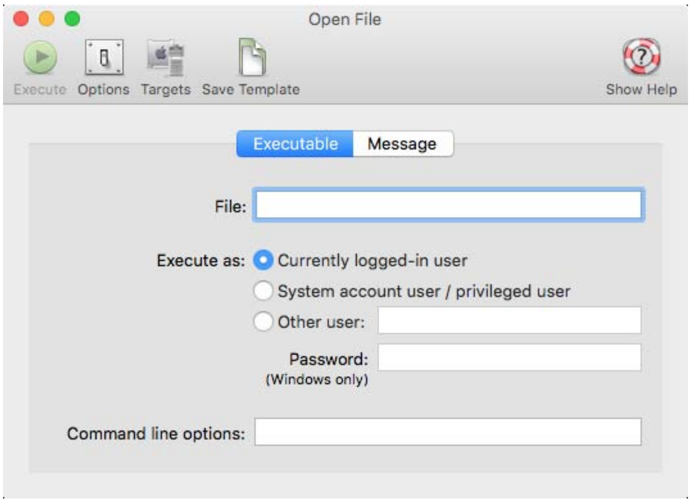
Choosing the command opens the **Open File** dialog, which has two tabs:

- **Executable**
- **Message**

The toolbar of command windows is described in “Command window toolbar” on page 402.

Executable

The **Executable** tab of the **Open File** dialog lets you specify the file to open:



File:

Execute as: ● Currently logged-in user
○ System account user / privileged user
○ Other user:
Password:
(Windows only)

Command line options:

The tab contains these elements:

- **File**: The location of the file on the target computers. If a file is selected in a browser window when you open this command, that files location is pre-entered. If you select more than one file, only the number of files is shown.
  On Windows targets, the PATH variable is automatically evaluated, allowing you to specify just the filename instead of the full path as long as the file is located in a directory that is included in PATH.
  You can use other environment variables as well, as described in "Environment variables" on page 176.
- **Currently logged-in user**: The file is opened with the privileges of the current user of the target computer.
- **System account / privileged user**: The file is opened with the privileges of an administrator account.
- **Other user**: The file is opened as if executed by the specified user. For Windows target computers, the password of the user account must also be specified.
  For Windows clients in networks with domains, the username must be specified as **domain\username**.
- **Command line options**: Any command-line options you specify here apply only if application files are opened.
  You can use shell variables in the options, as described in "Environment variables" on page 176.

Message

The **Message** tab of the **Open File** dialog lets you send a message to target computers before the file is opened.

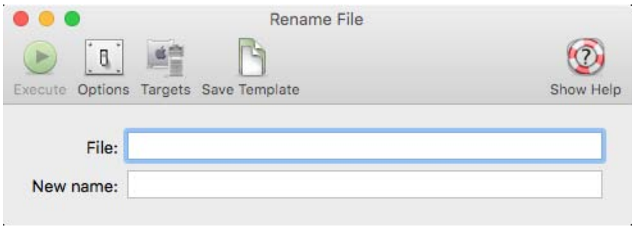
The elements of this pane are described in "Send Message" on page 415.

If a **Cancel** button is added to the dialog, the file will not be opened on any target computer on which the user clicks **Cancel**.

Rename File/Folder

The **Rename File/Folder** command changes the name of files or folders on target computers.

Choosing the command opens the **Rename File** dialog:



File:

New name:

The dialog contains these elements:

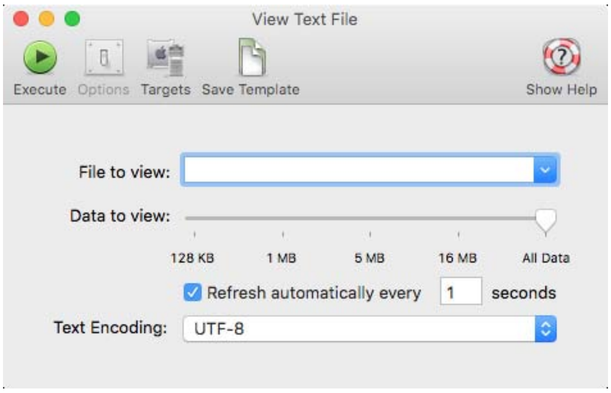
- **File**: The path of the file or folder that is to be deleted. If you select a file or folder before choosing the command, its path is pre-entered. If you select more than one file or folder, only the number of objects is shown.
  To specify a file or folder manually, enter the entire path, with slashes as path dividers for macOS files and backslashes for Windows files.
  For Windows targets, you can use environment variables, as described in “Environment variables” on page 176.
- **New name**: The new name of the selected files or folders, without the path.

The toolbar of command windows is described in “Command window toolbar” on page 402.

View Text File

The **View Text File** command displays the contents of files on remote computers – either text files or system log files – on your monitor.

Choosing the command opens the **View Text File** dialog:



File to view:

Data to view: All Data

☑ Refresh automatically every 1 seconds

Text Encoding: UTF-8

The dialog contains these elements:

- **File to view**: The file that you want to display. You specify the file in any of these ways:
  - Enter the complete path of the file on the computer, including the file’s name and extension (if any).
    For Windows targets, you can use environment variables, as described in “Environment variables” on page 176.
    When a file has been selected in a LANrev browser window before the **View Text File** command is chosen, that file’s path is pre-entered into the **File to view** field.
  - Choose one of the predefined files from the pop-up menu.
- **Data to view**: Specify how much of the file’s data LANrev is to display.
  You may not want to transmit very large files in their entirety across the network. In that case, you can limit the amount LANrev displays (and thus has to transmit). LANrev displays the amount of data you specify from the end of the file.
- **Refresh**: If this option is checked, LANrev automatically continues to fetch the contents of the file in the specified interval.
  Note: Fetching large files in short intervals can create significant network loads.
- **Text encoding**: The text encoding system used for the file.

Executing the command opens the specified file on all target computers. If more than one target computer was chosen, LANrev Admin opens multiple windows, one for each target computer.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Gather Process Information

The **Gather Process Information** command makes LANrev Server collect from all target computers information on currently running processes and enter it into the Processes table of its database.

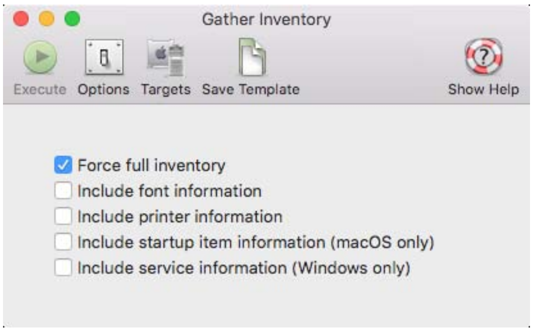
There are no options for this command; neither is there feedback after its execution.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Gather Inventory Information

The **Gather Inventory Information** command makes LANrev Server collect from all target computers information on all of its hardware and software-related information items and enter it into the Computers table of its database.

Choosing the command opens the **Gather Inventory** dialog:



☑ Force full inventory
□ Include font information
□ Include printer information
□ Include startup item information (macOS only)
□ Include service information (Windows only)

The dialog contains these elements:

- **Force full inventory**: If this option is checked, the server gets from the agents on the target computers all inventory information. If the option is unchecked, only information that has changed since the last transmission is transmitted to the server.
- **Include font information**: If this option is checked, font information is gathered from the target computers. If the option is unchecked, no font information is gathered.
- **Include printer information**: If this option is checked, information on printers is gathered from the target computers. If the option is unchecked, no printer information is gathered.
- **Include startup item information**: If this option is checked, information on startup items is gathered from the target macOS computers. If the option is unchecked, no startup item information is gathered.
- **Include service information**: If this option is checked, information on active services is gathered from the target Windows computers. If the option is unchecked, no services information is gathered.

NOTE The information collected by this command is also collected automatically through regular inventory scans. Use this command when you would like to check the status on some computers immediately or more frequently than allowed for by the inventory push interval set through the **Agent Settings** command.

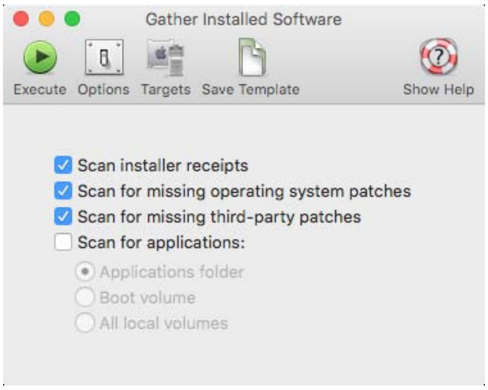
The toolbar of command windows is described in “Command window toolbar” on page 402.

Inventory information can also be gathered automatically by adding an action to a computer group. See “Working with actions” on page 178 for details.

Gather Installed Software

The **Gather Installed Software** command makes LANrev Server collect from all target computers information on the software installed on these computers and enter it into the Installed Software table of its database.

Choosing the command opens the **Gather Installed Software** dialog:



☑ Scan installer receipts
☑ Scan for missing operating system patches
☑ Scan for missing third-party patches
□ Scan for applications:
● Applications folder
○ Boot volume
○ All local volumes

The dialog contains these elements:

- **Scan installer receipts**: If this option is checked, LANrev scans target computers for installed software by looking for installer receipts. If it is unchecked, all installed software that was found through installer receipts is deleted from the Installed Software table in the LANrev database.
- **Scan for missing operating system patches**: If this option is checked, LANrev scans target computers for operating system patches. The Agent queries the operating system for any applicable patches that are available but not yet installed and reports them back. (Patches that were rejected by an administrator are not considered to be missing.) The results can be viewed in the **Missing Patches** window.
  Only computers for which **Include in OS patch management** has been checked in the **Agent Settings** dialog are scanned.
  Note: Patches that have been rejected by you or another administrator are not reported as missing.
- **Scan for missing third-party patches**: If this option is checked, LANrev scans target computers for third-party patches that are present in the Software Distribution Center and would apply to the target computers but are not installed on them. (Patches that were rejected by an administrator are not considered to be missing.) The results can be viewed in the **Missing Patches** window.
- **Scan for application**: If this option is checked, LANrev scans target computers for installed software by looking for applications in the specified locations and their subfolders.
  - **Applications folder**: the **Applications** folders (on macOS targets) or the **Program Files** folders (on Windows targets; folder chosen according to the local environment variable settings)
  - **Boot volume**: the entire startup volume

- **All local volumes**: all volumes currently mounted on the target computer, except server volumes

Note: Scanning entire hard disks can create a huge amount of data. We recommend scanning the boot volume or all local volumes only when really required.

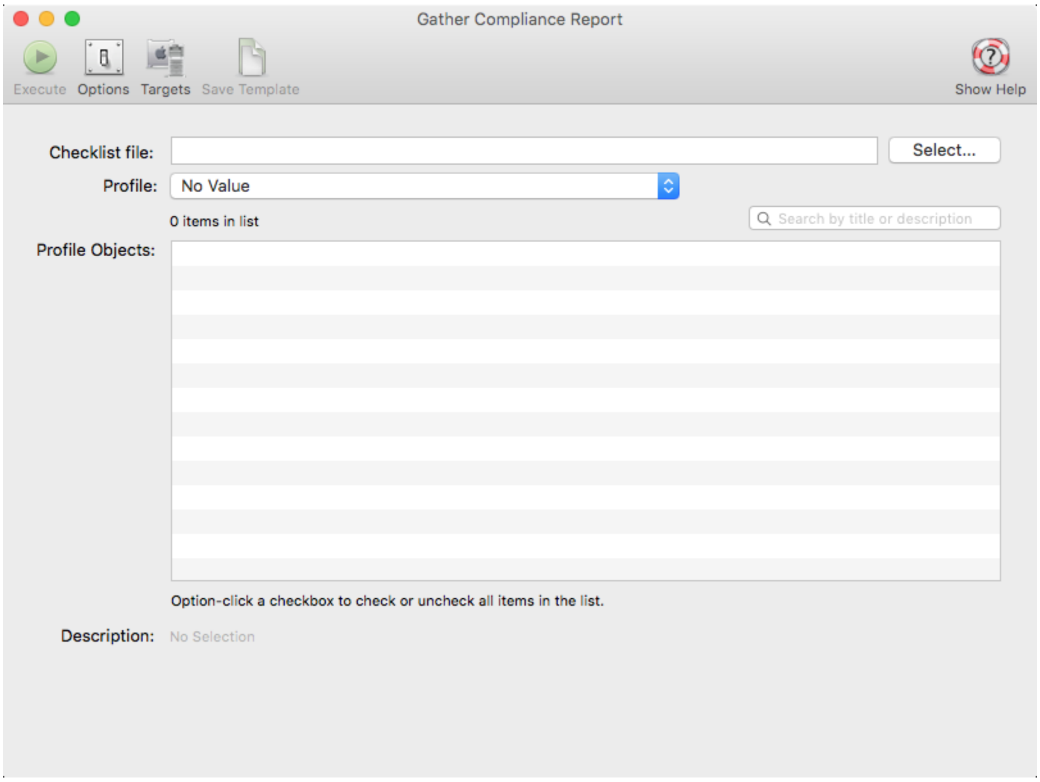
If the **Scan for application** option is unchecked, all installed software that was found through searching the application folders is deleted from the Installed Software table in the LANrev database.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Gather Compliance Report

The **Gather Compliance Report** command makes LANrev Server collect from all Windows target computers information required for FCCP SCAP compliance reports on these computers and enter it into the Compliance Report table of its database.

Choosing the command opens the **Gather Compliance Report** dialog:



Checklist file:

Profile: No Value

0 items in list

Profile Objects:

Option-click a checkbox to check or uncheck all items in the list.

Description: No Selection

The dialog contains these elements:

- **Checklist file**: This is the USGCB file containing the report parameters, an XML file the name of which usually contains “xccdf”. Clicking the **Select** button lets you choose a file from your hard disk.

- **Profile**: This pop-up menu lets you choose the desired profile from the profiles contained in the chosen file.
- **Profile Objects**: This list contains the individual options contained in the chosen profile. You can switch them off and on individually. Using the context menu commands, you can also switch on or off multiple selected items together. Entering text in the search field above the list restricts the list to display just the objects containing that text.
  Description: The description of the selected object.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Run Software Distribution Check

The **Run Software Distribution Check** causes LANrev Server to check the status of software distribution on the selected target computers. There are no options for this command.

NOTE This check also happens automatically in regular intervals. Use this command when you would like the status to be checked immediately on some computers or more frequently than allowed for by the package check interval set through the **Agent Settings** command.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Run License Monitoring Scan

The **Run License Monitoring Check** causes LANrev Server to check for licensed software on the selected target computers. There are no command-specific options.

NOTE The information collected by this command is also collected automatically through regular license monitoring scans. Use this command when you would like to check the status on some computers immediately or more frequently than allowed for by the license monitoring scan interval set through the **Agent Settings** command.

The toolbar of command windows is described in “Command window toolbar” on page 402.

Execute Command

The **Execute Command** command executes the command in the frontmost window with the current settings. The effect is the same as clicking the **Execute** button.

Execute Command is available only if a command window is the frontmost window.

Command Options

The **Command Options** command lets you change the options for a command.

Command Options is available only if the **Commands** window or a command window is the frontmost window.

Choosing the command opens the **Command Options** dialog described in “Options” on page 403.

Execute Command Now

The **Execute Command Now** command executes the selected command immediately, overriding its scheduling options. A confirmation alert is displayed before the actual execution takes place.

Execute Command Now is available only if the **Commands** window is the frontmost window and a queued (i.e, scheduled or deferred) command is selected.

Edit Command

The **Edit Command** command lets you change the settings for a command in the command queue.

Edit Command is available only if the **Commands** window is the frontmost window and a queued (i.e, scheduled or deferred) command is selected.

Choosing **Edit Command** displays a message asking you to choose between editing the command setting only for the selected target or for all targets for which the command was originally given.

When you have made your choice, the original command dialog will be opened, displaying the current settings. The target list contains all or one of the original targets, as per your choice.

After you have modified the command settings as desired, clicking the **Execute** button executes the command or re-enters it into the command queue in its edited form, depending on the scheduling options you have specified.

Reapply Command

The **Reapply Command** command lets you execute a command again that has already been executed, successfully or failing. You can change the command settings before re-executing the command.

Reapply Command is available only if the **Commands** window is the frontmost window.

Using **Reapply Command** is similar to using **Edit Command**, described above.

Show/Hide Target List

The **Show/Hide Target List** command toggles the target list of a command between visible and hidden. Choosing the command has the same effect as clicking the **Targets** button in a command window.

The target list is explained in “Command window toolbar” on page 402.

Show/Hide Target List is available only if a command window is the frontmost window.

Variables for mobile devices

LANrev supports a range of variables that you can use in commands and similar circumstances when specifying text that is sent to or displayed on the device (such as the body of an e-mail). This is described in “Information variables” on page 175.

To use a variable in a text field, enclose it in curly brackets and prefix a dollar sign, for example, `${MDU_Company}`.

For mobile devices, you can use all variables listed below. In addition, you can use any custom information fields for mobile devices that you have given a variable name. (See “Defining custom information fields” on page 108 for more information.)

Predefined variables for mobile devices

- Server-related variables:
  - MDMServerAddress (The DNS name or IP address, for example, mdmserver.mycompany.com.)
  - MDMServerPort (The port over which the MDM server communicates, for example, 443.)
  - MDMServerURL (The URL of the MDM server, for example, https://mdmserver.mycompany.com.)
- Device-related variables:

  - MD_CurrentCarrierNetwork (Mobile Device Current Carrier Network)
  - MD_DeviceModel (Mobile Device Model)
  - MD_DeviceName (Mobile Device Name)
  - MD_HomeCarrierNetwork (Mobile Device Home Network)
  - MD_IMEI (Mobile Device IMEI)
  - MD_UDID (Mobile Device Identifier (UDID))
  - MD_PhoneNumber (Mobile Device Phone Number)
  - MD_SerialNumber (Mobile Device Serial Number)
  - MD_LastMDMHeartbeat (Mobile Device Last Contact)
  - MD_IPAddress (Mobile Device Public IP Address)
  - MD_CellIPAddress (Mobile Device Cell IP Address)
  - MD_WifiIPAddress (Mobile Device WiFi IP Address)
  - MD_WifiMACAddress (Mobile Device WiFi MAC Address)
  - MD_WifiNetwork (Mobile Device WiFi Network)
  - MD_Model (Mobile Device Model Number)
  - MD_OSVersion (Mobile Device OS Version)
  - MD_IsJailbroken (Mobile Device Jailbroken)
  - MD_PasscodePresent (Mobile Device Passcode Present)
  - MD_IsRoaming (Mobile Device Is Roaming)
  - MD_DataRoamingEnabled (Mobile Device Data Roaming Enabled)
  - MD_VoiceRoamingEnabled (Mobile Device Voice Roaming Enabled)
- User-related variables:
  - MDU_FirstName (Device User First Name)
  - MDU_LastName (Device User Last Name)
  - MDU_LogOnName (Device User Log-on Name)
  - MDU_DisplayName (Device User Display Name)
  - MDU_EnrollmentUsername (Device User Enrollment Username)
  - MDU_EnrollmentDomain (Device User Enrollment Domain)
  - MDU_PhoneNumber (Device User Phone Number)
  - MDU_EMail (Device User E-Mail)
  - MDU_OrganizationalUnitPath(Device User Organizational Unit Path)
  - MDU_OrganizationalUnit(Device User Organizational Unit)
  - MDU_IsMemberOf (Device User Is Member Of)
  - MDU_Department (Device User Department)
  - MDU_Office (Device User Office)
  - MDU_Company (Device User Company)
  - MDU_Street (Device User Street)
  - MDU_City (Device User City)
  - MDU_State (Device User State)
  - MDU_Country (Device User Country)
  - MDU_ZIPCode (Device User ZIP Code)

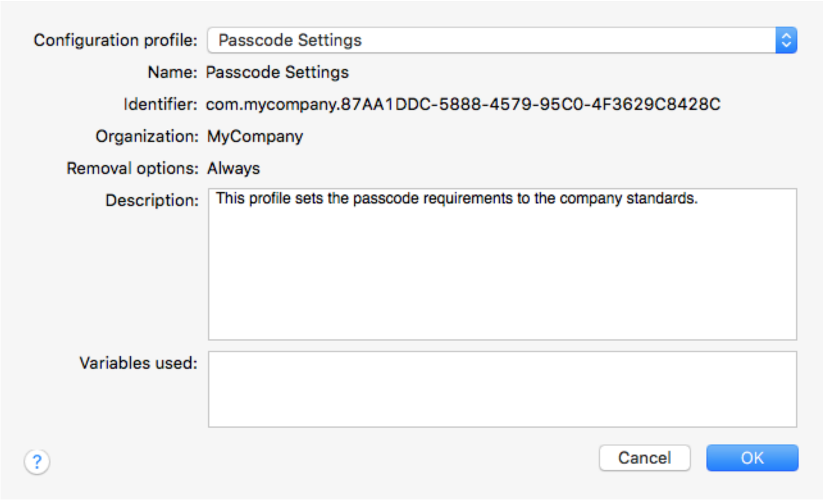
Install Configuration Profile

Choosing this command displays the **Install Configuration Profile** dialog in which you can choose a configuration profile file to install on the selected devices.

When a shared device is selected, pressing the Option key while choosing the command causes the selected profile to be installed only for the currently logged-in user of the device.

The effect of the command is slightly different, depending on the platform of the selected devices:

- For iOS and Android devices, the profile is added to the profiles already installed on the device (if any).
- For Windows Phone devices, the selected profile replaces the current EAS policy on the device.



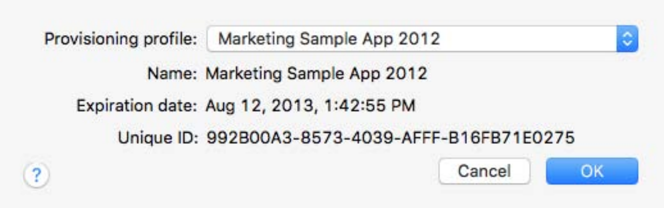
Configuration profile: Passcode Settings
Name: Passcode Settings
Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C
Organization: MyCompany
Removal options: Always
Description: This profile sets the passcode requirements to the company standards.
Variables used:

The dialog contains these elements:

- **Configuration profile**: The configuration profile you want to install. The pop-up menu contains all profiles that are available in LANrev.
  You can choose **Other** from this menu to open a configuration profile file that has not yet been imported into LANrev.
- **Name**: The name of the profile.
- **Identifier**: The identifier of the profile.
- **Organization**: The organization of the profile.
- **Removal options**: Whether the local user of the mobile device can remove the profile and whether a passcode is required for doing so.
- **Description**: A description of the profile. This description is displayed to the user of the managed mobile device. You can edit it before assigning the profile.

Install Provisioning Profile

Choosing this command displays the **Install Provisioning Profile** dialog in which you can choose a provisioning profile file to install on the selected iOS devices. (Provisioning profiles are not supported for Android and Windows Phone devices.)



Provisioning profile: Marketing Sample App 2012

Name: Marketing Sample App 2012

Expiration date: Aug 12, 2013, 1:42:55 PM

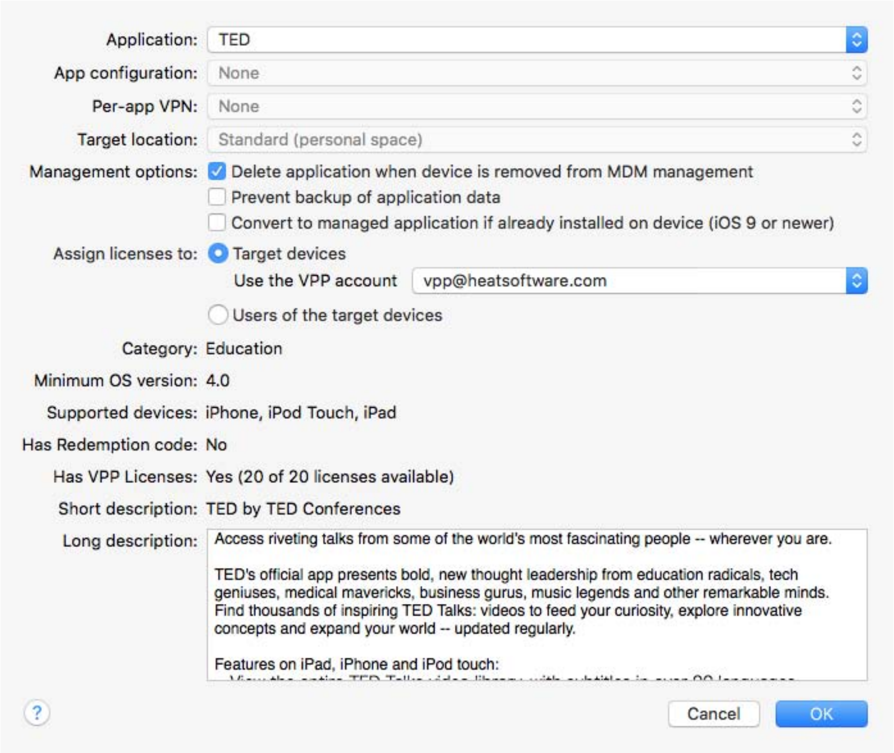
Unique ID: 992B00A3-8573-4039-AFFF-B16FB71E0275

The dialog contains these elements:

- **Provisioning profile**: The provisioning profile you want to install. The pop-up menu contains all profiles that are available in LANrev.
  You can choose **Other** from this menu to open a provisioning profile file that has not yet been imported into LANrev.
- **Name**: The name of the profile.
- **Expiration date**: The date on which the provisioning profile becomes invalid.
- **Unique ID**: The globally unique identifier for the profile.

Install Application

Choosing this command displays the **Install Application** dialog in which you can choose an enterprise or app store app to install on the selected iOS or Android devices. (Installing applications on Windows Phone devices is not supported.)



Application: TED

App configuration: None

Per-app VPN: None

Target location: Standard (personal space)

Management options: ☑ Delete application when device is removed from MDM management
□ Prevent backup of application data
□ Convert to managed application if already installed on device (iOS 9 or newer)

Assign licenses to: ● Target devices
Use the VPP account vpp@heatsoftware.com
○ Users of the target devices

Category: Education

Minimum OS version: 4.0

Supported devices: iPhone, iPod Touch, iPad

Has Redemption code: No

Has VPP Licenses: Yes (20 of 20 licenses available)

Short description: TED by TED Conferences

Long description: Access riveting talks from some of the world's most fascinating people -- wherever you are.

TED's official app presents bold, new thought leadership from education radicals, tech geniuses, medical mavericks, business gurus, music legends and other remarkable minds. Find thousands of inspiring TED Talks: videos to feed your curiosity, explore innovative concepts and expand your world -- updated regularly.

Features on iPad, iPhone and iPod touch:

The dialog contains these elements:

- **Application**: The app you want to install. The pop-up menu contains all apps for the operating system of the selected devices that are available in LANrev.
- **App configuration**: The configuration profile you want to apply to the app you install. The pop-up menu lists all profiles that are available for the app (if any).
  For more information about app configuration profiles, see "Working with configuration profiles" on page 181.
- **Per-app VPN**: The VPN configuration profile that you want to assign to the app you install. The pop-up menu lists all per-app VPN configuration profiles that are available in LANrev (if any). Per-app VPN configuration profiles can be created with the configuration profile editor by choosing to create an iOS profile.
- **Target location**: Whether this application is installed in the standard location or a special one:
  - **Standard (personal space)**: The application is installed in the usual location on the device.
  - **KNOX workspace**: The application is installed in the KNOX workspace on the device. This option is supported only for installing Android applications on Android devices on which KNOX is active.
- **Management options**: Choose whether and how the application is put under management on this device:
  - **Delete application when device is removed from MDM management**: If this option is checked, the application is removed from the device when the device is no longer under MDM management.
    This option is available only for iOS devices.
  - **Prevent backup of application data**: If this option is checked, the local data of the application on device cannot be backed up to iTunes or iCloud.
    This option is available only for iOS devices.
  - **Convert to managed application if already installed on device**: If this option is checked, any unmanaged copy of the application that is already present on the device is converted into a managed application.
    This option is available only for devices running iOS 9 and up.
- **Assign licenses to**: When installing compatible applications, you can choose whether to install the licenses to the devices or the users of the devices:
  - **Target devices**: If this option is chosen, the license is assigned to the selected devices. Choose the VPP account from which the license is to be taken.
    This option is available only for devices running iOS 9 and up, and only for compatible applications.
  - **Users of target devices**: If this option is chosen, the license is assigned to the users of the selected devices.
- **Bundle identifier**: The bundle identifier of the chosen application.
- **Version**: The version of the chosen application.
- **Build number**: The build number of the chosen application.

- **Minimum OS version**: The minimum version of the mobile OS required by the chosen application.
- **Supported devices**: The types of device on which the app can be used.
  This information is displayed only for iOS devices.
- **Short description**: The short description of the application that it was given when it was imported into LANrev.
- **Long description**: The long description of the application that it was given when it was imported into LANrev.

Clicking **OK** in this dialog transfers the app to the selected mobile devices upon the next contact and presents their users with a prompt to install the app. If a user declines, the app is not installed on that device.

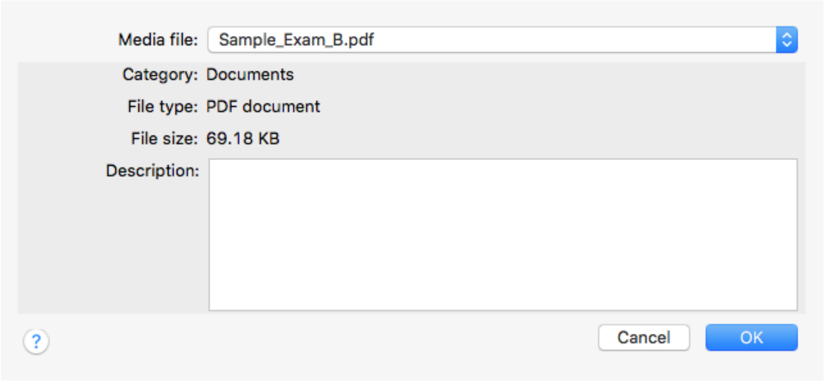
Note that you cannot install an application on device running an iOS version prior to 9.0 when the device already contains an unmanaged version of the application. (Unmanaged applications are all applications that have been installed by other means than through the MDM system.)

Install Media File

Choosing this command displays the **Install Media File** dialog through which you can install media files on managed devices.

You can install PDF, ePub, and iBooks files that have been imported into LANrev as well as files from the iBooks Store. These files can be installed on managed iOS devices running iOS 8 and above.

Imported file that are configured so that they may not leave LANrev Safe cannot be installed with this command.



Media file: Sample_Exam_B.pdf
Category: Documents
File type: PDF document
File size: 69.18 KB
Description:

The dialog contains these elements:

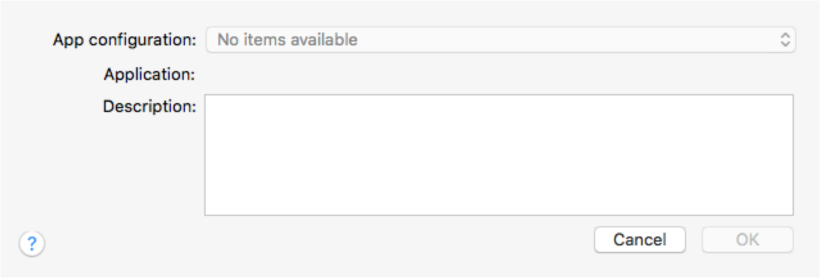
- **Media file**: The file you want to install. The pop-up menu contains all files that are available for installation.
- **Category**: The category to which the selected file was assigned when it was imported into LANrev.
- **File type**: The file type of the selected file.
- **File size**: The size of the selected file on disk.

- **Description**: The description of the file that it was given when it was imported into LANrev.

Clicking **OK** in this dialog transfers the file to the selected mobile devices upon the next contact.

Change Application Configuration

Choosing this command displays the **Change Application Configuration** dialog in which you can apply an app-specific configuration profile to selected devices running iOS 7.0 and up:


App configuration: No items available

Application:

Description:

The dialog contains these elements:

- **App configuration**: This pop-up menu lists all app-specific configuration profiles available in LANrev.
- **Application**: The application to which the selected profile applies
- **Description**: The description of the selected profile, as stored in the profile.

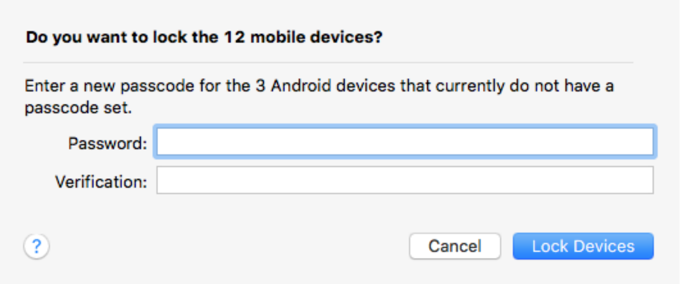
Clicking **OK** in this dialog applies the selected configuration profile to the appropriate app (shown in the application field) on the selected devices. If a profile is already applied to the app on any of the devices, it is replaced by the selected profile.

Issue Device Lock

Choosing this command locks the selected devices as if they had been switched off. Unlocking them requires entering the passcode locally (assuming that a passcode has been set on the device).

The device is locked as soon as it next contacts the mobile OS vendor’s notification server.

A confirmation dialog is displayed before the command is executed. If any of the devices does not currently have a passcode, you are prompted to provide a passcode for it:



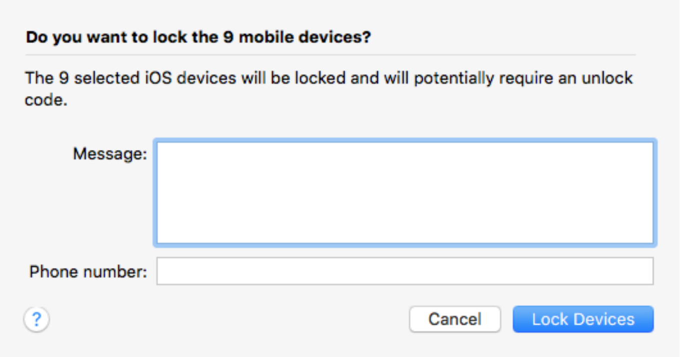
Do you want to lock the 12 mobile devices?

Enter a new passcode for the 3 Android devices that currently do not have a passcode set.

Password:

Verification:

For devices running iOS 7 and up, you can also specify a message and a phone number, which are displayed on the lock screen:



Do you want to lock the 9 mobile devices?

The 9 selected iOS devices will be locked and will potentially require an unlock code.

Message:

Phone number:

In the message text, you can use the variables described in “Variables for mobile devices” on page 458.

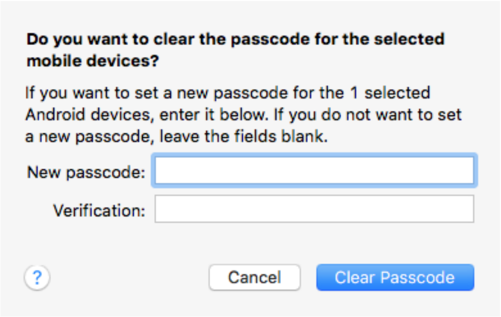
If you have selected both Android devices without a passcode and devices running iOS 7 and up, a combination of both dialogs is shown.

This command does not apply to Windows Phone devices.

Issue Clear Passcode

Choosing this command removes any passcode on the device so that it can be accessed without authentication and optionally lets you set a new passcode.

Choosing the command opens the **Clear Passcode** dialog:



Do you want to clear the passcode for the selected mobile devices?

If you want to set a new passcode for the 1 selected Android devices, enter it below. If you do not want to set a new passcode, leave the fields blank.

New passcode:

Verification:

The dialog contains these elements:

- **New passcode**: The new passcode that you want to set on the device after clearing the current one. Leave this field empty to not specify a new passcode.
  Setting a new passcode is possible only on Android devices.
- **Verification**: Repeat the passcode to guard against typos.

Clicking **Clear Passcode** removes the passcode as soon as the device next contacts the mobile OS vendor's notification server. The new passcode, if any, depends on several factors:

- If you have specified a new passcode, that new passcode is set on the device.
- If the configuration profile on the device specifies that a passcode is required, the user immediately has to create a new passcode.
- If neither is the case, the device is left without a passcode.

This command does not apply to Windows Phone devices.

Issue Clear Restrictions Passcode

Choosing this command removes any passcode set on the device for accessing restricted features. The command has no effect on the passcode to access the device itself.

Clicking **Remove Passcode** removes the passcode as soon as the device next contacts the mobile OS vendor's notification server.

This command applies only to iOS devices running iOS 8 or above.

Erase Device

Choosing this command erases all information on the selected mobile devices and returns them to their factory settings.

A confirmation dialog is displayed before the command is executed. For devices with SD cards, it gives you the choice of erasing just the internal storage or the SD card as well.

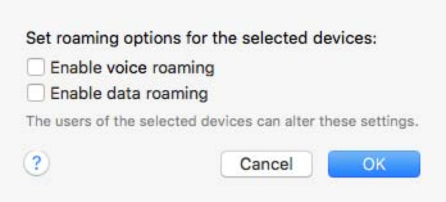
When activation locking is enabled on the device, you can enter the activation lock bypass code to remove the lock before erasing the device.

The device is erased as soon as it next contacts the mobile OS vendor’s notification server.

IMPORTANT Note that this action is not reversible and that the erased information cannot be recovered from the mobile device (although recovering the data from a backup, should one exist, might be possible). Erasing devices without the consent of their users may expose you to legal liability.
The erased device can no longer be administered through LANrev until it has been enrolled again.

Set Roaming Options

Choosing this command opens the **Set Roaming Options** dialog in which you can activate and deactivate voice and data roaming for selected mobile devices:



Set roaming options for the selected devices:

□ Enable voice roaming

□ Enable data roaming

The users of the selected devices can alter these settings.

The dialog contains these elements:

- **Enable voice roaming**: If this option is checked, voice roaming will be enabled on the mobile device. If it is unchecked, voice roaming will be disabled. (If it is in the third state, no change will be made.)
  Note that some mobile communications companies prevent access to this setting. If that is the case for the selected devices, this option is disabled.
- **Enable data roaming**: If this option is checked, data roaming will be enabled on the mobile devices. If it is unchecked, voice roaming will be disabled. (If it is in the third state, no change will be made.)

Note that local users of the mobile devices will still be able to change the settings you make in this dialog.

Roaming options can only be set for iOS devices running iOS 5 or newer.

Send Message to Device

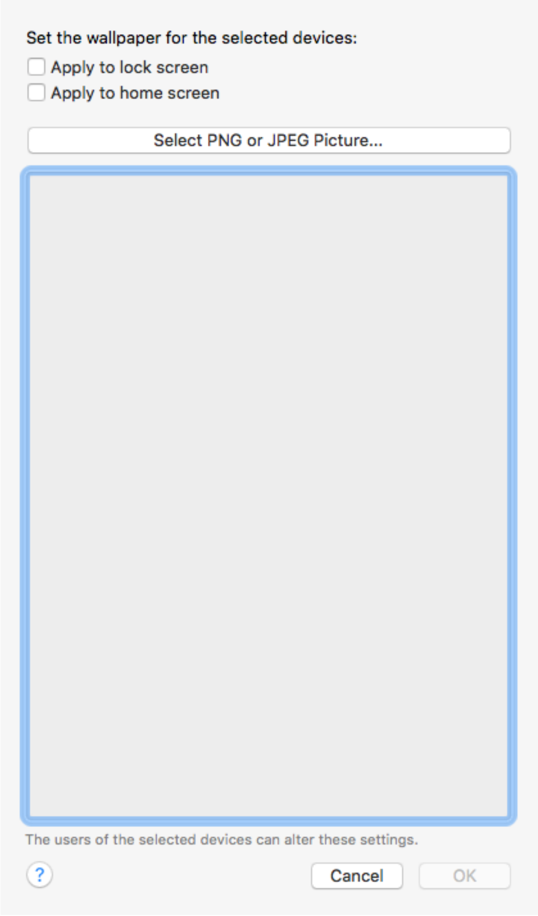
Choosing this command lets you send a message to all selected mobile devices, provided that the LANrev Apps application is installed on them. (This command does not support Windows Phone devices.)

The message is sent as soon as the device next contacts the mobile OS vendor's notification server.

Set Wallpaper

Choosing this command lets you set the wallpaper for the selected supervised devices running iOS 7.1 or later.

Choosing the command displays the **Set Wallpaper** dialog:



Set the wallpaper for the selected devices:

□ Apply to lock screen

□ Apply to home screen

The users of the selected devices can alter these settings.

The dialog contains these elements:

- **Apply to lock screen**: If this option is checked, the selected devices display the chosen image as the screen background as long as the device is locked.

- **Apply to home screen**: If this option is checked, the selected devices display the chosen image as the screen background of the device’s home screen.
- **Select PNG or JPEG Picture**: Clicking this button opens a standard Open dialog in which you can choose the image that you want to use as the wallpaper on the selected devices.
- The main part of the dialog displays the currently chosen image, if any.
  Instead of using the **Select PNG or JPEG Picture** button, you can also drag an image here.

Clicking **OK** sends the image to the selected devices and sets it as their wallpaper, as specified through the two checkboxes.

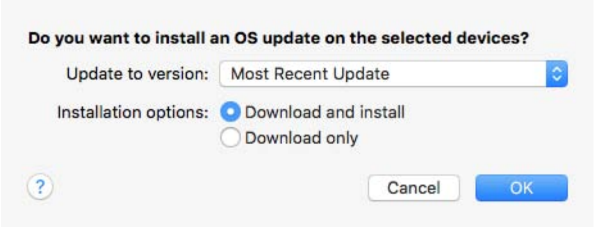
Note that the local users of the devices can change the wallpaper to other images if they so desire.

Install iOS Update

Choosing this command lets you prompt a device to download and install an available operating system update from Apple’s servers.

This command applies only to devices that run iOS 9 and up, have been enrolled through Apple’s device enrollment program, and also are supervised.

Choosing the command displays the **Install iOS Update** dialog:



Do you want to install an OS update on the selected devices?

Update to version: Most Recent Update

Installation options: ● Download and install ○ Download only

The dialog contains these elements:

- **Update to version**: The desired target version to update the device to. The pop-up menu contains the **Most Recent Update** entry and all versions that are available on Apple’s servers and that apply to the selected devices.
  If you choose a specific version, the devices are updated to that version; if you choose **Most Recent Update**, the devices are updated to the newest version available.
- **Installation options**: Whether to just download the updater or install it as well:
  - **Download and install**: The updater is downloaded and executed immediately afterwards. If the updater is already available on the device (for example, because it has been downloaded earlier using the **Download only** setting), it is executed immediately.

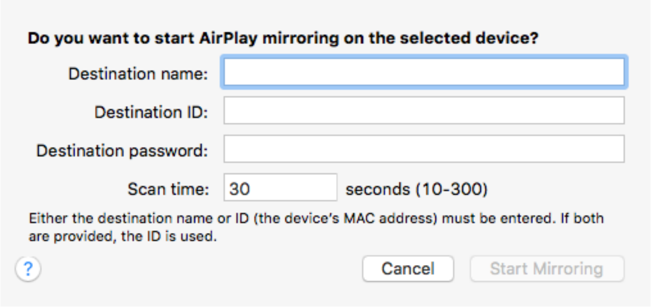
Note that some updaters give the user the option to postpone the update, but some do not. Also, some updaters require a device restart.
You can display the properties of the updater using the information items in the **Available OS Updates** category.

- **Download only**: The updater is downloaded to the device but not executed.
  If you choose this option, you can perform the installation at some later date using this command with the **Download and install** option.

Clicking **OK** causes the selected devices to request the installers from Apple's servers and, depending on the chosen options, install them.

Request AirPlay Mirroring

Choosing this command opens the **Start AirPlay Mirroring** dialog in which you can request the user of the mobile device to allow AirPlay screen mirroring, and specify a target device to which the mobile device screen is mirrored:



Do you want to start AirPlay mirroring on the selected device?

Destination name:

Destination ID:

Destination password:

Scan time: 30 seconds (10-300)

Either the destination name or ID (the device's MAC address) must be entered. If both are provided, the ID is used.

The dialog contains these elements:

- **Destination name**: The name of the device to which the AirPlay output is directed.
  If a destination ID (see below) is specified, the destination name is ignored and can be omitted.
- **Destination ID**: The MAC address of the device to which the AirPlay output is directed.
  For an Apple TV device, use the Ethernet MAC address, not the WiFi address.
  If a destination name (see above) is specified, the destination ID is optional. (If both are specified, the name is ignored.)
- **Destination password**: The password of the specified output device. If the device requires no password, leave this field empty.
- **Scan time**: The time the mobile device will search for the specified destination device. If the device is not found in this time, no AirPlay mirroring happens.

Clicking **Start Mirroring** displays an alert on the mobile device. The user of the device must allow the mirroring before it is activated.

This command applies only to supervised devices running iOS 7.0 or later. (Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)

Stop AirPlay Mirroring

Choosing this command stops AirPlay screen mirroring from the selected devices.

This command applies only to supervised devices running iOS 7.0 or later. (Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)

Change Personal HotSpot State

Choosing this command lets you activate or deactivate the personal hotspots on the selected devices.

This command applies only to supervised devices running iOS 7.0 or later. (Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)

Set Activation Lock Options

Choosing this command lets you specify whether the activation lock can be enabled on the selected devices via the "Find My iPhone" (or "Find My iPad") setting:

- If you allow the activation lock to be enabled, the feature will be automatically activated when "Find my iPhone" is switched on.
- If you disallow the activation lock, it will not be switched on together with "Find My iPhone".
  Note, however, that this does not disable an activation lock feature that is already activated. The activation lock setting remains in effect until "Find My iPhone" is next disabled, which automatically switches it off. Thereafter, it will not be enabled again, even if "Find my iPhone" is switched on again.

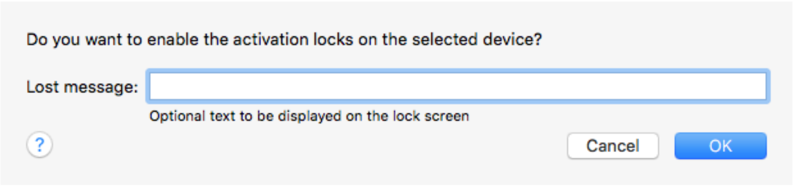
This command applies only to supervised devices running iOS 7.0 or later. (Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)

Enable Activation Lock

Choosing this command enables the activation lock on the selected devices. This command applies only to managed devices that are part of an Apple School Manager account. (To configure the activation lock on other iOS devices, use the **Set Activation Lock Options** command.)

As part of the execution of this command, an activation lock bypass key is generated that is stored in LANrev and can be displayed using the **Show Activation Lock Bypass Code** command. In normal operation, a separate key is generated for each device. If you press the Option key while choosing the command, a universal bypass code is instead generated, which is also stored in LANrev. This universal code is the same for all devices for which you have enabled the activation lock using this command, whether now or previously. (The code is specific to your installation of LANrev and will not allow you to unlock devices that have been locked elsewhere.)

Choosing the command opens the **Enable Activation Lock** dialog:



Do you want to enable the activation locks on the selected device?

Lost message:

Optional text to be displayed on the lock screen

In the dialog, you can specify the message that is display on the locked devices.

In the message text, you can use the variables described in “Variables for mobile devices” on page 458.

Clicking **OK** enables the activation lock on the selected devices and stores the generated bypass key in the LANrev database. Any future activation of the devices requires the bypass key.

Remove Activation Lock

Choosing this command removes the activation lock from the selected devices. The command can only be applied to supervised devices running iOS 7.1 and up on which “Find My iPhone” is enabled.

Removing an activation lock from a device means that it can be reset to its factory condition without requiring a password.

Show Activation Lock Bypass Code

Choosing this command displays the activation lock bypass code for the selected device. The command can only be applied to supervised devices running iOS 7.1 and up.

The bypass code can be used to access a device on which the activation lock has been engaged, either from LANrev Admin or by entering it locally on the device in the setup phase. The bypass code for a device changes if it is factory-reset and then re-enrolled.

For devices under classroom management, two different bypass codes may exist, only one of which is however active at any given time. If two codes exist for a device, both are displayed. The second code should be used if the first one does not unlock the device.

Enable Attention Mode

Choosing this command lets you activate the attention mode on the selected devices.

When a device is in attention mode, no interaction with it is possible, even after a restart. A message supplied by you is displayed on the screen until you disable the mode again. In the message text, you can use the variables described in “Variables for mobile devices” on page 458.

This command applies only to certain devices:

- iOS: Any supervised device.(Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple’s device enrollment program can be put into supervised mode in the enrollment profile, as described in “New Device Enrollment Profile” on page 640.)
- Android: Devices on which LANrev Apps 2.0.9 or up is installed or running Samsung SAFE on which LANrev Apps 2.0.5 or up is installed.

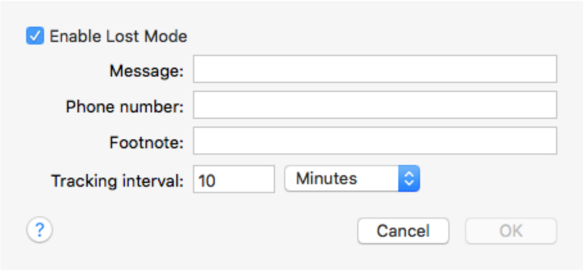
Disable Attention Mode

Choosing this command lets you deactivate the attention mode on the selected devices on which it is enabled.

See “Enabling and disabling the attention mode” on page 239 for more information on the attention mode.

Set Lost Mode

Choosing this command lets you activate or deactivate the Lost mode for the selected device. The command is compatible with supervised devices running iOS 9.3 and up.



☑ Enable Lost Mode

Message:

Phone number:

Footnote:

Tracking interval: 10 Minutes

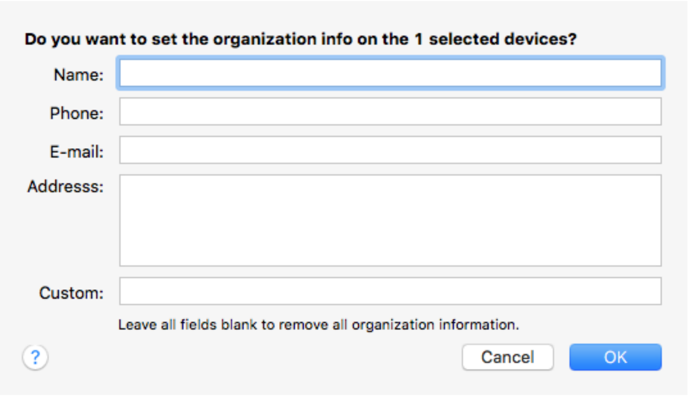
The dialog contains these elements:

- **Enable Lost Mode**: If this checkbox is checked, the Lost mode will be enabled on the on the selected device; if it is unchecked, the mode will be disabled.
  If this checkbox is unchecked, the following fields are ignored.
- **Message**: The message that is displayed on the lock screen of the device. This information is optional.
  You can use the variables described in “Variables for mobile devices” on page 458.
- **Phone number**: The phone number that is displayed on the lock screen. If the device is capable of making phone calls, this number can be called from the locked device. This information is optional.
- **Footnote**: This text is displayed at the bottom of the lock screen. This information is optional.
  You can use the variables described in “Variables for mobile devices” on page 458.
- **Tracking interval**: The frequency with which the position of the device is determined and recorded in the LANrev database. This information is optional.

Note that Lost mode is persistent: Erasing and re-enrolling the device will not take it out of Lost mode.

Set Organization Information

Choosing this command opens the **Set Organization Information** dialog through which you can store basic contact information for your organization on iOS 7 devices:



Do you want to set the organization info on the 1 selected devices?

Name:

Phone:

E-mail:

Addresss:

Custom:

Leave all fields blank to remove all organization information.

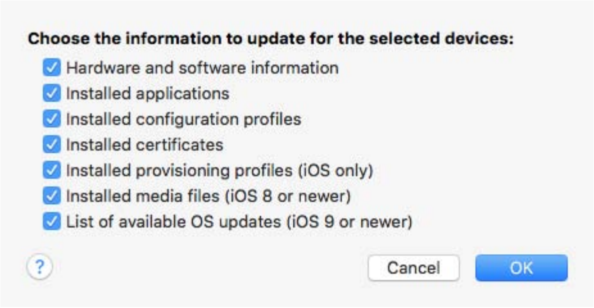
The dialog contains these elements:

- **Name**: The name of your organization.
  This field corresponds to the Mobile Device Organization Name information item.
- **Phone**: The phone number in your organization that you want external persons to call.
  This field corresponds to the Mobile Device Organization Phone information item.
- **E-mail**: The e-mail address in your organization that you want external persons to use for contacting you.
  This field corresponds to the Mobile Device Organization E-Mail information item.
- **Address**: The postal or street address of your organization.
  This field corresponds to the Mobile Device Organization Address information item.
- **Custom**: Additional information regarding your organization that you want to store on the selected mobile devices.
  This field corresponds to the Mobile Device Organization Custom information item.

Update Device Information

Choosing this command queries the device and updates the information about it in the LANrev database.

The command opens a dialog in which you can choose which categories of information to update:



Choose the information to update for the selected devices:

- ☑ Hardware and software information
- ☑ Installed applications
- ☑ Installed configuration profiles
- ☑ Installed certificates
- ☑ Installed provisioning profiles (iOS only)
- ☑ Installed media files (iOS 8 or newer)
- ☑ List of available OS updates (iOS 9 or newer)

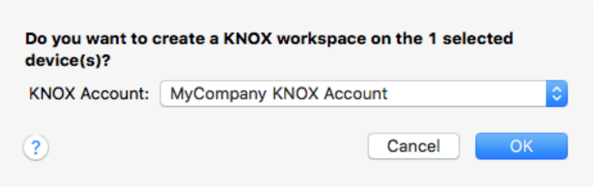
Some of the categories apply only to certain devices, as noted beside those options.

Choosing the command while holding down the Option key skips the dialog and collects information for all categories.

Create KNOX Workspace

This command lets you create a KNOX workspace on each selected device on which Samsung KNOX is available.

Choosing the command opens the **Create KNOX Workspace** dialog:



Do you want to create a KNOX workspace on the 1 selected device(s)?

KNOX Account: MyCompany KNOX Account

The KNOX account list lets you choose the KNOX account to which the workspace belongs. It contains all accounts that have been specified in the server settings. (See “Samsung KNOX Accounts dialog” on page 794 for more information.)

A newly created workspace initially has no password. The user of the device is prompted to specify a password the first time she or he accesses it.

Remove KNOX Workspace

Choosing this command removes the KNOX workspaces from all selected devices. It has no effect on devices on which no KNOX workspace is present.

When a KNOX workspace is removed, all KNOX apps and their data are removed from the device as well.

Lock KNOX Workspace

Choosing this command locks the KNOX workspaces on all selected devices. It has no effect on devices on which no KNOX workspace is present.

A locked KNOX workspace is inaccessible on the device until it is remotely unlocked again.

Unlock KNOX Workspace

Choosing this command unlocks the KNOX workspaces on all selected devices. It has no effect on devices on which no locked KNOX workspace is present.

Unlocking a KNOX workspace makes it normally accessible on the device. (That is, the user can access the workspace but still must enter the password to do so.)

Reset KNOX Workspace Password

Choosing this command removes the current passwords from the KNOX workspaces on the selected devices. The next time the user of the device tries to access the workspace, she or he is prompted to set a new password.

This command has no effect on devices on which no KNOX workspace is present.

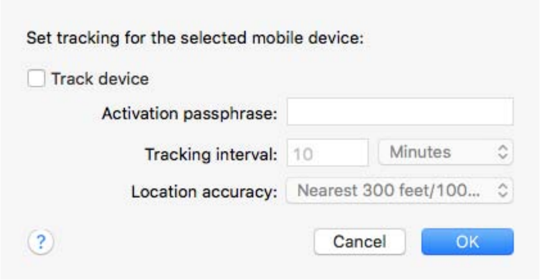
Track Device

This command lets you enable and disable geotracking for mobile devices and set tracking details. It is not available when multiple devices are selected. (This command does not support Windows Phone devices.)

IMPORTANT Because the location of a mobile device often is also the location of its user, tracking mobile devices is governed by privacy or data protection laws in many jurisdictions.
Usually, the express consent of the user of the device is required before it may be tracked. In addition, there may be regulations governing how long gathered data may be stored and how and by whom it may be accessed.
Failure to obtain the required consent or observe other applicable legal regulations may expose you to civil and/or criminal liability.

NOTE For information on geotracking iOS devices, contact HEAT Support.

Choosing the command opens the **Mobile Device Tracking** dialog:



Set tracking for the selected mobile device:

□ Track device

Activation passphrase:

Tracking interval: 10 Minutes

Location accuracy: Nearest 300 feet/100...

The dialog contains these elements:

- **Track device**: Checking this option enables tracking of the selected device, unchecking it disables it.
  Note that tracking can be enabled only for devices on which LANrev Apps is installed. Deploying LANrev Apps is described in “Preparing iOS devices for software installation” on page 195.
- **Activation passphrase**: The pin needed to access the selected mobile device.
  This pin is specified when LANrev Apps in launched for the first time on a mobile device or centrally after the deployment of LANrev Apps. See “Setting passphrases for mobile devices” on page 260 for details.
- **Tracking interval**: The interval in which a location record for the device is recorded.
  If the device has no contact with the MDM server at the scheduled time, it caches its locations and transmits it when it next has contact.
  If a device has no location information at the scheduled time, for example, because it has no GPS contact and is not in range of a known WiFi network, no location record is created.
  Specifying short tracking intervals can lead to very large numbers of tracking records and should therefore be carefully considered. For example, tracking 50 devices with an interval of five minutes creates more than five million records per year.
- **Location accuracy**: The maximum accuracy with which the device position is recorded.
  Lower accuracies mean that a device cannot be located as precisely but better preserves the privacy of the user.

If the Option key is pressed while choosing the **Track Device** command, a slightly different version of the dialog is displayed that allows you to enable geotracking on a device for which you do not have the passphrase. See “Dealing with lost passphrases” on page 264 for details.

For more information on geotracking, see “Geotracking mobile devices” on page 259.

Get Device Geolocation

This command queries the selected device for its current location and enters it in the LANrev database. (This command does not support Windows Phone devices.)

If geotracking is not currently activated on the device, you must enter the activation passphrase. You can query the locations of devices only if LANrev Apps is installed on them.

For more information on geotracking, see “Geotracking mobile devices” on page 259.

Reset Tracking Passphrase

Choosing this command removes the current passphrase from the selected mobile device. (This command does not support Windows Phone devices.)

When you choose this command, a confirmation dialog is displayed. Confirming your command removes the passphrase currently in effect on the mobile device and requires a new passphrase to be set (either locally or remotely) before LANrev Apps can be used again on the device.

See “Setting passphrases for mobile devices” on page 260 for details.

Chapter 15 *Server menu*

The **Server** menu contains commands that let you configure the LANrev server's settings and exchange information with it.

All commands affect only the server where you are currently logged in.

- **Synchronize All Tables** (page 480)
- **Reload All Tables** (page 481)
- **Synchronize Selected Records** (page 481)
- **Reload Selected Records** (page 481)
- **Save Distribution and Licensing Info** (page 481)
- **Restore Distribution and Licensing Info** (page 482)
- **Save Administrator Info** (page 482)
- **Restore Administrator Info** (page 482)
- **Save Custom Information Fields** (page 482)
- **Restore Custom Information Fields** (page 482)
- **Synchronize Custom Information Fields** (page 483)
- **Save Server Settings** (page 483)
- **Restore Server Settings** (page 483)
- **Synchronize Server Settings** (page 483)
- **Save All Settings** (page 484)
- **Restore All Settings** (page 484)
- **Synchronize VPP Licensing Data** (page 484)
- **Reload VPP Licensing Data** (page 484)
- **Synchronize Device Enrollment Data** (page 485)
- **Reload Device Enrollment Data** (page 485)
- **Reload Apple School Management Data** (page 485)
- **Import Classroom Data** (page 486)
- **Create Placeholder Computer Records** (page 493)
- **Create Placeholder Mobile Device Records** (page 494)
- **Change Server Registration** (page 497)

Synchronize All Tables

The **Synchronize All Tables** command downloads all updated information from the server to which you are connected.

Choosing the command prompts the server to send all information that the local copies of the database tables do not yet contain or contain in an outdated form.

This command makes sure that your copy of LANrev Admin has access to up-to-date information.

Pressing the Option key changes this command to **Reload All Tables** (see below).

Reload All Tables

The **Reload All Tables** command appears in the **Server** menu when the Option key is pressed. It downloads all information from the server to which you are connected.

Choosing the command prompts the server to send all information in the database tables, irrespective of whether it is already present in the local copies of the tables.

This command makes sure that the tables in your copy of LANrev Admin contain the same information as the tables in the LANrev Server database, even if they previously have been out of sync.

Synchronize Selected Records

The **Synchronize Selected Records** command downloads updated information for the selected computers from the server to which you are connected.

Choosing the command prompts the server to send all information on the selected records that the local copies of the database tables do not yet contain or contain in an outdated form.

This command makes sure that the information that is displayed in the selected records is up to date.

Pressing the Option key changes this command to **Reload Selected Records** (see below).

Reload Selected Records

The **Reload Selected Records** command appears in the **Server** menu when the Option key is pressed. It downloads all information for the selected records from the server to which you are connected.

Choosing the command prompts the server to send all information on the selected computers that is contained in the database tables, irrespective of whether it is already present in the local copies of the tables.

This command makes sure that the records in your copy of LANrev Admin contain the same information as the records in the LANrev Server database, even if they previously have been out of sync.

Save Distribution and Licensing Info

The **Save Distribution and Licensing Info** command writes the current settings for license monitoring and software distribution to the LANrev Server to which you are connected.

Choosing the command updates the information on groups, packages, licenses, and distribution points on the LANrev server to include any changes you have made locally.

Restore Distribution and Licensing Info

The **Restore Distribution and Licensing Info** command downloads the current settings for license monitoring and software distribution from the LANrev server to which you are connected.

Choosing the command updates the local information on groups, packages, licenses, and distribution points to be identical to that on the LANrev server.

Save Administrator Info

The **Save Administrator Info** command writes the current administrator account settings to the LANrev server to which you are connected.

Choosing the command updates the information on administrator accounts on the LANrev server to include any changes you have made locally.

Restore Administrator Info

The **Restore Administrator Info** command downloads the current administrator account settings from the LANrev server to which you are connected.

Choosing the command updates the local information on administrator accounts to be identical to that on the LANrev server.

Save Custom Information Fields

The **Save Custom Information Fields** command writes the current custom information field definitions to the LANrev server to which you are connected.

Choosing the command updates the information on custom information fields on the LANrev server to include any changes you have made locally.

Restore Custom Information Fields

The **Restore Custom Information Fields** command downloads the current information field definitions from the LANrev server to which you are connected.

Choosing the command updates the local information on custom information fields to be identical to that on the LANrev server.

Pressing the Option key changes this command to **Synchronize Custom Information Fields** (see below).

Synchronize Custom Information Fields

The **Synchronize Custom Information Fields** command appears in the **Server** menu when the Option key is pressed. It synchronizes the current custom information field definitions on your local computer with that of the LANrev server to which you are connected. If there are conflicts, a message informs you of the fact.

Choosing the command updates the information on custom information fields on the LANrev server to include any changes you have made locally.

Save Server Settings

The **Save Server Settings** command writes the current server settings to the LANrev server to which you are connected.

Choosing the command updates the server settings on the LANrev server to include any changes you have made locally.

Restore Server Settings

The **Restore Server Settings** command downloads the current server settings from the LANrev server to which you are connected.

Choosing the command updates the local information on settings to be identical to that on the LANrev server.

Pressing the Option key changes this command to **Synchronize Server Settings** (see below).

Synchronize Server Settings

The **Synchronize Server Settings** command appears in the **Server** menu when the Option key is pressed. It synchronizes the current server settings on your local computer with that of the LANrev server to which you are connected. If there are conflicts, a message informs you of the fact.

Choosing the command updates the server settings on the LANrev server to include any changes you have made locally.

Save All Settings

The **Save All Settings** command writes all current settings from the Server Center to the LANrev server to which you are connected.

Choosing the command updates the settings on the LANrev server to include any changes you have made locally. It is the equivalent of choosing all of these commands individually:

- **Save Distribution and Licensing Info**
- **Save Administrator Info**
- **Save Custom Information Fields**
- **Save Server Settings**

Restore All Settings

The **Restore All Settings** command downloads all current settings for the Server Center from the LANrev server to which you are connected.

Choosing the command updates the local information in the Server Center to be identical to that on the LANrev server. It is the equivalent of choosing all of these commands individually:

- **Restore Distribution and Licensing Info**
- **Restore Administrator Info**
- **Restore Custom Information Fields**
- **Restore Server Settings**

Pressing the Option key changes this command to **Synchronize Server Settings** (see below).

Synchronize VPP Licensing Data

The **Synchronize VPP Licensing Data** command updates the local cached data on VPP licensing with the new information from Apple's licensing server.

You can use this command to update the cached information between the automatic regular background updates when you want to be sure to have them reflect the most recent status.

Pressing the Option key changes this command to **Reload VPP Licensing Data** (see below).

Reload VPP Licensing Data

The **Reload VPP Licensing Data** command appears in the **Server** menu when the Option key is pressed. It downloads the data on VPP licensing from Apple's licensing server, overwriting any information cached locally.

You can use this command as a troubleshooting measure when you believe that the local cached data seriously deviates from the master data on Apple’s server and using **Synchronize VPP Licensing Data** does not appear to help.

Synchronize Device Enrollment Data

The **Synchronize Device Enrollment Data** command updates the local cached data on device enrollment with the new information from Apple’s enrollment program server.

The command synchronizes information about which devices belong to the program and account settings.

You can use this command to update the cached information between the automatic regular background updates when you want to be sure to have them reflect the most recent status.

Pressing the Option key changes this command to **Reload Device Enrollment Data** (see below).

Reload Device Enrollment Data

The **Reload Device Enrollment Data** command appears in the **Server** menu when the Option key is pressed. It downloads the data on device enrollment from Apple’s enrollment program server, overwriting any information cached locally.

The command synchronizes information about which devices belong to the program and account settings.

You can use this command as a troubleshooting measure when you believe that the local cached data seriously deviates from the master data on Apple’s server and using **Synchronize Device Enrollment Data** does not appear to help.

Reload Apple School Management Data

The **Reload Apple School Management Data** command downloads the classroom data on from Apple’s school management server, overwriting any information cached locally.

You can use this command for the initial data import from an existing classroom setup and as a troubleshooting measure when you believe that the local cached data seriously deviates from the master data on Apple’s server.

Import Classroom Data

The **Import Classroom Data** imports a JSON file containing classroom data.

Choosing the command displays an Open dialog in which you can specify the import file.

The information in the file must be formatted as described in below. A sample file demonstrating the syntax is available online in the LANrev knowledge base article 22347.

Depending on the settings in the **Classroom Settings** dialog, described in “Classroom Settings” on page 652, LANrev may perform certain automated operations during the import process.

Classroom data import file format

The file imported with the **Import Classroom Data** command must be a JSON file that implements the structure described below.The filename extension must be .json.

Except where stated otherwise, all keys are optional.

Top level

The top level of the JSON import file can contain these elements:

- ADEPAccountName: A string containing the name of the DEP account to which the imported items will be assigned.
  If you want to complete already existing records by importing this file, either this key or ADEPAccountUniqueID must be specified because they are needed for matching records. If you want to import new records, the two keys are not required.
- ADEPAccountUniqueID: A string containing the UUID of the DEP account to which the imported items will be assigned.
  As described above, either this key or ADEPAccountName is required to complete existing records but not for importing new ones.
- Modifiable: A boolean specifying whether the imported data may be modified in LANrev. If this key is omitted, the data may be modified.
- locations: An array containing defined locations. The structure of each array entry is specified below in “Locations”.
- courses: An array containing defined courses. The structure of each array entry is specified below in “Courses”.
- persons: An array containing defined persons. The structure of each array entry is specified below in “Persons”.
- person_images: An array containing images of defined persons. The structure of each array entry is specified below in “Person images”.
- person_password_prompts: An array specifying password prompts for defined persons. The structure of each array entry is specified below in “Password prompt array”.

- personal_devices: An array containing a list of associations between devices and the persons to whom they belong. The structure of each array entry is specified below in "Personal device associations".
- classes: An array containing defined classes. The structure of each array entry is specified below in "Classes".
- person_groups: An array containing definitions for groups of persons. The structure of each array entry is specified below in "Person groups".
- device_groups: An array containing definitions for groups of devices. The structure of each array entry is specified below in "Device groups".
- class_groups: An array containing definitions for groups of classes. The structure of each array entry is specified below in "Class groups".

Locations

Items in the locations array (described above in "Top level") can contain these elements:

- unique_identifier: A string containing a globally unique identifier for the location. This information must be specified.
- name: A string containing the name of the location. This information must be specified.
- source: A string containing a specification of the source of the location information. This can be any desired string, or it can be omitted entirely.
- source_system_identifier: A string containing an identifier for the location that is unique within the source system. This can be any desired string, or it can be omitted entirely.

Courses

Items in the courses array (described above in "Top level") can contain these elements:

- unique_identifier: A string containing a globally unique identifier for the course. This information must be specified.
- name: A string containing the name of the course. This information must be specified.
- source: A string containing a specification of the source of the course information. This can be any desired string, or it can be omitted entirely.
- source_system_identifier: A string containing an identifier for the course that is unique within the source system. This can be any desired string, or it can be omitted entirely.

Persons

Items in the persons array (described above in "Top level") can contain these elements:

- unique_identifier: A string containing a globally unique identifier for the person. This information must be specified.

- name: A string containing the name of the person.
  Either this information or at least one of the name components (first_name, middle_names, last_name) must be specified.
  If the full name is not specified, the content of this field will be determined from the specified name components.
  If both the full name and one or more components are specified, all information is imported unchanged.
- first_name: A string containing the first name of the person.
  See "name", above, for a discussion of required information regarding names.
- middle_names: A string containing the middle initial, name, or names of the person.
  See "name", above, for a discussion of required information regarding names.
- middle_name: This is a synonym for "middle_names" (see above). Only one of the two fields may be specified for a person.
- last_name: A string containing the last name of the person.
  See "name", above, for a discussion of required information regarding names.
- managed_apple_id: A string containing the Apple ID of the person which it uses in the classroom context.
- grade: A string containing the grade to which the person is assigned.
- role: A string containing the role which the person has in the classroom. This can be any desired string (or it can be omitted entirely), but it must be "Student" if the person is to appear in smart groups as a student, and "Instructor" if it is to appear as a teacher.
- custom_info_1: A string containing a value that you want to associate with the person. The content and its interpretation are entirely up to you.
- custom_info_2: A string containing a value that you want to associate with the person. The content and its interpretation are entirely up to you.
- source: A string containing a specification of the source of the person information. This can be any desired string, or it can be omitted entirely.
- source_system_identifier: A string containing an identifier for the person that is unique within the source system. This can be any desired string, or it can be omitted entirely.
- password_prompt: A string specifying the password prompt displayed for the user on a shared device:
  - "four": The user is prompted for a four-digit passcode.
  - "six": The user is prompted for a six-digit passcode.
  - "complex": The user is prompted for an arbitrary alphanumeric passphrase.
  - "" (empty string): No prompt is specified in the profile; which prompt is displayed is decided by the operating system defaults.

  If a password prompt is specified for a person in the password prompt array (see below), the setting specified there is used. Note that specifying a prompt that does not match the existing password of the user may prevent them from logging in. For example, specifying a six-digit code will present a keypad without letters, which makes it impossible to enter alphanumeric passwords.

Person images

Items in the person_images array (described above in “Top level”) can contain these elements:

- person_unique_identifier: A string containing the globally unique identifier of the person depicted in the image. This information must be specified.
- image_data: A string containing the binary image data in Base64 encoding. Either this key or image_file is required.
  If you specify this key with an empty string (but not if you omit it), the image in an existing matching person record is deleted.
- image_file: A string containing the path to a PNG or JPEG file with the image. The path must be an absolute path from the LANrev Server computer to the file. Either this key or image_data is required.
- image_data_type: A string containing the MIME type of the binary data in image_data. This key is required if image_data is specified and ignored otherwise.
  If you specify this key with the value `"(null)"`, the image in an existing matching person record is deleted.

Password prompt array

Items in the person_password_prompts array (described above in “Top level”) each must contain these elements:

- person_unique_identifier: A string containing the globally unique identifier of the person depicted in the image. This information must be specified.
- password_prompt: A string specifying the password prompt displayed for the user on a shared device:
  - “four”: The user is prompted for a four-digit passcode.
  - “six”: The user is prompted for a six-digit passcode.
  - “complex”: The user is prompted for an arbitrary alphanumeric passphrase.
  - “” (empty string): No prompt is specified in the profile; which prompt is displayed is decided by the operating system defaults.

  Note that specifying a prompt that does not match the existing password of the user may prevent them from logging in. For example, specifying a six-digit code will present a keypad without letters, which makes it impossible to enter alphanumeric passwords.
  This information must be specified.

Using the person_password_prompts array lets you specify password prompts for persons that are already present in the LANrev database. If you are setting password prompts for persons you are importing, we recommend that you specify them in the persons array (see above) instead, using the password_prompt element.

Personal device associations

Items in the personal_devices array (described above in “Top level”) can contain these elements:

- person_unique_identifier: A string containing the globally unique identifier of the person to whom the device belongs. This information must be specified.
- device_serial_numbers: An array of strings. Each string contains the serial number (as specified in the Mobile Device Serial Number information item) of a device that belongs to the specified person.
  If any of the specified devices is currently assigned to a different person, that assignment is removed. If devices that are currently associated with the specified person are not listed in the array, their assignment to the person is removed.
  If this key is specified, the remove_device_serial_numbers and add_device_serial_numbers keys are ignored.
- remove_device_serial_numbers: An array of strings. Each string contains the serial number of a device that should no longer be associated with the specified person.
  If the device_serial_numbers key is specified, this key is ignored.
  If both remove_device_serial_numbers and add_device_serial_numbers keys are specified, remove_device_serial_numbers is applied first.
- add_device_serial_numbers: An array of strings. Each string contains the serial number of a device that should be associated with the specified person.
  If the device_serial_numbers key is specified, this key is ignored.
  If both remove_device_serial_numbers and add_device_serial_numbers keys are specified, remove_device_serial_numbers is applied first.

Classes

Items in the classes array (described above in “Top level”) can contain these elements:

- unique_identifier: A string containing a globally unique identifier for the class. This information must be specified.
- name: A string containing the name of the class.
  This information must normally be specified. However, if a valid course is specified (see below) and this key is omitted, the name of the course is also used as the class name.
- room: A string containing the room where the class is held.
- location: A dictionary containing the required unique identifier of the location and optionally its name.
- course: A dictionary containing the required unique identifier of the course and optionally its name.
- instructor_unique_identifiers: An array containing the unique identifiers of all persons that are instructors in this class.

Note that instructors are not required to have any particular role; for example, a person with the “Student” role can be specified as an instructor.

- student_unique_identifiers: An array containing the unique identifiers of all persons that are students in this class.
  Note that instructors are not required to have any particular role; for example, a person with the “Instructor” role can be specified as a student.
- source: A string containing a specification of the source of the class information. This can be any desired string, or it can be omitted entirely.
- source_system_identifier: A string containing an identifier for the class that is unique within the source system. This can be any desired string, or it can be omitted entirely.

Person groups

Items in the person_groups array (described above in “Top level”) can contain these elements:

- uuid: A string containing the UUID of the group. This information must be specified.
- name: A string containing the name of the group.
  This information must be specified.
- group_type: The type of the group. Available types include:
  - plain
  - smart
  - smart/teacher
  - smart/student

  This information is optional. If it is missing, the type of the group depends on whether a “filter” element or a “members” element (see below) is specified.
- filter: The condition for group membership.
  This information is required for smart groups and must not be provided for plain groups.
  The structure of the filter is undocumented. If you want to create smart group definitions outside of LANrev (as opposed to simply exporting and importing them), create a smart group that uses the information items and Boolean operator you need (“all” or “any”) and export it. You can then use this exported group definition as a template and modify the comparison value in the CompareValue key as required.
- members: An array containing the unique identifiers of all persons that are members of the group.
  This information is required for plain groups and must not be provided for smart groups.

Device groups

Items in the device_groups array (described above in “Top level”) can contain these elements:

- uuid: A string containing the UUID of the group. This information must be specified.
- name: A string containing the name of the group.

This information must be specified.

- group_type: The type of the group. Available types include:
  - plain
  - smart
  - smart/teacher
  - smart/student

  This information is optional. If it is missing, the type of the group depends on whether a “filter” element or a “members” element (see below) is specified.
- filter: The condition for group membership.
  This information is required for smart groups and must not be provided for plain groups.
  The structure of the filter is undocumented. If you want to create smart group definitions outside of LANrev (as opposed to simply exporting and importing them), create a smart group that uses the information items and Boolean operator you need (“all” or “any”) and export it. You can then use this exported group definition as a template and modify the comparison value in the CompareValue key as required.
- members: An array containing the unique identifiers of all devices that are members of the group.
  This information is required for plain groups and must not be provided for smart groups.

Class groups

Items in the class_groups array (described above in “Top level”) can contain these elements:

- uuid: A string containing the UUID of the group. This information must be specified.
- name: A string containing the name of the group.
  This information must be specified.
- group_type: The type of the group. Available types include:
  - plain
  - smart
  - smart/teacher
  - smart/student

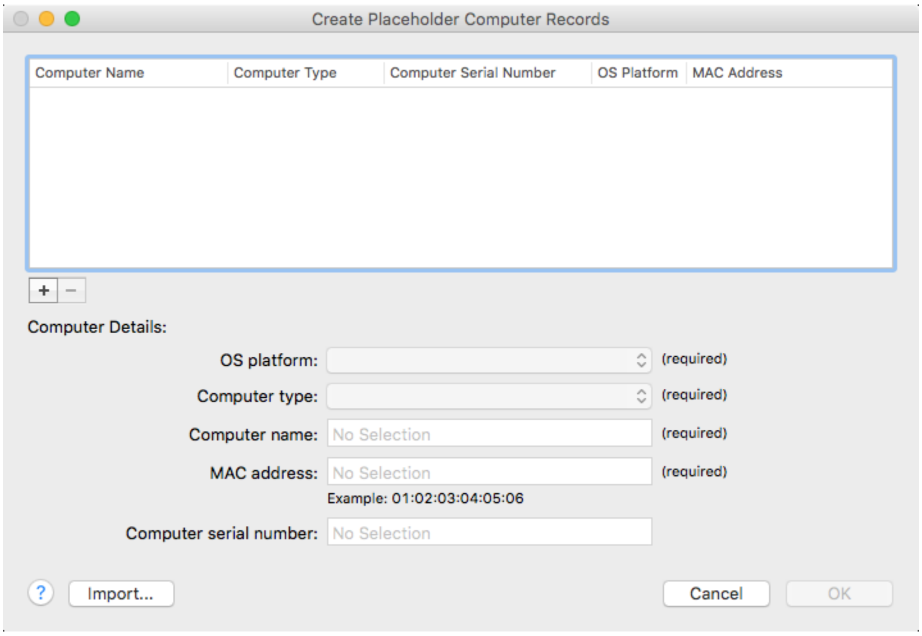
  This information is optional. If it is missing, the type of the group depends on whether a “filter” element or a “members” element (see below) is specified.
- filter: The condition for group membership.
  This information is required for smart groups and must not be provided for plain groups.
  The structure of the filter is undocumented. If you want to create smart group definitions outside of LANrev (as opposed to simply exporting and importing them), create a smart group that uses the information items and Boolean operator you need (“all” or “any”) and export it. You can then use this exported group definition as a template and modify the comparison value in the CompareValue key as required.
- members: An array containing the unique identifiers of all classes that are members of the group.
  This information is required for plain groups and must not be provided for smart groups.

A sample file demonstrating the syntax is available online in the LANrev knowledge base article 22347.

Create Placeholder Computer Records

The **Create Placeholder Computer Records** lets you create dummy records for use in reinstalling Windows computers on which no LANrev Agent is yet installed.

Choosing the command opens the **Create Placeholder Computer Records** dialog:



The dialog contains these elements:

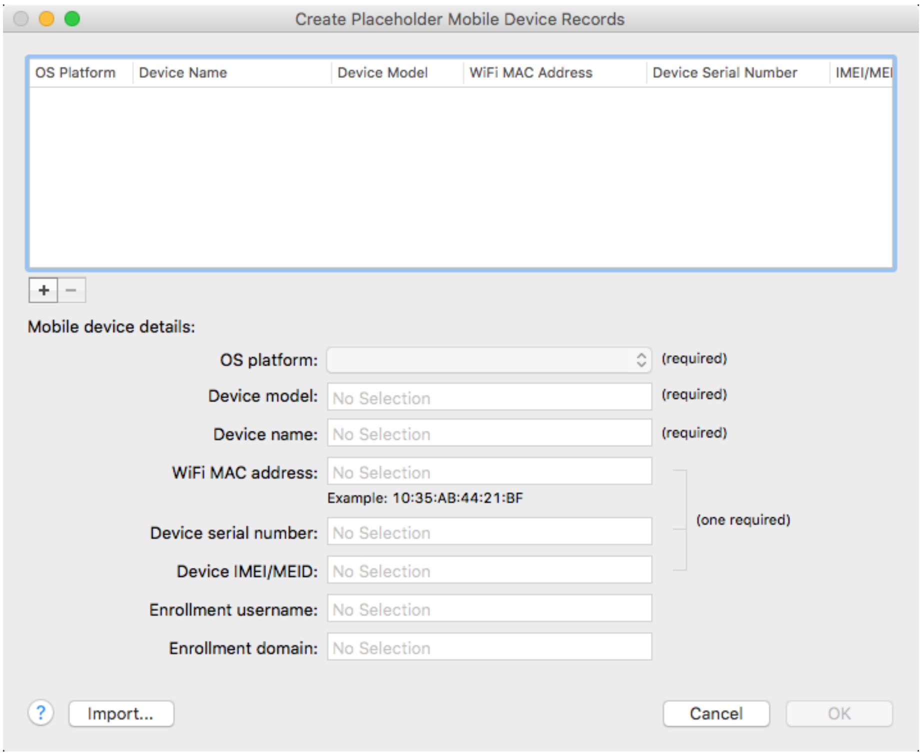
- The list at the top contains all custom computer records that you have specified since opening the dialog.
  The list does not contain records that you have specified in earlier uses of this dialog.
- The **+** button lets you create a new record. Clicking the button creates a new entry in the list and activates the entry fields below the list.
- Clicking the **-** button deletes the currently selected records from the list.
- **OS platform**: The flavor of operating system used on the computer. This information appears in the **OS Platform** column of browser windows.
- **Computer type**: The make of the computer that is being specified. This information appears in the **Computer Type** column of browser windows.
- **Computer name**: A descriptive name for the computer. This information appears in the **Agent Name** column of browser windows.

- **MAC address**: The MAC address of the network interface of the specified computer. This information appears in the **Primary MAC Address** column of browser windows.
- **Computer serial number**: The serial number of the computer. This information is optional; if provided, it appears in the **Computer Serial Number** column of browser windows.
- **Import**: Clicking this button displays a standard Open dialog in which you can selec a tab-delimited text file that contains the information for the placeholder records you want to create. The file must contain one line for each record, with this information (in this order, separated by tabs):
  - OS platform: “macOS” or “Windows”
  - Computer type: The type as displayed in the Computer Type information item
  - Computer name: The name as displayed in the Computer Name information item
  - MAC address: The MAC address of the computer’s main network interface
  - Computer serial number: The serial number as displayed in the Computer Serial Number information item. This information is optional.
- **OK**: Clicking the **OK** button creates dummy computer records in the LANrev database. These records appear in browser windows but can be used only as targets for the **Reinstall Windows Computer** command.

Create Placeholder Mobile Device Records

The **Create Placeholder Mobile Device Records** lets you create dummy records for use in MDM management, when you want to prepare the administration of devices that you know will have to be managed but are not enrolled yet.

Choosing the command opens the **Create Placeholder Mobile Device Records** dialog:



Mobile device details:

OS platform: (required)

Device model: No Selection (required)

Device name: No Selection (required)

WiFi MAC address: No Selection

Example: 10:35:AB:44:21:BF

Device serial number: No Selection

Device IMEI/MEID: No Selection

(one required)

Enrollment username: No Selection

Enrollment domain: No Selection

The dialog contains these elements:

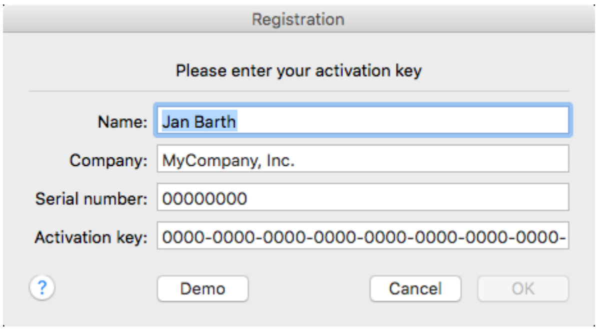
- The list at the top contains all custom mobile device records that you have specified since opening the dialog.
  The list does not contain records that you have specified in earlier uses of this dialog.
- The **+** button lets you create a new record. Clicking the button creates a new entry in the list and activates the entry fields below the list.
- Clicking the **-** button deletes the currently selected records from the list.
- **OS platform**: The flavor of operating system used on the computer. This information appears in the **Mobile Device OS Platform** column of browser windows.
- **Device model**: The make of the device that is being specified. This information appears in the **Mobile Device Model** column of browser windows.
- **Device name**: A descriptive name for the device. This is the information that appears in the **Mobile Device Name** column of browser windows.
- **WiFi MAC address**: The MAC address of the WiFi network interface of the specified device. This information is optional if either the serial number or the IMEI or MEID number (see below) has been specified. If provided, the information appears in the **Mobile Device WiFi MAC Address** column of browser windows.
- **Device serial number**: The serial number of the device. This information is optional if either the MAC address (see above) or

the IMEI or MEID (see below) has been specified. If provided, the information appears in the **Mobile Device Serial Number** column of browser windows.

- **Device IMEI/MEID**: The IMEI or MEID number of the device. This information is optional if either the MAC address or the serial number (see above) is specified. If provided, the information appears in the **Mobile Device IMEI** column of browser windows.
- **Enrollment username**: The account name of the Active Directory or Open Directory account to which the device will be connected. This information is optional; if provided, it appears in the **Device User Enrollment Username** column of browser windows.
- **Enrollment domain**: The domain name of the Active Directory account. This information is optional; if provided, it appears in the **Device User Enrollment Domain** column of browser windows.
- **Import**: Clicking this button displays a standard Open dialog in which you can selec a tab-delimited text file that contains the information for the placeholder records you want to create. The file must contain one line for each record, with this information (in this order, separated by tabs):
    - OS platform: "Android", "iOS", or "Windows Phone"
    - Device model: The type of the device as displayed in the Mobile Device Model information item
    - Device name: The name as displayed in the Mobile Device Name information item
    - WiFi MAC address: The MAC address of the device's WiFi network interface. This information is optional if the serial number or IMEI/MEID number is specified.
    - Device serial number: The serial number as displayed in the Mobile Device Serial Number information item. This information is optional if the WiFi MAC address or IMEI/MEID number is specified.
    - Device IMEI/MEID: The serial number as displayed in the Mobile Device IMEI or Mobile Device MEID information item, respectively. This information is optional if the WiFi MAC address or serial number is specified.
    - Enrollment username: The name of the Active Directory or Open Directory account to which the device is connected, as displayed in the Device User Enrollment Username information item. This information is optional.
    - Enrollment domain: The domain of the Active Directory account to which the device is connected, as displayed in the Device User Enrollment Domain information item. This information is optional.
- **OK**: Clicking the **OK** button creates dummy device records in the LANrev database. These records can be assigned to policies but cannot be used as command targets.

Change Server Registration

The **Change Server Registration** command opens the **Registration** dialog that lets you change the registration specifications for the server, for example, to increase the number of users:


Registration

Please enter your activation key

Name: Jan Barth

Company: MyCompany, Inc.

Serial number: 00000000

Activation key: 0000-0000-0000-0000-0000-0000-0000-0000-

The dialog contains these fields:.

- **Name**: Your name.
- **Company**: The name of your company.
- **Serial number**: The serial number of your copy of LANrev.
- **Activation key**: The LANrev activation key that you have received.
- **Demo**: Clicking this button starts LANrev Server in demo mode. In demo mode, LANrev can be used for 45 days to administer up to ten computers and up to ten mobile devices. *Note: The demo mode is only available when the server has not yet been registered.*

NOTE The **Change Server Registration** command can be used only by administrators with the **Change Server Settings** right. See “New Administrator” on page 758 for details.

Chapter 16 Window menu

The **Window** menu contains commands related to working with windows. There are commands for arranging windows, commands to open a range of predefined windows, and commands for opening user-created windows:

- **Zoom** (page 498)
- **Minimize** (page 498)
- **Show Previous Tab** (page 499)
- **Show Next Tab** (page 499)
- **Move Tab to New Window** (page 499)
- **Merge All Windows** (page 499)
- **Bring All to Front** (page 499)
- **Computers** (page 499)
- **Files** (page 500)
- **Fonts** (page 500)
- **Processes** (page 500)
- **Installed Software** (page 500)
- **Missing Patches** (page 502)
- **Registry Entries** (page 504)
- **Compliance Reports** (page 504)
- **Power Usage Reports** (page 505)
- **Mobile Devices** (page 508)
- **Classroom Management** (page 508)
- **Server Center** (page 509)
- **Agent Deployment Center** (page 509)
- **Commands** (page 509)
- **Command Templates** (page 510)
- **Window Reinstallation Tasks** (page 511)
- **Information Items** (page 513)
- **Activity** (page 513)
- **User windows** (page 514)

The frontmost window is indicated by a checkmark ✓; other open windows are marked with a dash –.

Zoom

The **Zoom** command toggles the frontmost window between its normal size and full-screen size.

Minimize

The **Minimize** command reduces the frontmost window to an icon and puts it in the dock.

Show Previous Tab

The **Show Previous Tab** command displays the previous tab in the front-most window, if that window contains multiple tabs.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Note that the commands in this menu section relate to the tab management provided by macOS. They have nothing to do with LANrev's tabs that can be created with the **New Tab** command.

Show Next Tab

The **Show Next Tab** command displays the next tab in the front-most window, if that window contains multiple tabs.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Move Tab to New Window

The **Move Tab to New Window** command displays the front-most tab in a window of its own.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Merge All Windows

The **Merge All Windows** command moves all open LANrev Remote windows as tabs into a single window.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Bring All to Front

The **Bring All to Front** command puts all windows of LANrev Admin in front of the windows of all other applications.

Computers

The **Computers** command opens the **Computers** window.

The **Computers** window is a predefined browser window that displays the contents of the Computers table of the LANrev database, that is, all administered client computers.

Browser windows are described in “Browser windows” on page 517. The columns in the **Computers** window are described in “Information items” on page 831.

Files

The **Files** command opens the **Files** window.

The **Files** window is a predefined browser window that displays the contents of the Files table of the LANrev database, that is, all files that have been searched for on client computers.

Browser windows are described in “Browser windows” on page 517. The columns in the **Files** window are described in “Files” on page 867.

Fonts

The **Fonts** command opens the **Fonts** window.

The **Fonts** window is a predefined browser window that displays the contents of the Fonts table of the LANrev database, that is, all fonts that have been found to be installed on client computers.

Browser windows are described in “Browser windows” on page 517. The columns in the **Fonts** window are described in “Fonts” on page 861.

Processes

The **Processes** command opens the **Processes** window.

The **Processes** window is a predefined browser window that displays the contents of the Processes table of the LANrev database, that is, all processes that have been found to be running on client computers.

Browser windows are described in “Browser windows” on page 517. The columns in the **Processes** window are described in “Processes” on page 866.

Installed Software

The **Installed Software** command opens the **Installed Software** window.

The **Installed Software** window is a predefined browser window that displays the contents of the Installed Software table of the LANrev database, that is, all software that has been found to be installed on client computers by means of the **Gather Installed Software** command described on page 453.

NOTE The **Gather Installed Software** command may not find all software on client computers. Software outside the Applications or Program Files folders the installation of which has not generated an installer receipt is not listed in this window.

Browser windows are described in “Browser windows” on page 517. The columns in the **Processes** window are described in “Processes” on page 866.

The **Installed Software** window contains some additional groups and context menu items that are not present in standard browser windows. These are described below.

Groups

There are a number of predefined smart groups in the **Installed Software** window:

- **Mac Software**: All installed software – both installer receipts and the contents of the **Applications** folder – that has been found on macOS clients.
- **Mac Installer Receipts**: Installed software that has been found on macOS clients by checking installer receipts.
- **Mac Applications**: Installed software that has been found on macOS clients by searching the specified folders on client computers.
- **Apple Software**: Software from Apple Computer, Inc., that has been found on macOS clients.
- **Non-Apple Software**: Software that has been found on macOS clients and that has not been created by Apple Computer, Inc.
- **PC Software**: All installed software – both installer receipts and the contents of the **Program Files** folder – that has been found on Windows clients.
- **PC Installer Receipts**: Installed software that has been found on Windows clients by checking installer receipts.
- **PC Applications**: Installed software that has been found on Windows clients by searching the specified folders on client computers.
- **PC Hotfixes**: Any installed patches from Microsoft were found on client computers and are marked as hotfixes.
- **Mac Installer Receipt Statistics**: Summary information on the kinds and numbers of all installed software that has been found on client macOS computers by scanning installer receipts.
- **Mac Application Statistics**: Summary information on the kinds and numbers of all installed software that has been found on client macOS computers by searching the **Applications** folders.

- **PC Installer Receipt Statistics**: Summary information on the kinds and numbers of all installed software that has been found on client Windows computers by scanning installer receipts.
- **PC Application Statistics**: Summary information on the kinds and numbers of all installed software that has been found on client Windows computers by searching the **Program Files** folders.

Context menu commands

In addition to some commands found in other browser windows, the context menu of the **Installed Software** window contains some unique commands:

- **New Smart Group: Installed Software**: This command opens a dialog in which you can define a new smart group for the contents of the Installed Software table (that is, the contents of the **Installed Software** window).
- **New Smart Group: Installed Software Statistics**: This command opens a dialog in which you can define a new smart group for statistics information on installed software.
- **New Smart Group: Computers by Installed Software**: This command opens a dialog in which you can define a new smart group for computers based on software that is installed on it or software that is not installed on it.
  You can choose:
  - Whether to list computers that match some or all of the specified software.
  - Whether to list computers that have or do not have the software.
  - Which method to use to decide whether the software is installed.

  Smart groups defined by this command list only computers running the operating system family specified by the matching method. For example, if you specify software matching by PC installer receipt, the resulting group contains only Windows client computers. Even if the group contains computers missing the specified software, macOS client computers – who by definition miss the specified software – are not listed.

NOTE Creating smart groups is described in “Creating a smart group” on page 140.

Missing Patches

The **Missing Patches** command opens the **Missing Patches** window.

The **Missing Patches** window is a predefined browser window that displays OS and third-party patches that are known to LANrev but are not installed on applicable computers.

The data displayed in this window is collected using the **Gather Installed Software** command.

NOTE Patches that were rejected by an administrator are not considered to be missing patches. Furthermore, only client computers that are part of the automated patch management are considered.

The **Missing Patches** window has slightly different predefined smart groups and context menu than other browser windows, as described below.

Predefined smart groups

The **Missing Patches** window contains four default smart groups:

- **Missing macOS Patches**: Patches missing on macOS computers.
- **Missing Windows Patches**: Patches missing on Windows computers.
- **Missing macOS Patch Statistics**: An overview of all patches that are missing on at least one client macOS computer and the total number of computers on which each of these patches is missing.
- **Missing Windows Patch Statistics**: Same as **Missing macOS Patch Statistics** but for Windows computers.

Context menu

The context menu contains these commands:

- **New Missing macOS Patches Smart Group**: Creates a new smart group for missing macOS patches.
- **New Missing Windows Patches Smart Group**: Creates a new smart group for missing Windows patches.
- **New Missing macOS Patch Statistics Smart Group**: Creates a new smart group for summary information on missing patches on macOS computers.
- **New Missing Windows Patch Statistics Smart Group**: Creates a new smart group for summary information on missing patches on Windows computers.

The dialog for defining smart groups is described in “New Smart Group” on page 522.

Computer- and file-related commands in the context menu are described in “Commands menu” on page 399.

For the remaining three commands (**Rename Group**, **Edit Smart Group**, and **Remove Group**), see the description of browser windows in “Browser windows” on page 517.

Further information

Browser windows in general are described in “Browser windows” on page 517. The columns in the **Missing Patches** window are described in “Missing Patches” on page 865 and “Missing Patch Statistics” on page 892.

Details of LANrev’s patch management are described in “Automated patch management” on page 333.

Registry Entries

The **Registry Entries** command opens the **Registry Entries** window.

The **Registry Entries** window is a predefined browser window that displays registry entries which have been found by the **Search Windows Registry** command.

Predefined smart groups

The usual **Macs only** and **All Computers** smart groups are not present in the **Registry Entries** window because registries are found only on PCs.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 517.

Further information

Browser windows in general are described in “Browser windows” on page 517. The columns in the **Registry Entries** window are described in “Registry Entries” on page 870.

Compliance Reports

The **Compliance Reports** command opens the **Compliance Reports** window.

The **Compliance Reports** window is a predefined browser window that displays compliance reports which have been created by means of the **Gather Compliance Report** command.

Double-clicking any report opens the **Compliance Report** window for that report. See “Compliance Report window” on page 531 for details.

Predefined smart groups

The only predefined smart group is the **All Reports** group.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 517. (The **New Smart Compliance Report Group** command is similar to the **New Smart Group** command.)

The context menu in the main window area contains an additional command, **Show Report Details**. Choosing this command opens the **Compliance Report** window for that report, just like double-clicking the report would.

Further information

Browser windows in general are described in “Browser windows” on page 517. The columns in the **Compliance Reports** window are described in “Compliance Reports” on page 892.

Power Usage Reports

The **Power Usage Reports** command opens the **Power Usage Reports** window.

The **Power Usage Reports** window is a special window that displays summary information on power savings achieved by using LANrev’s power management features.

Predefined smart groups

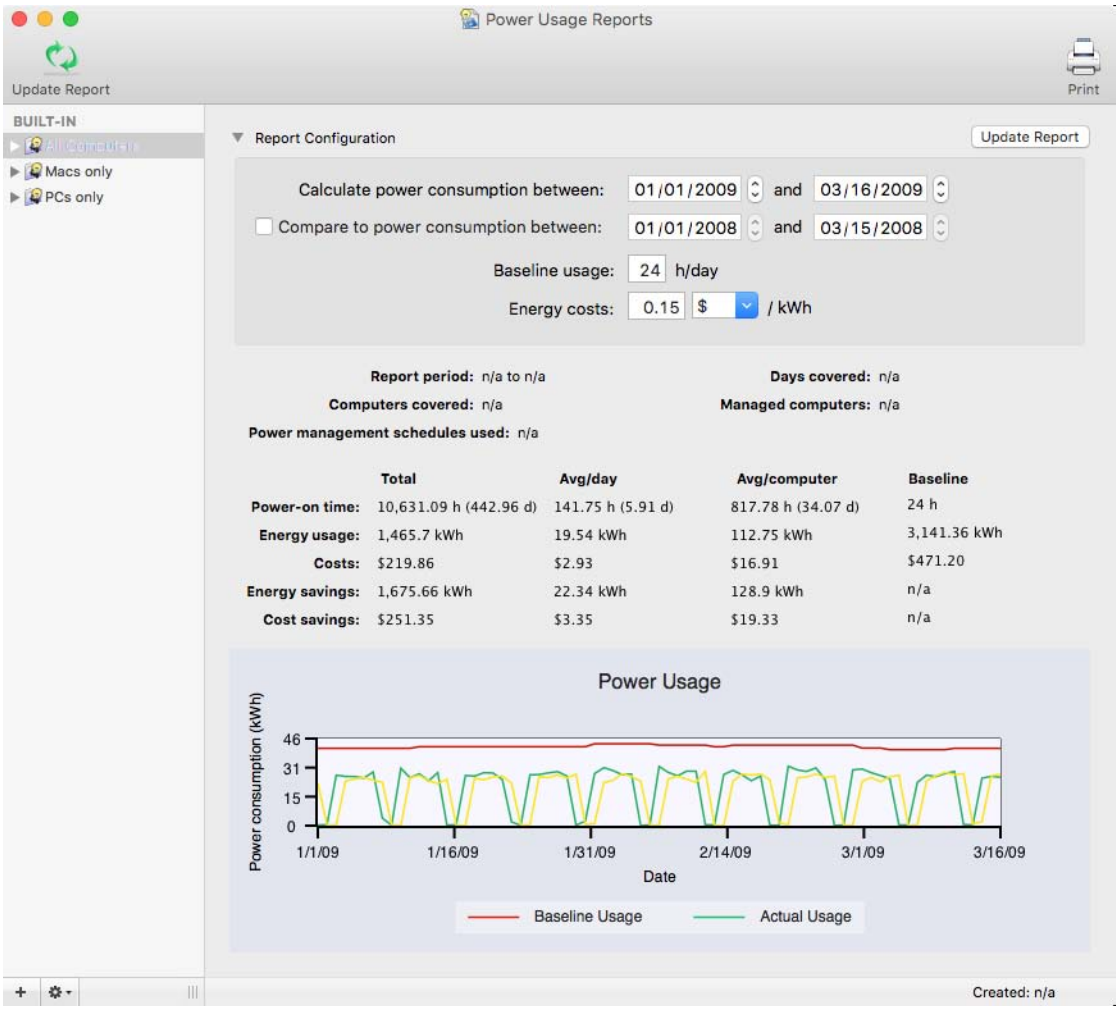
The predefined smart groups are similar to the ones in standard browser windows, as described in “Sidebar” on page 521. Reports are created for the selected groups.

Context menu

The context menu commands are covered in the description of browser windows in “Browser windows” on page 517.

Main window area

The main area of the compliance report window contains a configuration section, a statistics section, and a graphical display of the power consumption.



Calculate power consumption between: 01/01/2009 and 03/16/2009

□ Compare to power consumption between: 01/01/2008 and 03/15/2008

Baseline usage: 24 h/day

Energy costs: 0.15 $ / kWh

Report period: n/a to n/a

Days covered: n/a

Computers covered: n/a

Managed computers: n/a

Power management schedules used: n/a

	Total	Avg/day	Avg/computer	Baseline
Power-on time:	10,631.09 h (442.96 d)	141.75 h (5.91 d)	817.78 h (34.07 d)	24 h
Energy usage:	1,465.7 kWh	19.54 kWh	112.75 kWh	3,141.36 kWh
Costs:	$219.86	$2.93	$16.91	$471.20
Energy savings:	1,675.66 kWh	22.34 kWh	128.9 kWh	n/a
Cost savings:	$251.35	$3.35	$19.33	n/a

Created: n/a

In the configuration section:

- **Update Report**: Clicking this button recalculates the displayed statistics and the graph based on the current configuration settings for the selected computer group.
- **Calculate power consumption between**: The power consumption between the dates you specify here (inclusive) is displayed both in the statistics section and the graph.
- **Compare to power consumption between**: If this option is checked, the historic power consumption in the specified period is displayed in the graph for comparison purposes. This period is exactly as long as the primary period chosen above.
- **Baseline usage**: This is the number of hours per day that an administered computer is considered to be running without the LANrev power management. In effect, this number provides the value from which your savings are calculated.

- **Energy costs**: The price you pay for a kilowatt-hour of electricity. Enter a value and a currency; some common currencies can be chosen from the pop-up menu.

In the statistics section:

- **Report period**: The days for which the statistics are provided. Note that this may differ from the dates in the configuration section if you have changed the period and not yet clicked the **Update Report** button.
- **Days covered**: The number of days in the report period.
- **Computers covered**: The number of computers that have been included in the report.
- **Managed computers**: The number of computers to which power management schedules are currently being applied.
- **Power management schedules used**: A list of power management schedules that are being applied to the managed computers.
- **Power-on time**: The time the computers included in the report have been running. Reported values include:
  - **Total**: the sum over all computers and report days
  - **Avg/day**: the daily average for all computers
  - **Avg/computer**: the average per computer over the entire report period
  - **Baseline**: the comparison value over all computers and days if no power management had happened
- **Energy usage**: The power consumption of the computers in the report.
  The consumption is calculated using these typical values:
  - Desktop computer: 105 W operational, 5 W sleep
  - Laptop computer: 30 W operational, 2 W sleep
  - LCD monitor: 35 W operational, 0 W sleep
  - CRT monitor: 65 W operational, 0 W sleep

  See **Power-on time**, above for explanations of the individual values.
- **Costs**: The costs of the consumed power.
  See **Power-on time**, above for explanations of the individual values.
- **Energy savings**: The power saved when compared to the baseline level.
  See **Power-on time**, above for explanations of the individual values.
- **Cost saving**: The money saved when compared to the baseline level.
  See **Power-on time**, above for explanations of the individual values.

The graph provides a visual overview of the power that has been used during the report period. It contains three data series:

- Baseline usage: The amount of power that would have been consumed without the power management schedules. (Based on the number of hours that is specified in the **Baseline usage** field.)

- Actual usage: The amount of power that was consumed during each displayed interval.
- Historic usage: The power usage during the specified comparison period.

NOTE Both the actual and the baseline power consumption is calculated based on the values in the **Power Consumption** preferences pane.

Further information

LANrev's power management functions are described in "Scheduling power management events" on page 148.

Mobile Devices

The **Mobile Devices** command opens the **Mobile Devices** window that integrates all aspects of working with administered mobile devices, such as iPhones and iPads.

The **Mobile Devices** window is much like a browser window. However, in contrast to a normal browser window, it displays information from one of several database tables grouped into multiple categories, depending on which smart group or other sidebar entry is selected.

The items and action menu commands of the **Mobile Devices** window are described in "Mobile Devices" on page 538.

Browser windows in general are described in "Browser windows" on page 517. The columns in the **Mobile Devices** window are described in "Mobile Device Information" on page 894.

Classroom Management

The **Classroom Management** command opens the **Classroom Management** window that integrates all aspects of working with classes, teachers, students, and devices used in education.

The **Classroom Management** window is much like a browser window. However, in contrast to a normal browser window, it displays information from one of several database tables grouped into multiple categories, depending on which smart group or other sidebar entry is selected.

The items and action menu commands of the **Classroom Management** window are described in "Classroom Management" on page 649.

Browser windows in general are described in "Browser windows" on page 517. The columns in the **Classroom Management** window are described in "Classroom Management" on page 936.

Server Center

The **Server Center** command opens the **Server Center** window that integrates all aspects of configuring software distribution, license monitoring, and administrator accounts, and server monitoring.

The **Server Center** window is much like a browser window. However, in contrast to a normal browser window, it displays information from one of several database tables grouped into multiple categories, depending on which smart group or other sidebar entry is selected.

The items and action menu commands of the **Server Center** window are described in "Server Center" on page 684.

Browser windows in general are described in "Browser windows" on page 517. The columns in the **Server Center** window are described in "Server Center" on page 872.

Agent Deployment Center

The **Agent Deployment Center** command opens the **Agent Deployment Center** window that integrates all aspects of centrally installing and updating LANrev Agent on administered computers.

The **Agent Deployment Center** window is much like a browser window. However, in contrast to a normal browser window, it displays information on devices in the network – computers and other devices.

The items and action menu commands of the **Agent Deployment Center** window are described in "Agent Deployment Center" on page 803.

Browser windows in general are described in "Browser windows" on page 517. The columns in the **Agent Deployment Center** window are described in "Agent Deployment Center" on page 890.

NOTE The Agent Deployment Center can be used only by administrators with the **Deploy Agents** right. See "New Administrator" on page 758 for details.

Commands

The **Commands** command opens the **Commands** window that displays all pending and currently executing commands as well as the command history and lets you edit and reschedule commands. You can also issue new commands by selecting the desired target computers and choosing the desired option from the **Commands** menu.

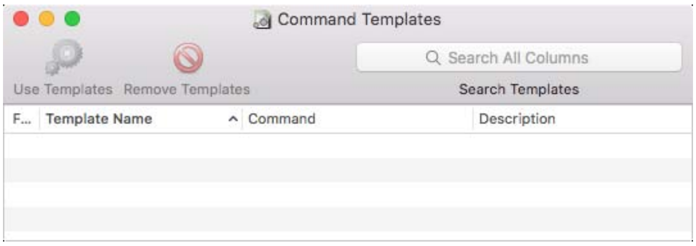
The **Commands** window is much like a browser window. However, in contrast to a normal browser window, it displays information items from the **Commands** category (described in “Commands” on page 871).

The items and action menu commands of the **Commands** window are described in “Commands window” on page 822.

Browser windows in general are described in “Browser windows” on page 517.

Command Templates

The **Command Templates** command opens the **Command Templates** window that lists all commands that have been saved as templates.



The window contains these elements:

- **Search Templates**: This field lets you quickly restrict the display to command templates that contain the search text.
- **Favorite**: Command templates checked in this column appear in the **Favorites** submenu of the **Commands** menu.
- **Template Name**: The name under which the template has been saved. You can click this field of a selected command template to edit the name.
- **Command**: The command that is executed by the template.
- **Description**: The description of the command template that you have entered when saving the template. You can click this field of a selected command template to edit the description.

Toolbar buttons

The toolbar can contain these buttons (in addition to standard elements common to toolbars in all applications):

- **Search Templates**: When text is entered into this field, the display is restricted to command templates containing that text.
- **Use Templates**: Clicking this toolbar button opens the selected templates, just like the **Use Template** context menu command described below.
- **Remove Templates**: Clicking this toolbar button deletes the selected templates, just like the **Remove Template** context menu command described below.

Context menu

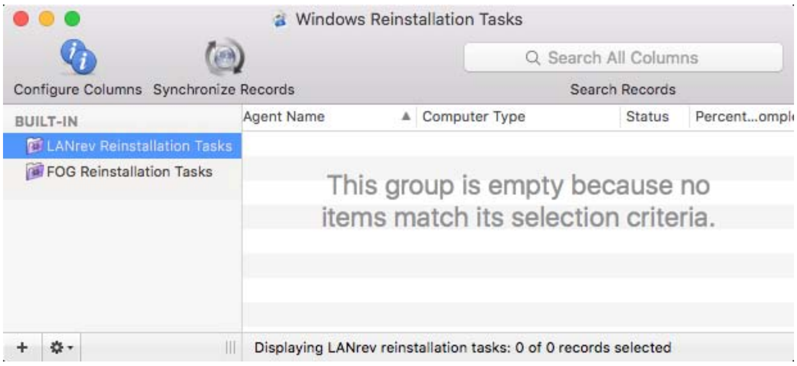
The window’s context menu contains these commands:

- **Use Template**: Choosing this command opens the selected templates, displaying the respective commands’ command dialogs.
  You can edit all the options in these dialogs, including the target list, before clicking the **Execute** button to actually issue the command.
- **Remove Template**: Choosing this command deletes the selected templates from the Command Templates window.
  If the template was included in the **Favorites** submenu, it is removed there as well.
- **Import Templates**: Choosing this command displays a standard Open dialog in which you can select a command templates file that has previously been exported using the **Export Templates** command or by dragging templates to the desktop.
  Clicking **OK** in the Open dialog imports all templates in the command templates file into LANrev Admin.
  If an imported template has the same name as an existing template, the imported template is renamed.
  Instead of using **Import Template**, you can also drag the template file into the **Command Templates** window from the desktop or double-click the file.
- **Export Template**: Choosing this command displays a standard Save dialog.
  Clicking **OK** in this dialog saves all selected templates in one command template file.
  Instead of using **Export Template**, you can also drag the templates to the desktop from the **Command Templates** window.

You can edit a template’s name or description by double-clicking it in the **Command** window’s table area.

Window Reinstallation Tasks

The **Windows Reinstallation Tasks** command opens the **Windows Reinstallation Tasks** window that lists all Windows reinstallation commands that have been sent to a LANrev PXE server or a FOG server.



This group is empty because no items match its selection criteria.

Displaying LANrev reinstallation tasks: 0 of 0 records selected

The window lists all issued reinstallation tasks for Windows target computers (that is, tasks started with the **Reinstall Windows Computer** command).

It may also include tasks executed by a FOG server that have not come from LANrev, for example, because they were entered through the FOG web interface.

Toolbar buttons

The toolbar can contain these buttons (in addition to standard elements common to toolbars in all applications):

- **Synchronize Records**: Clicking this button updates the displayed information with current data from the PXE server.

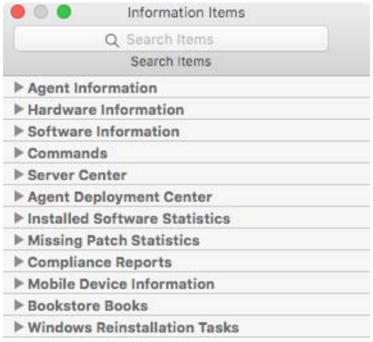
Context menu

The window’s context menu contains these commands (in addition to standard commands for all browser windows described in “Action menu” on page 521 and “Context menu” on page 524, respectively):

- **Show Computer Detail View**: This command is similar to the **Show Detail View** command standard to all browser windows.
  Choosing this command displays the selected computer’s detail information in the **Computers** window.
- **Synchronize Records**: Clicking this button updates the displayed information with current data from the PXE server.

Information Items

The **Information Items** command opens the **Information Items** window that lists all information items.



The window contains these elements:

- **Search Items**: This field lets you quickly restrict the display to information items the name of which contains the search text. The pop-up menu in the field lets you repeat recent searches.
- **Groups & Items**: A hierarchical list of information items, grouped by category.

Dragging an information item to a browser window adds a column displaying the information item to the window.

Context menu

The **Information Items** window's context menu contains these commands:

- **Copy**: This command copies the name of the current information item. It has the same effect as the **Copy** command from the **Edit** menu.
- **Edit Custom Field**: This command is available only for custom information items. Choosing it lets you edit the selected custom information item in the **Custom Information Field** dialog.
  A custom information item can also be edited by double-clicking in the **Information Items** window.

Activity

The **Activity** command opens the **Activity** window that displays the progress of asynchronous VPP operations, like assigning or revoking of VPP licenses.

The **Activity** window opens automatically whenever an asynchronous action is initiated. It displays any actions in progress, with an individual progress bar for each action. Completed actions are automatically removed from the window.

Any errors during these actions are displayed in the Notification Center.

User windows

The bottom part of the menu contains all browser windows and command dialogs that you have opened. If no such window has yet been opened, this section is not displayed.

Chapter 17 *Help menu*

The **Help** menu lets you access the LANrev online help:

- **Search** (page 515)
- **LANrev Admin Help** (page 515)
- **HEAT Software Global Support** (page 515)
- **Resource Center** (page 515)
- **Knowledge Base** (page 515)
- **Customer Forum** (page 516)
- **Release Notes** (page 516)
- **HEAT Software Web Site** (page 516)
- **Acknowledgements** (page 516)

Search

The **Search** command and text field lets you search both LANrev's menu commands and its online help.

Entering text into the text field at the right of the menu command displays all menu commands that contain that text and the most relevant help topics.

LANrev Admin Help

The **LANrev Admin Help** command opens LANrev Admin's online help.

HEAT Software Global Support

The **HEAT Software Global Support** command opens the main HEAT support web page in your default web browser.

Resource Center

The **Resource Center** command opens the main HEAT support web page in your default web browser.

Knowledge Base

The **Knowledge Base** command opens the online LANrev knowledge base in your default web browser.

Customer Forum

The **Customer Forum** command opens the online LANrev discussion forums in your default web browser.

Release Notes

The **Release Notes** command opens the release notes for the installed release of LANrev in a PDF reader.

HEAT Software Web Site

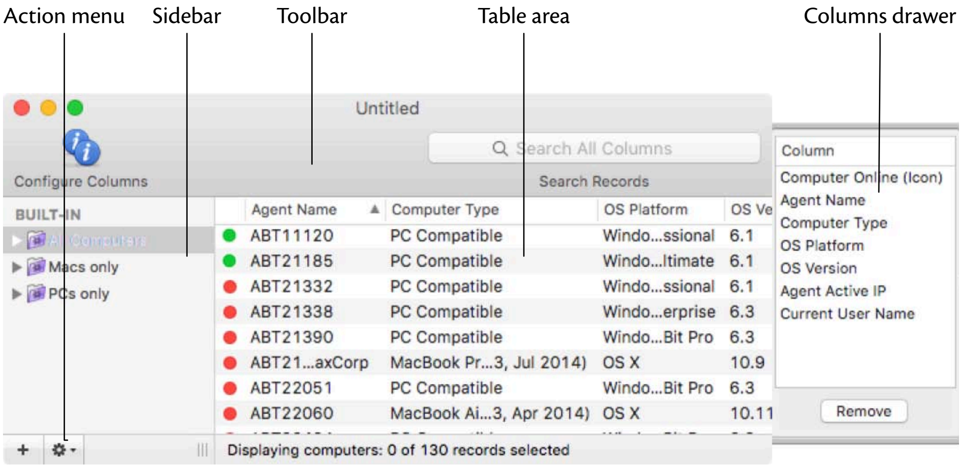
The **HEAT Software Web Site** command opens the main HEAT Software page in your default web browser.

Acknowledgements

The **Acknowledgements** command opens a window displaying the acknowledgements for code incorporated into LANrev and other contributions.

Chapter 18 Browser windows

Browser windows display the contents of LANrev's internal database in a configurable table view.



	Agent Name ▲	Computer Type	OS Platform	OS Ve
●	ABT11120	PC Compatible	Windo...ssional	6.1
●	ABT21185	PC Compatible	Windo...ltimate	6.1
●	ABT21332	PC Compatible	Windo...ssional	6.1
●	ABT21338	PC Compatible	Windo...erprise	6.3
●	ABT21390	PC Compatible	Windo...Bit Pro	6.3
●	ABT21...axCorp	MacBook Pr...3, Jul 2014)	OS X	10.9
●	ABT22051	PC Compatible	Windo...Bit Pro	6.3
●	ABT22060	MacBook Ai...3, Apr 2014)	OS X	10.11

Displaying computers: 0 of 130 records selected

Browser windows contain these elements:

- **Toolbar** (page 518)
- **Status bar** (page 519)
- **Table columns** (page 520)
- **Drawer** (page 520)
- **Sidebar** (page 521)
- **Action menu** (page 521)
  - **New Group** (page 522)
  - **New Smart Group** (page 522)
  - **New Category** (page 523)
  - **Rename Group** (page 523)
  - **Edit Smart Group** (page 523)
  - **Remove Group** (page 524)
  - **Remove Category** (page 524)
  - **Remove from Group** (page 524)
- **Context menu** (page 524)
  - **Copy** (page 525)
  - **Copy "<information item>"** (page 525)
  - **New Smart Group from "<information item>"** (page 525)
  - **Make Group from Selected Computers** (page 525)
  - **Show Detail View** (page 526)
  - **Synchronize Records** (page 526)
  - **Enter Custom Field Data** (page 526)
  - **Remove from Server** (page 527)
  - **Remove Inventory Data** (page 527)
  - **Computer Tracking** (page 528)
  - **Remove from Group** (page 528)
  - **Remote Control** (page 528)
  - **View in Separate Window** (page 529)
  - **Open in Preview** (page 530)
  - **Show FileVault Recovery Key** (page 530)

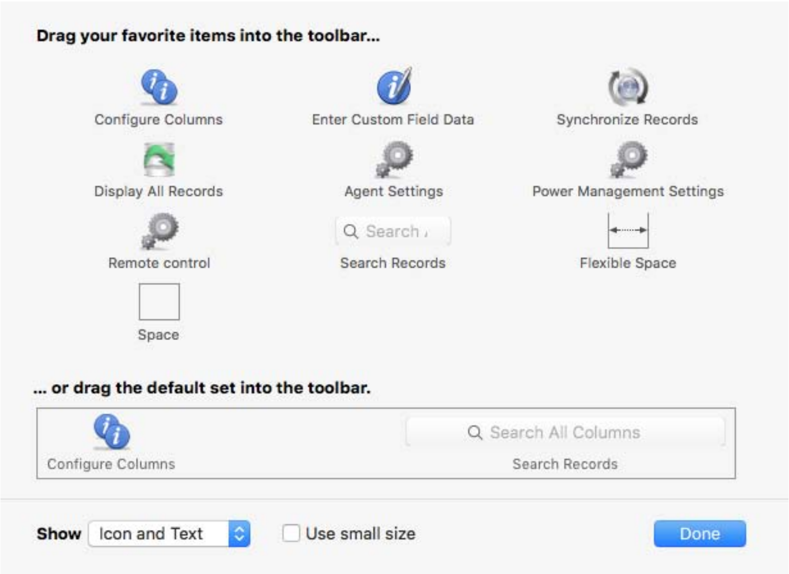
The + button in the lower left-hand corner is not separately described. Clicking it creates a new smart group as if you had chosen **New Smart Group**; clicking it with the Option key held down acts like you had chosen **New Group**.

Toolbar

Browser windows have toolbars that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398.

The toolbar can contain these elements (some commands omitted in the screenshot):



Show Icon and Text

□ Use small size

The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** through **Print**).

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Enter Custom Field Data

The **Enter Custom Field Data** button lets you edit the content of the custom information fields or the selected devices.

It has the same effect as the **Enter Custom Field Data** command described on page 526.

Synchronize Records

The **Synchronize Records** button downloads updated information for the selected records from the server to which you are connected.

It has the same effect as the **Synchronize Selected Records** command described on page 481.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

It has the same effect as the **Display All Records** command described on page 397.

Command buttons

For each command from the **Commands** menu (except those that are only usable in the **Commands** window), there is one button. Clicking that button has the same effect as choosing the corresponding command from the **Commands** menu.

Search Records

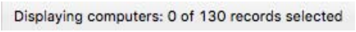
The **Search Records** field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Pressing Return executes the search.

Status bar

Browser windows have status bars displaying information on the state of the window.

The status bar displays the number of records currently shown in the window. It also shows the kind of information displayed:



Displaying computers: 0 of 130 records selected

If the window does not display all records from the server database table (because the number of records exceeds the initial display limit set in the **Preferences** dialog’s **General** pane), this is indicated with the addition “(more…)” after the record count in the status bar. Clicking **more** displays the additional records.

If data on an individual computer is displayed (as described in “Sidebar” on page 521), the status bar also indicates how old the currently shown information is.

Table columns

The columns displayed in browser windows are completely configurable.

The columns display information items from the **Agent Information**, **Hardware Information**, **Software Information**, **Command History**, and **License Status per Agent** categories. Information items are described in “Information items” on page 831.

Columns can be dragged around in the window to be rearranged. Dragging an item from the **Information Items** window into a browser window creates a new column at the right of the table.

Deleting columns is possible in the **Columns** drawer, in addition to rearranging and adding columns. This is described below.

Double-clicking a column title in the browser window sorts the table by that column or, if the column is already a sort column, reverses the sort order. If there already are sorting columns, double-clicking a new column makes it a subsorting column. Double-clicking while holding down the Command key unsorts a column.

If individual computers are selected in the sidebar (see below), the columns are hidden and information on the selected computer is displayed.

Drawer

Browser windows contain a drawer for rearranging the columns in the window.

It is opened by choosing **Configure Columns** from the **View** menu.

The drawer contains the titles of all columns that are displayed in the browser window.

The order of the column titles is the same as that of the columns in the table in the window. Dragging a column title to another location in the drawer repositions the column in the window.

Dragging an information item into the drawer adds a corresponding column to the window. You can also drag columns from one Columns drawer to another or transfer them by copying and pasting.

Clicking the **Remove** button deletes the selected columns from the window.

Sidebar

Browser windows contain a sidebar with a number of categories and predefined smart groups to which more can be added.

Categories

New browser windows contain the **Built-in** category. (Predefined windows may contain other or additional categories.) More categories can be added using the **New Category** context menu command.

Categories group other categories, groups, and smart groups very much like folders in a file system.

Smart groups

- **All Computers**: All computers listed in the Computers table in the LANrev database.
- **Macs only**: All macOS computers contained in the database.
- **PCs only**: All Windows computers contained in the database.

Additional smart groups and groups can be added using the **New Group** and **New Smart Group** commands in the action context menu.

NOTE Smart groups are defined by selection criteria, dynamically displaying computers that match the criteria at the moment. Groups are folder-like, containing the computers that have been put into them manually.

You can rearrange smart groups by dragging them to the desired place in the list.

Details

The smart groups can be expanded to reveal the computers contained in them. A computer can be clicked to reveal basic information on that computer in the table area.

Expanding a computer displays a range of categories in the sidebar. Clicking on of the categories displays information from that category for the respective computer in the table area.

Details can be displayed in the same way for computers in user-created groups and smart groups.

Action menu

The action menu of browser windows contains commands for managing groups and smart groups.

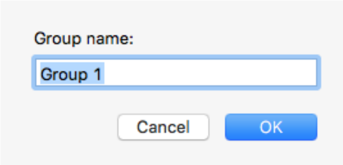
The commands are described in detail in the following sections.

- “New Group” on page 522
- “New Smart Group” on page 522
- “New Category” on page 523
- “Rename Group” on page 523
- “Rename Category” on page 523
- “Edit Smart Group” on page 523
- “Remove Group” on page 524
- “Remove Category” on page 524
- “Remove from Group” on page 524

New Group

The **New Group** command creates a new (non-smart) group.

Choosing the command opens the **New Group** dialog:



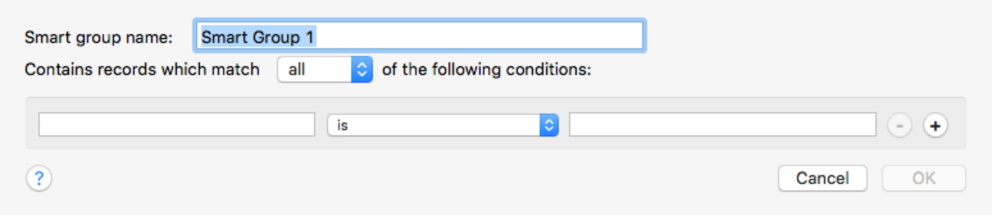
Group name: Group 1

The dialog contains a field for naming the new group.

New Smart Group

The **New Smart Group** command creates a new smart group.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Group 1

Contains records which match all of the following conditions:

is

The dialog contains these elements:

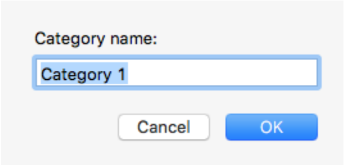
- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand text field lets you specify an information item on which records are to be matched.
  - The pop-up menu in the middle contains the possible comparison operators.

- The right-hand text field lets you specify the value to compare record values against.
- The **+** and **–** buttons let you add new conditions or remove existing ones.

New Category

The **New Category** command creates a new category in the browser window's sidebar.

Choosing the command opens the **New Category** dialog:



Category name:

Category 1

The dialog contains a field for editing the name of the category.

Rename Group

The **Rename Group** command renames an existing smart or non-smart group.

Choosing the command lets you edit the name of the group (inline in the window's sidebar).

If a category is selected, this command is renamed **Rename Category**.

Rename Category

If a category in the sidebar is selected, the **Rename Group** command is renamed **Rename Category**.

Choosing the command is similar to choosing **Rename Group**; see there for details.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the **Smart Group** dialog, described in **New Smart Group**, above.

Remove Group

The **Remove Group** command deletes the selected smart or non-smart groups.

Choosing the command deletes the selected groups. A confirmation alert is displayed first. The computers listed in the groups is not deleted from the database.

If a category is selected, this command is renamed **Remove Category**.

Remove Category

If a category in the sidebar is selected, the **Remove Group** command is renamed **Remove Category**.

Choosing the command is similar to choosing **Remove Group**; see there for details.

Remove from Group

The **Remove from Group** command deletes the selected computers from the displayed group.

It is not available when a smart group is being displayed.

Context menu

The context menu of browser windows contains commands from the **Commands** menu. In addition, it contains a number of specific commands:

- "Copy" on page 525
- "Copy "<information item>"" on page 525
- "New Smart Group from "<information item>"" on page 525
- "Make Group from Selected Computers" on page 525
- "Show Detail View" on page 526
- "Synchronize Records" on page 526
- "Remove from Server" on page 527
- "Remove Inventory Data" on page 527
- "Computer Tracking" on page 528
- "Remove from Group" on page 528
- "Remote Control" on page 528
- "View in Separate Window" on page 529
- "Open in Preview" on page 530
- "Show FileVault Recovery Key" on page 530

For information on the rest of the commands in the context menu, see "Commands menu" on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

In the **Computer Tracking** section of a computer's detail view, you can use **Copy** to copy a screenshot.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 481.

Copy "<information item>"

The **Copy "<information item>"** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (for example, **Copy "Computer Type"**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Group from "<information item>"

The **New Smart Group from "<information item>"** command lets you create a smart group with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

Make Group from Selected Computers

The **Make Group from Selected Computers** command lets you create a smart group with prefilled criteria.

Choosing the command creates a new group from the selected computers. A dialog is displayed in which you must give the group a name; when you close the dialog, the group is added to the sidebar.

Show Detail View

The **Show Detail View** command displays the detailed information for the currently selected computer.

It has the same effect as the **Details** command described on page 396.

Synchronize Records

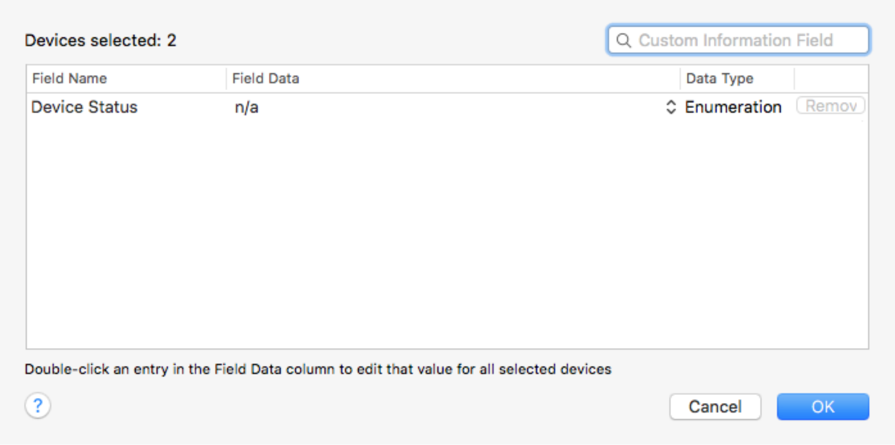
The **Synchronize Records** command downloads updated information for the selected records from the server to which you are connected.

It has the same effect as the **Synchronize Selected Records** command described on page 481.

Enter Custom Field Data

The **Enter Custom Field Data** command lets you edit the content of manual custom information fields for multiple computers in one step.

Choosing the command opens the **Enter Custom Field Data** dialog:



Devices selected: 2

Field Name	Field Data	Data Type	
Device Status	n/a	Enumeration	Remov

Double-click an entry in the Field Data column to edit that value for all selected devices

The dialog contains a list of available manual custom information fields.

Clicking one of the fields’ **Field Data** column lets you edit the content of that field for all selected computers.

Clicking the **Remove** button removes the field content from all selected computers.

Only fields that are checked in the **Modified** column are modified when you click OK.

NOTE The **Modified** column is not displayed if only one computer was selected before the dialog was opened.

Remove from Server

The **Remove from Server** command deletes the selected records from the server. A confirmation alert is displayed first. If licenses are still assigned to the devices whose records you are removing, an alert is also displayed.

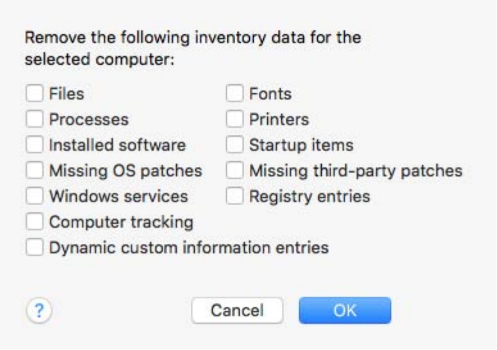
NOTE If a computer is deleted from the server, it may be automatically reappear at a later time if it is still present in the network and LANrev Agent is running on it.

NOTE The **Remove from Server** command can be used for computer records only by administrators with the **Remove Computer Records** right. See "New Administrator" on page 758 for details.

Remove Inventory Data

The **Remove Inventory Data** command lets you remove data related to the selected computers from LANrev's databases. It is useful for deleting extensive information that was needed only for a specific purpose, speeding up LANrev processes.

Choosing the command opens the **Remove Inventory Data** dialog:



Remove the following inventory data for the selected computer:

□ Files
□ Processes
□ Installed software
□ Missing OS patches
□ Windows services
□ Computer tracking
□ Dynamic custom information entries

□ Fonts
□ Printers
□ Startup items
□ Missing third-party patches
□ Registry entries

The checkboxes allow you to specify the data to be deleted.

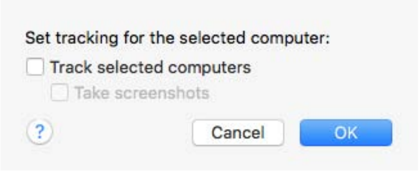
Clicking **OK** deletes all data on the server of the marked types which relate to the selected computers.

NOTE The **Remove Inventory Data** command can be used for computer records only by administrators with the **Remove Inventory Data** right. See "New Administrator" on page 758 for details.

Computer Tracking

The **Computer Tracking** command lets you activate or deactivate tracking for the selected computers and specify tracking options.

Choosing the command opens the **Computer Tracking** dialog:



Set tracking for the selected computer:

□ Track selected computers

□ Take screenshots

The dialog contains these options:

- **Track selected computers**: Check this option to activate tracking the computers; uncheck it to stop tracking them.
- **Take screenshots**: If this option is checked, the tracked computers take screenshots and transmit them to LANrev Server whenever they send a 'heartbeat' (for example, when the network connection is changed, when a user logs in or out, when the computer is woken up, or in regular intervals otherwise).

NOTE The **Computer Tracking** command is available only to administrators with the **Change Computer Tracking** right. See "New Administrator" on page 758 for details.

Remove from Group

The **Remove from Group** command deletes the selected computers from the displayed group or computer group.

It is not available when a smart group is being displayed.

Remote Control

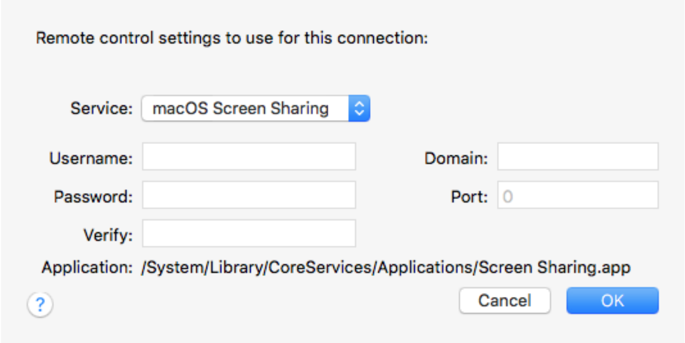
The **Remote Control** command lets you remotely control the selected client computers using screen sharing software.

Choosing the command launches a local remote control software – such as LANrev Remote, Timbuktu, macOS Screen Sharing, MS

Remote Desktop, or a VNC application – and connects it to the selected client computer.

Details of the process are described in “Remotely controlling computers” on page 151.

A screen sharing client for the application must be available on the remote computer. If LANrev does not detect any such client or if you hold down the Option key while choosing the command, the **Remote Control Settings** dialog opens:



Remote control settings to use for this connection:

Service: macOS Screen Sharing

Username:

Domain:

Password:

Port: 0

Verify:

Application: /System/Library/CoreServices/Applications/Screen Sharing.app

The dialog contains these elements. Fields that do not apply to the chosen service are disabled:

- **Service**: The desired protocol to use for remotely controlling the target computer.
- **Username**: The user account for the remote control software on the client computers.
- **Password** and **Verify**: The password for the specified account. *Note: Some VNC applications do not support being supplied with a username and password when they are launched; when you are using these applications, you must enter a username and password within the application, even if you have already supplied both in LANrev. This is a limitation of these applications, not of LANrev.*
- **Application**: The local application that will be used to connect to the client. If “n/a” is displayed, no application for the selected protocol was found.
- **Select**: Click this button to choose the desired application to use.
- **Domain**: The Window networking domain to be used for accessing client computers.
Note: Some VNC applications do not support domains.
- **Port**: The network port on which to contact the remote control software on the client computers.

View in Separate Window

The **View in Separate Window** command opens the selected image in its own window.

The command is available only in the context menu for a screenshot in the **Computer Tracking** section of a computer’s detail view.

Open in Preview

The **Open in Preview** command opens the selected image in Apple’s Preview application.

The command is available only in the context menu for a screenshot in the **Computer Tracking** section of a computer’s detail view.

Show FileVault Recovery Key

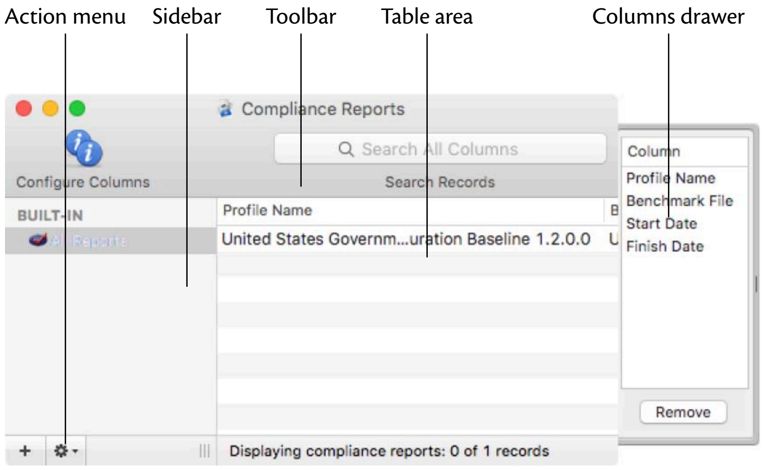
The **Show FileVault Recovery Key** command lets you retrieve the recovery key for the FileVault of a managed computer, provided that the key was stored on the LANrev server through the **Save personal FileVault recovery key on the LANrev server** option, as described in “macOS profiles” on page 668.

Choosing the command displays a dialog in which the key is shown.

Chapter 19 Compliance Report window

The **Compliance Report** window displays the details of an USGCB SCAP compliance report: The tested computers, their individual results and compliance results, item-by-item breakdowns, and summaries by item across all computers.

The window is opened by double-clicking a report in the **Compliance Reports** window.



Displaying compliance reports: 0 of 1 records

The elements of a **Compliance Report** window are described below:

- **Toolbar** (page 532)
- **Information panel** (page 532)
- **Table columns** (page 532)
- **Sidebar** (page 532)
- **Action and context menus** (page 533)
  - **Copy** (page 533)
  - **Copy "<information item>"** (page 533)
  - **Show Details for This Computer** (page 534)
  - **Show Details for This Scoring Item** (page 534)
  - **New Smart Report Summary Group** (page 534)
  - **New Smart Report Item Summary Group** (page 535)
  - **New Smart Report Details Group** (page 535)
  - **New Category** (page 536)
  - **Rename Group** (page 536)
  - **Rename Category** (page 536)
  - **Edit Smart Group** (page 537)
  - **Remove Smart Group** (page 537)
  - **Remove Category** (page 537)

The + button in the lower left-hand corner is not separately described. Clicking it creates a new queue smart group as if you had chosen **New Smart Report Item Summary Group**; clicking it with the Option key held down acts like you had chosen **New Smart Report Summary Group**.

Toolbar

The **Compliance Report** window has a toolbar that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar can contain the same elements as browser window toolbars, described in “Toolbar” on page 518.

Information panel

The information panel at the top of a **Compliance Report** window displays information on the report itself.

Clicking the triangle ▶ at the left of the panel left expands and collapses it.

In its collapsed state, it displays the name of the report as well as the profile and the benchmark file used.

In its expanded state, it displays additional information on the report. These information items are described in “Reports” on page 893.

Table columns

The columns displayed in a **Compliance Report** window are described in “Compliance Reports” on page 892.

Sidebar

The **Compliance Report** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

- **Summary – All Computers**: Summary information on all computers for which the report has been completed.
- **Summary by Scored Item**: Summary information on all score items, showing how the compliance for each item was across all tested computers.
  Expand the category and click any score item to display the individual results of each computer.
- **Details – All Computers**: Detailed information for one computer on each score item.
  Expand the category and click the desired computer in the sidebar to display its details.

- **Pending Reports**: All reports that are in the process of being collected.
- **Completed Reports**: All reports that have been completely gathered.

Any additional smart groups that you define are displayed below these groups.

Action and context menus

The action and the context menus of a **Compliance Report** window contains commands for managing reports and smart groups.

The commands are described in detail in the following sections.

- "Copy" on page 533
- "Copy "<information item>"" on page 533
- "Show Details for This Computer" on page 534
- "Show Details for This Scoring Item" on page 534
- "New Smart Report Summary Group" on page 534
- "New Smart Report Item Summary Group" on page 535
- "New Smart Report Details Group" on page 535
- "New Category" on page 536
- "Rename Group" on page 536
- "Rename Category" on page 536
- "Edit Smart Group" on page 537
- "Remove Smart Group" on page 537
- "Remove Category" on page 537

For information on the rest of the commands in the context menu, see "Commands menu" on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 392.

Copy "<information item>"

The **Copy "<information item>"** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (for example, **Copy "Command Name"**).

If multiple records are selected, the contents of the information item from all of them are copied.

Show Details for This Computer

The **Show Details for This Computer** command displays the detailed report scores for the computer on which you click.

Using this command is the same as selecting the computer in the sidebar under **Details – All Computers**.

Show Details for This Scoring Item

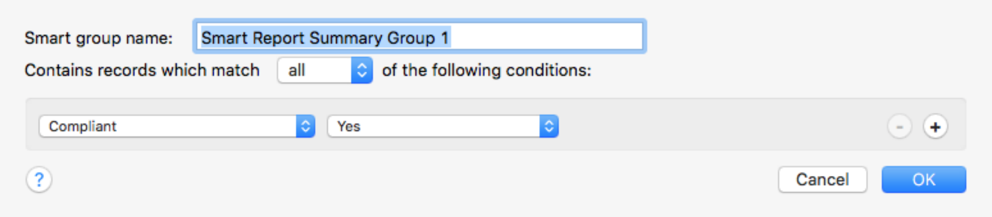
The **Show Details for This Scoring Item** command displays the detailed report scores for the scoring item on which you click.

Using this command is the same as selecting the scoring item in the sidebar under **Summary by Scored Item**.

New Smart Report Summary Group

The **New Smart Report Summary Group** command lets you create a smart group that displays all report summaries meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Report Summary Group 1

Contains records which match all of the following conditions:

Compliant Yes

The dialog contains these elements:

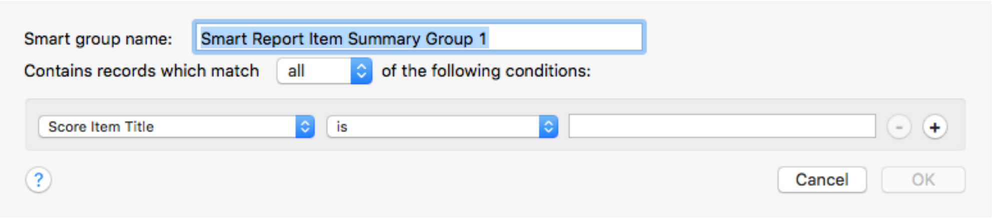
- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Computer Summary” on page 893.
  - The second pop-up menu contains the possible comparison operators.

- The right-hand text field lets you specify the value to compare record values against.
- The **+** and **–** buttons let you add new conditions or remove existing ones.

New Smart Report Item Summary Group

The **New Smart Report Item Summary Group** command lets you create a smart group that displays all score item summaries meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Report Item Summary Group 1

Contains records which match all of the following conditions:

Score Item Title | is

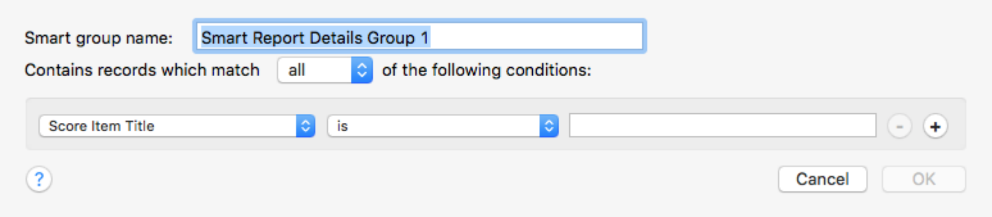
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Item Summary” on page 893.
  - The second pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Smart Report Details Group

The **New Smart Report Details Group** command lets you create a smart group that displays all report details on individual computers meeting criteria you specify.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Report Details Group 1

Contains records which match all of the following conditions:

Score Item Title is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Score Items” on page 894.
  - The second pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Category

The **New Category** command creates a new category in the window’s sidebar.

Rename Group

The **Rename Group** command renames an existing smart group.

Choosing the command lets you edit the name of the group (inline in the window’s sidebar).

If a category is selected, this command is renamed **Rename Category**.

Rename Category

If a category in the sidebar is selected, the **Rename Group** command is renamed **Rename Category**.

Choosing the command is similar to choosing **Rename Group**; see there for details.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the specification dialog for the type of smart group that is selected. For details, see the command for creating that type of smart group:

- “New Smart Report Summary Group” on page 534
- “New Smart Report Item Summary Group” on page 535
- “New Smart Report Details Group” on page 535

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Remove Category

If a category in the sidebar is selected, the **Remove Smart Group** command is renamed **Remove Category**.

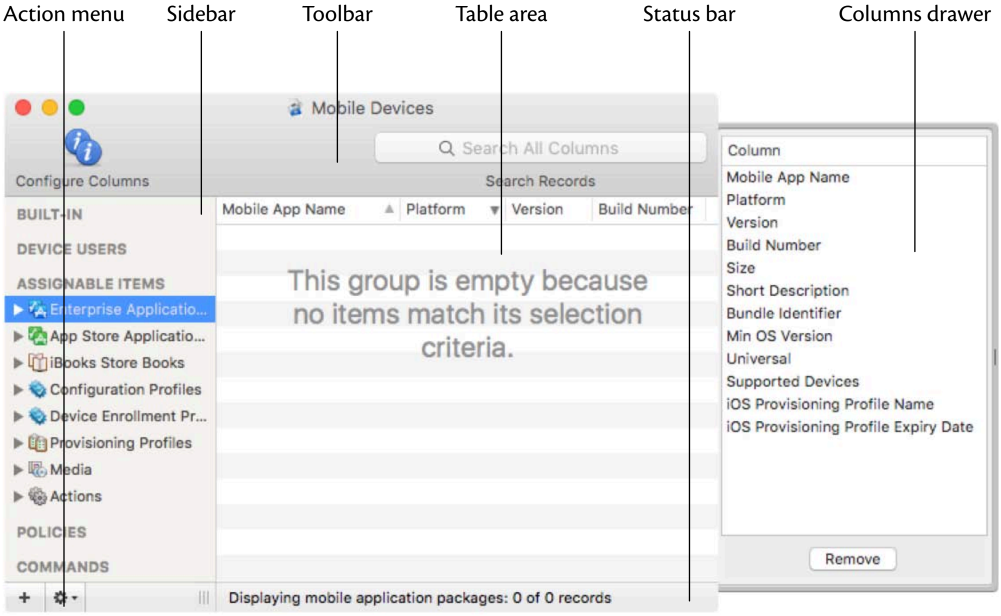
Choosing the command is similar to choosing **Remove Smart Group**; see there for details.

Chapter 20 *Mobile Devices*

The **Mobile Devices** window displays information on mobile devices enrolled in the MDM server that is specified in the server settings. (See “MDM” on page 787 for more information.) It also displays limited information on iOS devices that are managed through a copy of iTunes installed on any administered computer.

NOTE Administrators can see in this window only information about devices to which they have been assigned, unless the **Can manage all devices** option has been activated for their account.

The window is opened by choosing the **Mobile Devices** command from the **Window** menu.



This group is empty because no items match its selection criteria.

Displaying mobile application packages: 0 of 0 records

The elements of the **Mobile Devices** window are described below:

- **Toolbar** (page 544)
- **Table columns** (page 546)
- **Sidebar** (page 546)
- **Action menu** (page 550)
  - **Mobile Applications** (page 552)
    - **New Enterprise Application Package** (page 553)
    - **New iOS App Store Application Package** (page 554)
    - **New Google Play Application Package** (page 558)
    - **Duplicate Application Package** (page 559)
    - **New Smart Group: Enterprise Application Packages** (page 559)
    - **New Smart Group: App Store Application Packages** (page 559)
    - **New Smart Group: iOS Provisioning Profiles** (page 559)

- **New Command History Smart Group from “<information item>”** (page 610)
- **New Policy with Selected Devices** (page 611)
- **Install Configuration Profile** (page 611)
- **Install Provisioning Profile** (page 611)
- **Install Application** (page 611)
- **Install Media File** (page 611)
- **Change Application Configuration** (page 611)
- **Validate Managed Applications** (page 611)
- **Validate Selected Applications** (page 612)
- **Issue Device Lock** (page 612)
- **Issue Clear Passcode** (page 612)
- **Issue Clear Restrictions Passcode** (page 612)
- **Erase Device** (page 612)
- **Set Roaming Options** (page 612)
- **Send Message to Device** (page 612)
- **Set Wallpaper** (page 613)
- **Install iOS Update** (page 613)
- **Set Device Name** (page 613)
- **Request AirPlay Mirroring** (page 613)
- **Stop AirPlay Mirroring** (page 613)
- **Change Personal HotSpot State** (page 613)
- **Enable Attention Mode** (page 614)
- **Disable Attention Mode** (page 614)
- **Set Lost Mode** (page 614)
- **Set Organization Information** (page 614)
- **Set Activation Lock Options** (page 614)
- **Enable Activation Lock** (page 614)
- **Remove Activation Lock** (page 614)
- **Show Activation Lock Bypass Code** (page 614)
- **Log Out User** (page 614)
- **Delete User Data** (page 615)
- **Set Passcode Lock Grace Period** (page 615)
- **Configure Diagnostic Data Transmission** (page 616)
- **Delete Application** (page 616)
- **Update Device Information** (page 617)
- **Make Device Contact Server** (page 617)
- **Remote Control** (page 617)
- **Create KNOX Workspace** (page 617)
- **Remove KNOX Workspace** (page 617)
- **Lock KNOX Workspace** (page 617)
- **Unlock KNOX Workspace** (page 617)
- **Reset KNOX Workspace Password** (page 618)
- **Register Device User in VPP** (page 618)
- **Send VPP Invitation** (page 619)
- **Retire Device Users from VPP** (page 621)
- **Assign Application Licenses to Device Users** (page 621)
- **Assign Application Licenses to Devices** (page 622)
- **Revoke Application Licenses** (page 624)
- **Convert Application Licenses from Users to Devices** (page 624)
- **Assign Book Licenses to Device Users** (page 626)
- **Assign Book Licenses to Devices** (page 627)
- **Remove Users from Server** (page 627)
- **Register Users in VPP** (page 627)

- **Retire Users from VPP** (page 627)
- **Assign Device Enrollment Profile** (page 627)
- **Unassign Device Enrollment Profile** (page 628)
- **Reload Device Enrollment Data** (page 629)
- **Configure Devices for Current Classroom Setup** (page 629)
- **Manage Personal Device Assignment** (page 629)
- **Delete Profile** (page 629)
- **Show Detail View** (page 629)
- **Create Home Screen Layout Configuration Profile** (page 630)
- **Synchronize Records** (page 630)
- **Enter Custom Field Data** (page 630)
- **Import Custom Field Data** (page 630)
- **Ignore Devices** (page 631)
- **Reset All Ignored Devices** (page 631)
- **Re-execute All Actions for This Device** (page 631)
- **Re-execute This Action for This Device** (page 631)
- **Retry All Failed Profiles** (page 631)
- **Retry All Failed Applications** (page 632)
- **Retry All Failed Books** (page 632)
- **Remove from Group** (page 632)
- **Remove from Policy** (page 632)
- **Track Device** (page 632)
- **Get Device Geolocation** (page 632)
- **Reset Tracking Passphrase** (page 633)
- **Show Location on Google Maps** (page 633)
- **Show Location on Bing Maps** (page 633)
- **Set Device Ownership** (page 633)
- **Set Enrollment User** (page 634)
- **Update AD User Information** (page 634)
- **Send Re-enrollment Message to Device** (page 634)
- **Update Installed Application Statistics** (page 635)
- **Show User Details** (page 635)
- **Show Mobile Application Package Details** (page 635)
- **New Mobile Application Package** (page 636)
- **New iOS App Store Application Package** (page 636)
- **New Google Play Application Package** (page 636)
- **Edit Mobile Application Package** (page 636)
- **Duplicate Mobile Application Package** (page 636)
- **Remove Mobile Application Package** (page 636)
- **Assign Application Licenses to Users** (page 637)
- **Revoke Application Licenses** (page 638)
- **Show Book Details** (page 638)
- **New iBooks Book** (page 639)
- **Edit Book** (page 639)
- **Duplicate Book** (page 639)
- **Remove Book** (page 639)
- **Show Configuration Profile Details** (page 640)
- **New Configuration Profile** (page 640)
- **Edit Configuration Profile** (page 640)
- **Remove Configuration Profile** (page 640)
- **Remove Configuration Profile from Policy** (page 640)
- **Show Device Enrollment Profile Details** (page 640)
- **New Device Enrollment Profile** (page 640)

- **Edit Device Enrollment Profile** (page 640)
- **Duplicate Device Enrollment Profile** (page 641)
- **Remove Device Enrollment Profile** (page 641)
- **Show Provisioning Profile Details** (page 641)
- **Show Media File Details** (page 641)
- **Set Availability Time** (page 642)
- **New Media File** (page 643)
- **Edit Media File** (page 643)
- **Remove Media File** (page 643)
- **Show Action Details** (page 643)
- **Duplicate Action** (page 643)
- **Edit Action** (page 643)
- **Remove Action** (page 643)
- **Re-execute This Action for All Devices** (page 644)
- **Re-execute This Action for This Policy** (page 644)
- **New Send Message Action** (page 644)
- **New Send E-Mail Action** (page 644)
- **New Send SMS (Text Message) Action** (page 644)
- **New Set Roaming Options Action** (page 644)
- **New Set Activation Lock Options Action** (page 645)
- **New Enable Activation Lock Action** (page 645)
- **New Set Wallpaper Action** (page 645)
- **New Set Device Name Action** (page 645)
- **New Set Custom Field Value Action** (page 645)
- **New Install iOS Update Action** (page 645)
- **New Validate Applications Action** (page 645)
- **New Update Device Information Action** (page 645)
- **New Set Attention Mode Action** (page 646)
- **New Set Lost Mode Action** (page 646)
- **New Set Passcode Lock Grace Period Action** (page 646)
- **New Configure Diagnostic Data Transmission Action** (page 646)
- **New Freeze Device Action** (page 646)
- **New Clear Passcode Action** (page 646)
- **New Register User in VPP Action** (page 646)
- **New Send VPP Invitation Action** (page 646)
- **New Retire User from VPP Action** (page 647)
- **New Remove Configuration Profile Action** (page 647)
- **New Demote to Unmanaged Device Action** (page 647)
- **New Configure Devices for Current Classroom Setup Action** (page 647)
- **Change Action Schedule** (page 647)
- **Remove Action from Policy** (page 648)
- **Show Policy Members** (page 648)
- **Remove Policy** (page 648)

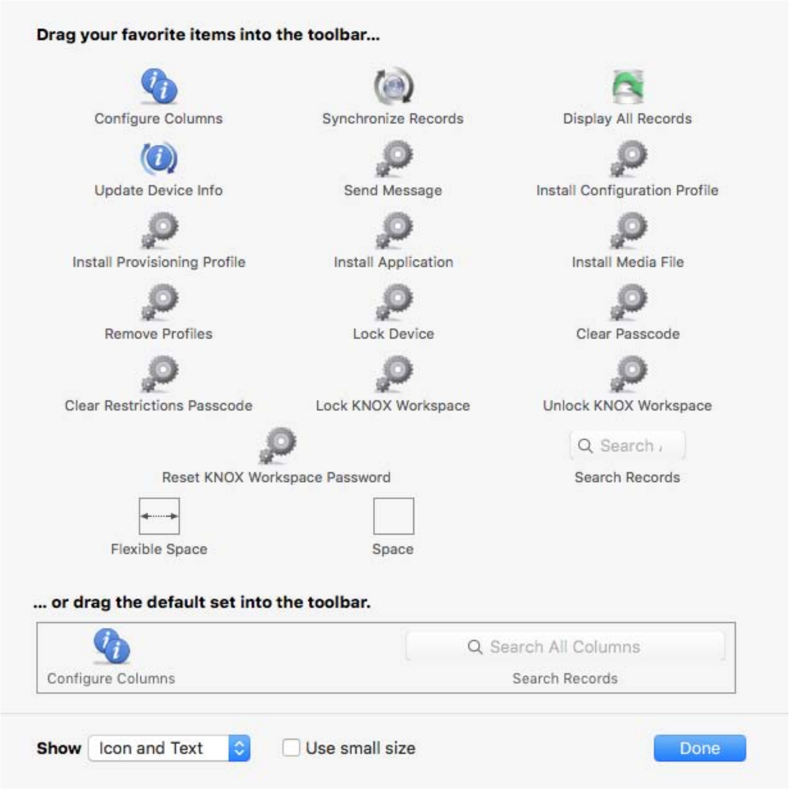
The + button in the lower left-hand corner is not separately described. Clicking it creates an item, depending on the kind of object currently selected in the sidebar.

Toolbar

The **Mobile Devices** window has a toolbar that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar can contain these elements:



Drag your favorite items into the toolbar...

... or drag the default set into the toolbar.

Show: Icon and Text

□ Use small size

The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** through **Customize**).

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Synchronize Records

Clicking the **Synchronize Records** button synchronizes the display in the **Mobile Devices** window with the report data on the server.

It has the same effect as the **Synchronize Selected Records** command described on page 481.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

It has the same effect as the **Display All Records** command described on page 397.

Update Device Information

This is the **Update Device Information** command described on page 617.

Send Message

This is the **Send Message to Device** command described on page 612.

Install Configuration Profile

This is the **Install Configuration Profile** command described on page 459.

Install Provisioning Profile

This is the **Install Provisioning Profile** command described on page 460.

Install Application

This is the **Install Application** command described on page 461.

Remove Profiles

This is the **Install Application** command described on page 461.

Lock Device

This is the **Issue Device Lock** command described on page 464.

Clear Passcode

This is the **Issue Clear Passcode** command described on page 465.

Clear Restrictions Passcode

This is the **Issue Clear Restrictions Passcode** command described on page 466.

Lock KNOX Workspace

This is the **Lock KNOX Workspace** command described on page 477.

Unlock KNOX Workspace

This is the **Unlock KNOX Workspace** command described on page 477.

Reset KNOX Workspace

This is the **Reset KNOX Workspace Password** command described on page 477.

Search Records

The **Search Records** field lets you quickly restrict the display to commands that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Pressing Return executes the search.

Table columns

The columns displayed in a **Mobile Devices** window are described in “Mobile Device Information” on page 894.

Sidebar

The **Mobile Devices** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

Built-in

- **All mobile devices**: All found managed mobile devices. Devices that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iOS devices**: All found mobile devices running iOS. Any devices that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPhones**: All found iPhones. Any iPhones that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPads**: All found iPads. Any iPads that have been removed with the **Ignore Devices** context menu command are not listed.
- **All iPod touch devices**: All found iPod touch devices. Any iPods that have been removed with the **Ignore Devices** context menu command are not listed.
- **All Android devices**: All found mobile devices running Android.

- **All Android phones**: All found mobile phones running Android.
- **All Android tablets**: All found tablets running Android.
- **All Windows Phone devices**: All found mobile devices running Windows Phone.
- **All installed applications**: All applications that were found on the listed devices. No applications from devices that have been removed with the **Ignore Devices** context menu command are listed.
- **All installed provisioning profiles**: All provisioning profiles that were found on the listed devices.
- **All installed configuration profiles**: All configuration profiles that were found on the listed devices.
- **All installed certificates**: All certificates that were found on the listed devices.
- **Installed software statistics**: Summary information on the applications that were found on the mobile devices. No applications from devices that have been removed with the **Ignore Devices** context menu command are included in the summary.
  These statistics are not automatically updated. To update them, choose **Update Installed Application Statistics** from the context menu.

Device Users

All users that have enrolled with their Active Directory or Open Directory accounts that have been created in LANrev.

Each user entry in the sidebar can be expanded to list the mobile devices assigned to the user.

The users listed are the same as in the sidebar of the Server Center window, although the devices are different.

Note that local users of shared iOS devices are not listed here. To see them, expand the entry for the device in the sidebar and select the **Shared Users** category.

Assignable Items

- **Enterprise Applications**: All packages for enterprise iOS and Android apps that have been created in LANrev.
- **App Store Applications**: All packages for mobile app store apps that have been created in LANrev.
- **iBooks Store Books**: All books from the iBooks Store that have been specified in LANrev.
- **Configuration Profiles**: All configuration profiles that have been imported into LANrev. This includes EAS policies for Windows Phone.
  LANrev comes with a predefined configuration profile, “VPP Invite Web Clip”, that you can use to change the label and icon of web clips sent to users to invite them to participate in Apple’s volume purchase program, as described in “Managing VPP app codes and licenses” on page 209.

- **Device Enrollment Profiles**: All device enrollment profiles that have been created in LANrev.
- **Provisioning Profiles**: All provisioning profiles that have been assigned to applications inside LANrev.
- **Media**: All mobile media files that have been specified in LANrev.
- **Actions**: All mobile device actions that have been specified in LANrev.

Policies

All policies that have been created in LANrev plus a special policy:

- **Unmanaged devices**: All mobile devices that are found by LANrev but are not under MDM management.
  You can assign Send SMS and Send Message actions to this special policy but none of the other kinds of assignable items.
  You can use this policy, in particular, to generate notifications when one of your managed devices becomes unmanaged.

Each policy has a number of categories:

- **Enterprise Apps**: Apps developed by your organization:
  - **Auto-install**: Apps that are mandatory on the devices belonging to the policy.
  - **On-demand**: Apps that are available for installation in LANrev Apps on the devices belonging to the policy.
  - **Auto-install, Auto-remove**: Apps that are automatically installed on devices that are added to the policy and uninstalled from devices that are removed from the policy (unless the devices belong to another policy in which the app is automatically installed).
  - **On-demand, Auto-remove**: Apps that are available for installation in LANrev Apps on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the app is automatically installed).
  - **Forbidden**: Apps that may not be installed on the devices belonging to the policy.
- **App Store Applications**: Apps from an app store:
  - **Auto-install**: Apps that are mandatory on the devices belonging to the policy.
  - **On-demand**: Apps that are available for installation in LANrev Apps on the devices belonging to the policy.
  - **Auto-install, Auto-remove**: Apps that are automatically installed on devices that are added to the policy and uninstalled from devices that are removed from the policy (unless the devices belong to another policy in which the app is automatically installed).
  - **On-demand, Auto-remove**: Apps that are available for installation in LANrev Apps on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the app is automatically installed).

- **Configuration Profiles**: Configuration profiles that have been imported into LANrev. There are several subcategories:
  - **Auto-install**: Configuration profiles that are mandatory on the devices belonging to the policy.
  - **On-demand**: Configuration profiles that users of the devices belonging to the policy can install if desired.
  - **Auto-install, Auto-remove**: Configuration profiles that are automatically installed on devices that are added to the policy and uninstalled from devices that are removed from the policy (unless the devices belong to another policy in which the profile is automatically installed).
  - **Forbidden**: Configuration profiles that must not be installed on the devices belonging to the policy.
- **iBooks Store Books**: DRM-protected books from the iBooks Store. (See also “iBooks Media”, below.
  - **Auto-install**: Books that are automatically downloaded to devices that are added to the policy. They are not automatically removed when the device leaves the policy.
  - **On-demand**: Books that have been recommended for use on the devices belonging to the policy.
- **iBooks Media**: Book files that are installed in iBooks on mobile devices belonging to this policy. This category includes books that do not have DRM; for DRM-protected books, see “iBooks Store Books”, above.
  Custom books can only be installed on iOS devices running iOS 8 or above.
  - **Auto-install**: Books that are automatically downloaded to devices that are added to the policy. They are not automatically removed when the device leaves the policy.
  - **On-demand**: Books that are available for installation in iBooks on the devices belonging to the policy. They are not automatically removed when the device leaves the policy.
  - **Auto-install, Auto-remove**: Books that are automatically downloaded to devices that are added to the policy and deleted from devices that are removed from the policy (unless the devices belong to another policy in which the media files are automatically downloaded).
  - **On-demand, Auto-remove**: Books that are available for installation in iBooks on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the media files are automatically downloaded).
- **LANrev Safe Media**: Media files that are made available in LANrev Safe on mobile devices belonging to this policy.
  - **Auto-install**: Media files that are automatically downloaded to devices that are added to the policy. They are not automatically removed when the device leaves the policy.
  - **On-demand**: Media files that are available for installation in LANrev Safe on the devices belonging to the policy. They are not automatically removed when the device leaves the policy.
  - **Auto-install, Auto-remove**: Media files that are automatically downloaded to devices that are added to the policy and deleted from devices that are removed from the policy

    (unless the devices belong to another policy in which the media files are automatically downloaded).
  - **On-demand, Auto-remove**: Media files that are available for installation in LANrev Safe on the devices belonging to the policy and that are automatically removed from devices leaving the policy (unless the devices belong to another policy in which the media files are automatically downloaded).
- **Device Enrollment Profile**: The device enrollment profile that is automatically installed on all members of the policy, except for devices on which a device enrollment profile has already been installed through another policy.
  Note that, if a device belongs to multiple policies that each specify an enrollment profile, it is undefined which profile is assigned to the device. We therefore recommend that you set up your policies so that no device belongs to more than one policy with a device enrollment profile.

Commands

- **Queued Commands**: Commands issued to managed mobile devices that have not yet been reported as completed.
- **Command History**: Commands issued to managed mobile devices that have been completed, successfully or unsuccessfully.

Any additional smart groups that you define are displayed below these groups.

Action menu

The action and the context menus of the sidebar of the **Mobile Devices** window contain commands for grouping devices as well as working with applications, profiles, certificates, and policies.

The commands are described in detail in the following sections.

- “Mobile Applications” on page 552
  - “New Enterprise Application Package” on page 553
  - “New iOS App Store Application Package” on page 554
  - “New Google Play Application Package” on page 558
  - “Duplicate Application Package” on page 559
  - “New Smart Group: Enterprise Application Packages” on page 559
  - “New Smart Group: App Store Application Packages” on page 559
  - “New Smart Group: iOS Provisioning Profiles” on page 559
  - “New Smart Group: Installed Applications” on page 559
  - “New Smart Group: Installed Application Statistics” on page 559
  - “New Smart Group: Mobile Devices by Installed Software” on page 560
  - “New Smart Group: Installed iOS Provisioning Profiles” on page 560

  - “New Smart Group: Installed iOS Provisioning Profiles Statistics” on page 560
  - “New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles” on page 560
- “Configuration Profiles and Certificates” on page 560
  - “New Configuration Profile” on page 561
  - “New Smart Group: Configuration Profiles” on page 564
  - “New Smart Group: Installed Configuration Profiles” on page 564
  - “New Smart Group: Installed Configuration Profiles Statistics” on page 564
  - “New Smart Group: Mobile Devices by Installed Configuration Profiles” on page 564
  - “New Smart Group: Installed Certificates” on page 564
  - “New Smart Group: Installed Certificates Statistics” on page 565
  - “New Smart Group: Mobile Devices by Installed Certificates” on page 565
- “Media” on page 565
  - “New Media File” on page 566
  - “Duplicate Media File” on page 567
  - “New Smart Group: Media Files” on page 568
  - “New Smart Group: Installed Media Files” on page 568
  - “New Smart Group: Installed Media File Statistics” on page 568
  - “New Smart Group: Mobile Devices by Installed Media Files” on page 568
- “Books” on page 568
  - “New iBooks Book” on page 569
  - “Duplicate iBooks Book” on page 569
  - “New Smart Group: iBooks Books” on page 569
- “Actions” on page 570
  - “New Send Message Action” on page 571
  - “New Send E-Mail Action” on page 572
  - “New Send SMS (Text Message) Action” on page 573
  - “New Set Roaming Options Action” on page 574
  - “New Set Activation Lock Options Action” on page 575
  - “New Enable Activation Lock Action” on page 576
  - “New Set Wallpaper Action” on page 577
  - “New Update Device Information Action” on page 582
  - “New Set Attention Mode Action” on page 583
  - “New Set Lost Mode Action” on page 584
  - “New Freeze Device Action” on page 587
  - “New Register User in VPP Action” on page 588
  - “New Send VPP Invitation Action” on page 590
  - “New Retire User from VPP Action” on page 592
  - “New Remove Configuration Profile Action” on page 593
  - “New Demote to Unmanaged Device Action” on page 593
  - “New Configure Devices for Current Classroom Setup Action” on page 594
  - “Duplicate Action” on page 595
  - “New Smart Group: Actions” on page 595
- “Policies” on page 595
  - “New Policy” on page 596
  - “New Smart Policy: Mobile Devices” on page 596

    - “New Smart Policy: Mobile Devices by Installed Applications” on page 596
    - “New Smart Policy: Mobile Devices by Installed Configuration Profiles” on page 596
- “Device Enrollment Profiles” on page 597
    - “New Enrollment Profile” on page 597
    - “New Smart Group: Enrollment Profiles” on page 603
- “New Group: Mobile Devices” on page 603
- “New Smart Group: Mobile Devices” on page 603
- “New Smart Group: Command Queue” on page 603
- “New Smart Group: Command History” on page 603
- “New Category” on page 603
- “Rename <item>” on page 604
- “Edit <item>” on page 604
- “Remove <item>” on page 604

For information on the rest of the commands in the context menu, see “Commands menu” on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

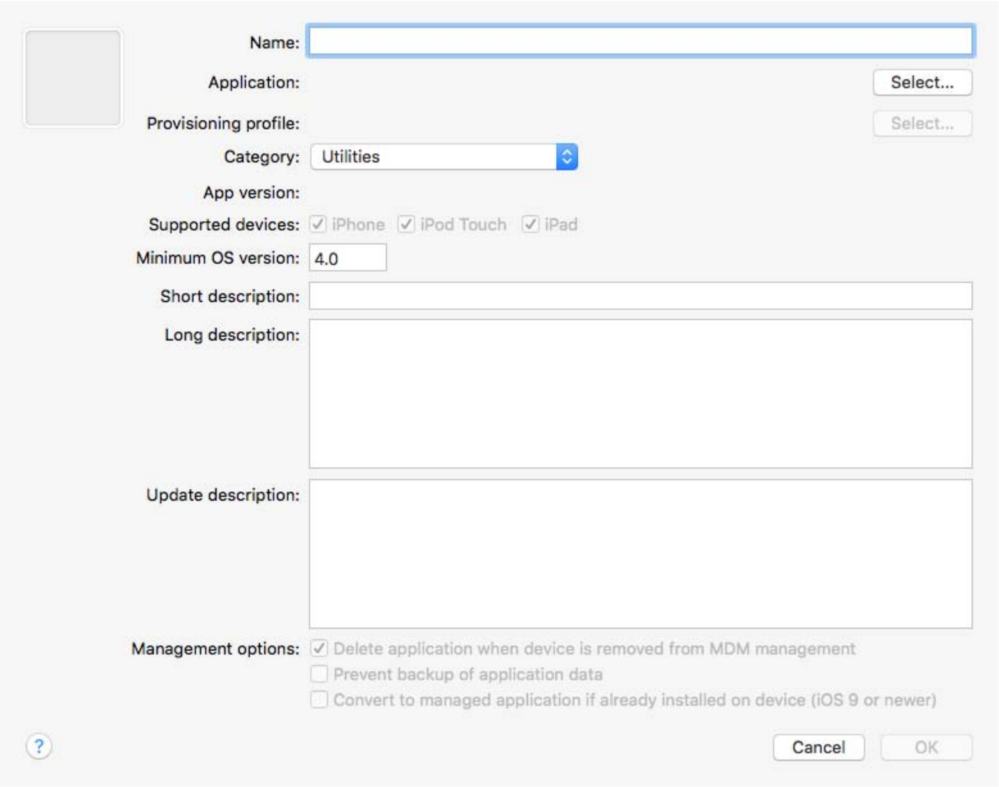
Mobile Applications

The **Mobile Applications** submenu contains commands for working with application packages and provisioning profiles:

- “New Enterprise Application Package” on page 553
- “New iOS App Store Application Package” on page 554
- “New Google Play Application Package” on page 558
- “Duplicate Application Package” on page 559
- “New Smart Group: Enterprise Application Packages” on page 559
- “New Smart Group: App Store Application Packages” on page 559
- “New Smart Group: iOS Provisioning Profiles” on page 559
- “New Smart Group: Installed Applications” on page 559
- “New Smart Group: Installed Application Statistics” on page 559
- “New Smart Group: Mobile Devices by Installed Software” on page 560
- “New Smart Group: Installed iOS Provisioning Profiles” on page 560
- “New Smart Group: Installed iOS Provisioning Profiles Statistics” on page 560
- “New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles” on page 560

New Enterprise Application Package

This command opens the **Mobile Application** dialog in which you can specify a new application package for an app that does not come from an app store.



Name:

Application:

Provisioning profile:

Category: Utilities

App version:

Supported devices: ☑ iPhone ☑ iPod Touch ☑ iPad

Minimum OS version: 4.0

Short description:

Long description:

Update description:

Management options: ☑ Delete application when device is removed from MDM management
□ Prevent backup of application data
□ Convert to managed application if already installed on device (iOS 9 or newer)

The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the application package file is selected, but you can paste in a custom graphic.
- **Name**: The name for the package. This name is displayed in LANrev Apps.
- **Application**: The application file, which must have the .ipa extension. Clicking the **Select** button lets you select the file on your computer.
- **Provisioning profile**: The provisioning profile authorizing the application for deployment on the intended mobile device. The provisioning profile is provided by the application developer. Clicking the **Select** button lets you select the file on your computer containing the profile.
  Provisioning profiles do not apply to Android apps.
- **Category**: The software category to which the app belongs.
- **App version**: The version of the app that is installed by this profile. The version information is automatically read from the app package and cannot be changed.
- **Supported devices**: The devices on which this app can be used. Check all devices that support this app.

This option applies only to iOS apps.

- **Short description**: A brief description of the application. This description is displayed in LANrev Apps.
- **Long description**: A more extensive description of the application. This description is displayed in LANrev Apps.
- **Update description**: A description of the changes in the application compared to the previous version. This description is displayed in LANrev Apps. It should only be filled in when the application package contains an application for which an earlier version exists.
- **Management options**: Choose whether and how the application is put under management on this device.
  - **Delete application when device is removed from MDM management**: If this option is checked, the application is removed from the device when the device is no longer under MDM management.
    This option is available only for iOS devices.
  - **Prevent backup of application data**: If this option is checked, the local data of the application on device cannot be backed up to iTunes or iCloud.
    This option is available only for iOS devices.
  - **Convert to managed application if already installed on device**: If this option is checked, any unmanaged copy of the application that is already present on the device is converted into a managed application.
    This option is available only for devices running iOS 9 and up.

New iOS App Store Application Package

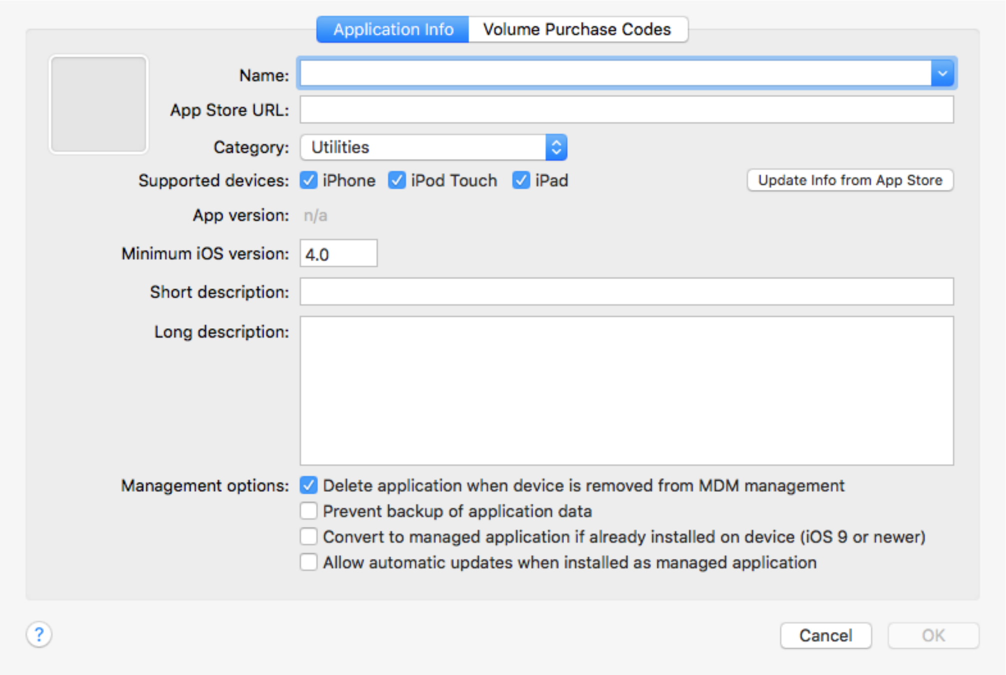
This command opens the **iOS App Store Application** dialog in which you can specify a new application package for an application from the iOS App Store.

The dialog includes two tabs:

- **Application Info tab** (page 555)
- **Volume Purchase Codes tab** (page 557)

Application Info tab

The **Application Info** tab lets you specify the app and its important parameters.



Name:

App Store URL:

Category: Utilities

Supported devices: ☑ iPhone ☑ iPod Touch ☑ iPad

App version: n/a

Minimum iOS version: 4.0

Short description:

Long description:

Management options:
☑ Delete application when device is removed from MDM management
□ Prevent backup of application data
□ Convert to managed application if already installed on device (iOS 9 or newer)
□ Allow automatic updates when installed as managed application

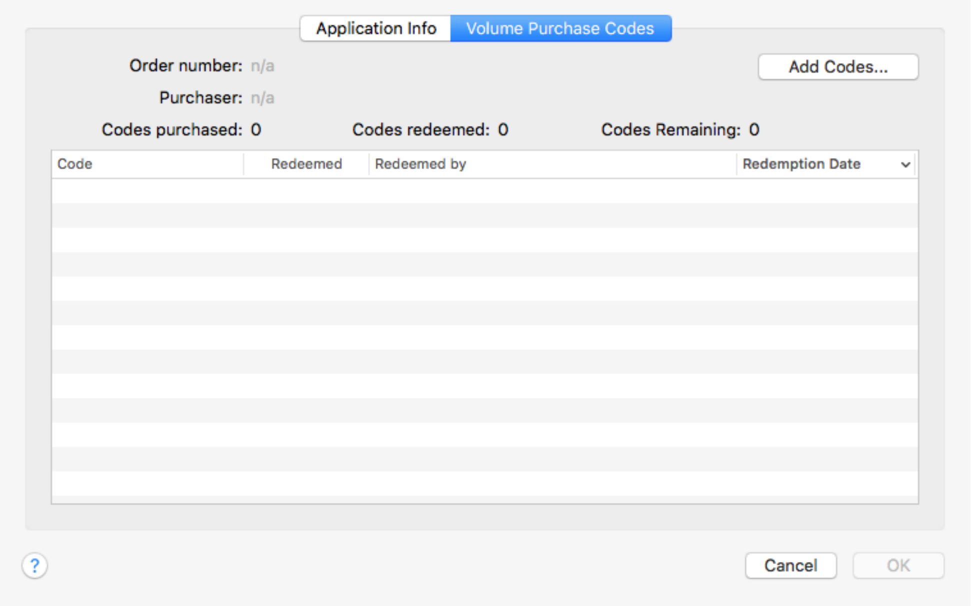
The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the App Store URL is specified but you can paste in a custom graphic.
- **Name**: The name for the package. This name is displayed in LANrev Apps.
  If you begin typing a name, after a few characters have been entered, LANrev will automatically search the App Store and display a list of matching apps in a drop-down list. Clicking one of those apps selects it for the package and fills in the URL and some other fields.
- **Apple App Store URL**: The URL of the App Store page for this app.
  The URL is entered automatically when you click on a found app in the **Name** field. You can also manually obtain the URL by right-clicking the app’s icon anywhere in Apple’s App Store and choosing **Copy Link** from the context menu.
  Entering the URL and leaving this field fills in some of the other fields with information downloaded from the App Store.
- **Category**: The App Store category to which the app belongs.
- **Supported devices**: The iOS hardware platforms on which the app can run.
- **Update Info from App Store**: Clicking this button re-reads the metadata for the app from the App Store.
- **App version**: The version of the app that is available in the App Store.
- **Minimum iOS version**: The minimum version of iOS required to run this app.

- **Short description**: A brief description of the application. This description is displayed in LANrev Apps.
- **Long description**: A more extensive description of the application. This description is displayed in LANrev Apps.
- **Management options**: Choose whether and how the application is put under management on this device.
  - **Delete application when device is removed from MDM management**: If this option is checked, the application is removed from the device when the device is no longer under MDM management.
    This option is available only for iOS devices.
  - **Prevent backup of application data**: If this option is checked, the local data of the application on device cannot be backed up to iTunes or iCloud.
    This option is available only for iOS devices.
  - **Convert to managed application if already installed on device**: If this option is checked, any unmanaged copy of the application that is already present on the device is converted into a managed application.
    This option applies only to devices running iOS 9 and up.
  - **Allow automatic updates when installed as managed application**: Checking this option allows LANrev to automatically update the app when it is assigned to a device.
    If the option is later switched off, auto-updating is suspended while it is switched off. While auto-update is active, LANrev updates the version and minimum OS version information from Apple’s servers about once per day.
    The option applies only when the app is put into the “Auto-install” or “Auto-install, Auto-remove” group and automatic updates are enabled when the app is put into the group.
    This option applies only to devices running iOS 7 and up.

Volume Purchase Codes tab

The **Volume Purchase Code** tab lets you import and manage available App Store volume purchase program redemption codes.



Order number: n/a
Purchaser: n/a
Codes purchased: 0 Codes redeemed: 0 Codes Remaining: 0

Code	Redeemed	Redeemed by	Redemption Date

The dialog contains these elements:

- **Order number**: The order number for the redemption code purchase.
- **Purchaser**: The user through whose App Store account the codes were purchased.
- **Codes purchased**: The total number of redemption codes purchased for this app.
- **Codes redeemed**: The number of codes for this app that have already been redeemed.
- **Codes remaining**: The number of redemption codes for this app that have not yet been redeemed.
  Codes purchased is always the sum of codes redeemed and codes remaining.
- **Import Codes**: Clicking this button let you import redemption codes into the app package definition. It opens a standard Open dialog where you can choose a text file in one of the following formats:
  - A file exported from the Excel file with the purchased code you received from Apple.
    To create this file, open the Excel file and save it as tab-delimited text. Files of this type must begin with two asterisks (**).
  - A standard tab-delimited text file.
    Files of this type contain in each line a redemption code followed by a tab and the redemption link. This kind of file must not begin with a double asterisk.

  The codes in the imported file are appended to the list of codes in the dialog.

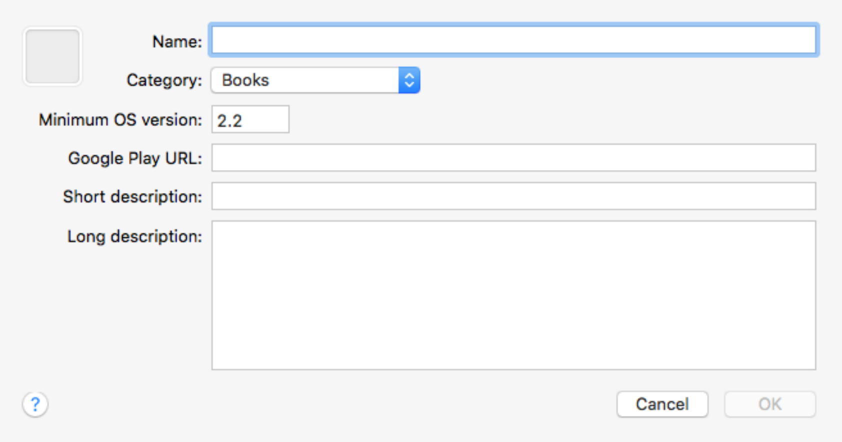
The list that takes up the main part of the dialog lists all redemption code for this app package. It contains these columns:

- **Code**: The redemption code.
- **Redeemed**: Whether this code has already been redeemed.
- **Redeemed by**: The device on which this code was redeemed.
- **Redemption date**: The date on which the code was redeemed.

Pasting text that conforms to the two supported import file formats into the list enters the codes just as if they had been imported.

New Google Play Application Package

This command opens the **Google Play Application** dialog in which you can specify a new application package for an application from the Google Play.



Name:

Category: Books

Minimum OS version: 2.2

Google Play URL:

Short description:

Long description:

The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the Google Play URL is specified but you can paste in a custom graphic.
- **Name**: The name for the package. This name is displayed in LANrev Apps.
- **Category**: The Google Play category to which the app belongs.
- **Minimum OS version**: The minimum version of Android required to run this app.
- **Google Play URL**: The URL of the Google Play page for this app.
  You can obtain the URL by right-clicking the app's icon anywhere in Google Play and choosing **Copy Link** from the context menu.
- **Short description**: A brief description of the application. This description is displayed in LANrev Apps.
- **Long description**: A more extensive description of the application. This description is displayed in LANrev Apps.

Duplicate Application Package

This command opens the selected mobile application package in the **Mobile Application** dialog with a new name. You can edit the settings as desired and save the duplicate.

See “New Enterprise Application Package” on page 553 for details of the dialog.

New Smart Group: Enterprise Application Packages

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile enterprise application packages defined in LANrev.

For details, see “New Smart Group” on page 522.

New Smart Group: App Store Application Packages

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for App Store and Google Play application packages defined in LANrev.

For details, see “New Smart Group” on page 522.

New Smart Group: iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for provisioning profiles that are present on administered iOS devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Applications

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for applications installed on managed mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Application Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for installed application statistics.

For details, see “New Smart Group” on page 522.

New Smart Group: Mobile Devices by Installed Software

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that lists mobile devices based on what software is or is not installed on them.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for provisioning profiles that are present on administered mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed iOS Provisioning Profiles Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for installed provisioning profile statistics.

For details, see “New Smart Group” on page 522.

New Smart Group: Mobile Devices by Installed iOS Provisioning Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for iOS devices based on which provisioning profiles are or are not installed on them.

For details, see “New Smart Group” on page 522.

Configuration Profiles and Certificates

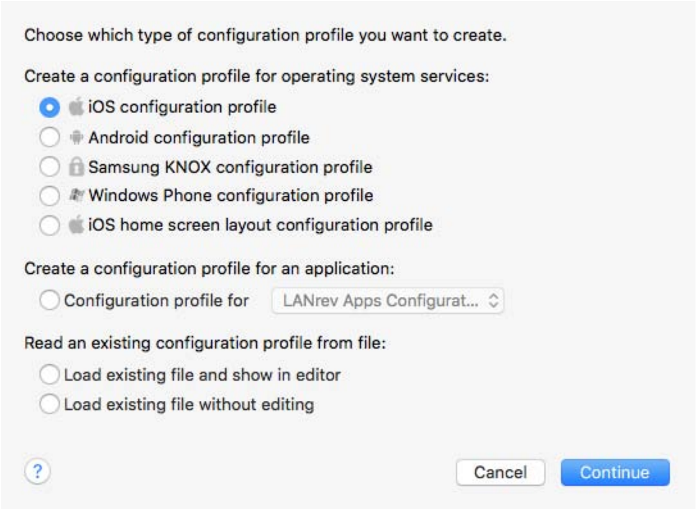
The Mobile Applications submenu contains commands for working with configuration profiles:

- “New Configuration Profile” on page 561
- “New Smart Group: Configuration Profiles” on page 564
- “New Smart Group: Installed Configuration Profiles” on page 564
- “New Smart Group: Installed Configuration Profiles Statistics” on page 564

- “New Smart Group: Mobile Devices by Installed Configuration Profiles” on page 564
- “New Smart Group: Installed Certificates” on page 564
- “New Smart Group: Installed Certificates Statistics” on page 565
- “New Smart Group: Mobile Devices by Installed Certificates” on page 565

New Configuration Profile

This command opens the **Configuration Profile Type** dialog, in which you can choose the type of configuration you want to create.



Choose which type of configuration profile you want to create.

Create a configuration profile for operating system services:

● iOS configuration profile
○ Android configuration profile
○ Samsung KNOX configuration profile
○ Windows Phone configuration profile
○ iOS home screen layout configuration profile

Create a configuration profile for an application:

○ Configuration profile for LANrev Apps Configurat...

Read an existing configuration profile from file:

○ Load existing file and show in editor
○ Load existing file without editing

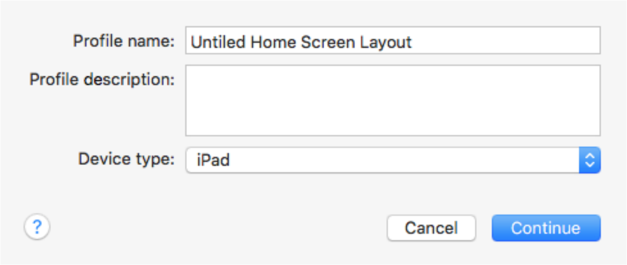
Depending on which option you choose, clicking **OK** has different effects:

- **iOS configuration profile**: The profile editor is opened with the settings for an iOS configuration profile displayed. Choosing **Android configuration profile**, **Samsung KNOX configuration profile**, **Windows Phone configuration profile**, or **Configuration profile for**, has a similar effect. (In the latter case, you can also choose the desired application to configure.)
  For more information on the profile editor, see “Configuration profile editor” on page 666.
- **iOS home screen layout configuration profile**: The Home Screen Layout Profile Settings dialog is displayed, which is described in “Home Screen Layout Profile Settings dialog”, below. Clicking **Continue** in that dialog opens the home screen profile editor, which is described in “Home screen layout editor” on page 679.
- **Load existing file and show in editor**: You can choose a configuration profile file from disk and open it in the profile editor.
- **Load existing file without editing**: You can choose a configuration profile file from disk and import it into LANrev without editing it.

The profile is displayed in the **Configuration Profile** dialog (see below).

Home Screen Layout Profile Settings dialog

The **Home Screen Layout Profile Settings** dialog lets you specify basic information for a new iOS home screen layout configuration profile.



Profile name: Untiled Home Screen Layout

Profile description:

Device type: iPad

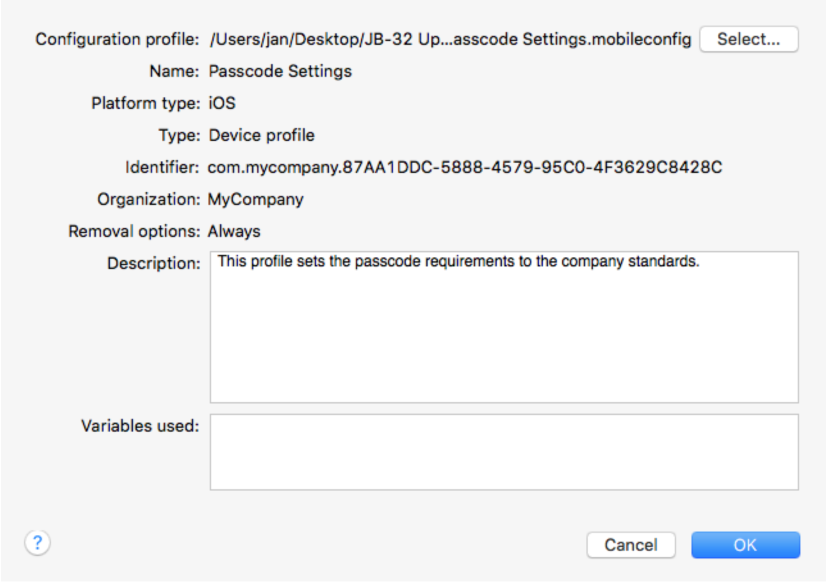
The dialog contains these elements:

- **Profile name**: The name you want to give the profile.
- **Profile description**: A description of the profile. This description is displayed to the user of the managed mobile device.
- **Device type**: The target device for the profile, which determines how many rows and columns there are for laying out the icons.

Clicking **Continue** opens the home screen profile editor, which is described in “Home screen layout editor” on page 679.

Configuration Profile dialog

The **Configuration Profile** dialog lets you import an existing configuration profile from disk into LANrev that can then be distributed to administered mobile devices.



Configuration profile: /Users/jan/Desktop/JB-32 Up...asscode Settings.mobileconfig

Name: Passcode Settings

Platform type: iOS

Type: Device profile

Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C

Organization: MyCompany

Removal options: Always

Description: This profile sets the passcode requirements to the company standards.

Variables used:

The dialog contains these elements:

- **Configuration profile**: The file containing the configuration profile. Clicking the **Select** button lets you select the file on your computer.
- **Name**: The name of the profile. The name is automatically read from the profile and cannot be changed in this dialog.
- **Platform type**: The operating system to which the profile applies. The type is automatically detected and cannot be changed in this dialog.
- **Type**: The kind of profile – device or app profile.
- **Identifier**: The identifier of the profile. The identifier is automatically read from the profile and cannot be changed in this dialog.
- **Organization**: The organization which issued the profile. The identifier is automatically read from the profile and cannot be changed in this dialog.
- **Removal options**: Whether the local user of the mobile device can remove the profile and whether a passcode is required for doing so.
- **Description**: A description of the profile. This description is displayed to the user of the managed mobile device.
- **Variables used**: The variables used in this profile that will be replaced with actual values during the installation. (See “Using variables in configuration profiles” on page 185 for information on using variables in profiles.)

Clicking **OK** imports the profile into the **Configuration Profiles** section of the **Mobile Devices** window.

New Smart Group: Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile device configuration profiles defined in LANrev.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for configuration profiles installed on managed mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Configuration Profiles Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for statistics on configuration profiles installed on administered mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Mobile Devices by Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices based on the configuration profiles that are or are not installed on them.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Certificates

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for certificates installed on managed mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Certificates Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for statistics on certificates installed on administered mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Mobile Devices by Installed Certificates

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices based on which certificates are or are not installed on them.

For details, see “New Smart Group” on page 522.

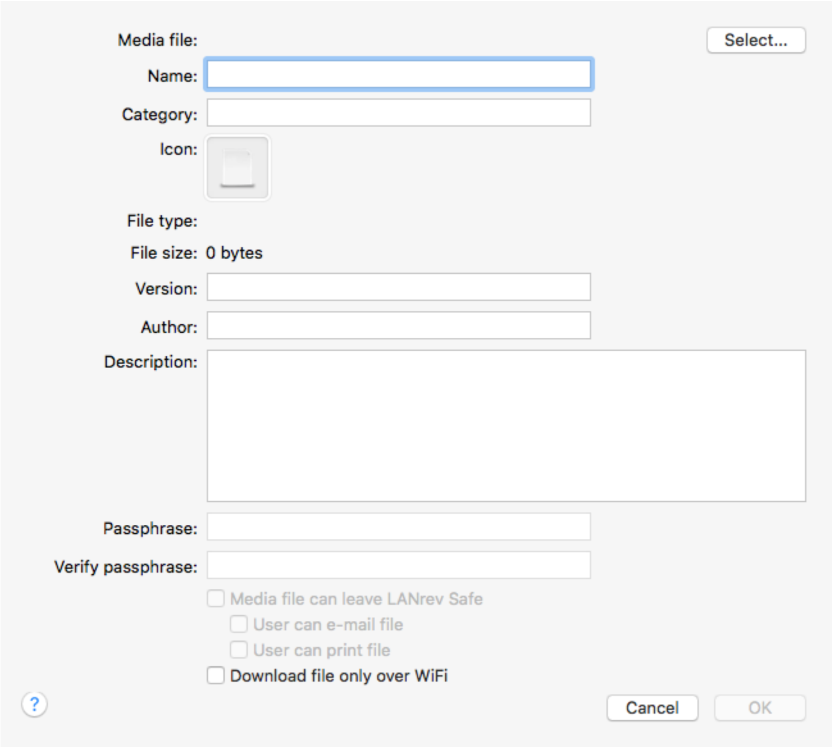
Media

The **Media** submenu contains commands for working with media objects:

- “New Media File” on page 566
- “Duplicate Media File” on page 567
- “New Smart Group: Media Files” on page 568
- “New Smart Group: Installed Media Files” on page 568
- “New Smart Group: Installed Media File Statistics” on page 568
- “New Smart Group: Mobile Devices by Installed Media Files” on page 568

New Media File

This command opens the **Mobile Media File** dialog in which you can specify a media file that is to be made available to managed mobile devices:



Media file:

Name:

Category:

Icon:

File type:

File size: 0 bytes

Version:

Author:

Description:

Passphrase:

Verify passphrase:

□ Media file can leave LANrev Safe

□ User can e-mail file

□ User can print file

□ Download file only over WiFi

The dialog contains these elements:

- **Media file**: The file you want to make available. Clicking the **Select** button lets you choose a file. You can also drag a file or folder from the desktop into this area to choose it.
- **Name**: The name under which the file appears on managed mobile devices. This field is deactivated when a folder is selected; the name is in that case automatically set from the filename.
- **Category**: The category in which it is displayed by LANrev Safe on the managed device. This field is prepopulated by LANrev based on the kind of file selected, but you can enter any desired category name.
  If the category does not yet exist, LANrev Safe will create it.
  If you have selected a folder (instead of a single file), you can leave the category free to have LANrev automatically assign a category to each file depending on its file type or enter a category that is applied to all files contained in the folder.
- **Icon**: The icon that is displayed for the media file on the managed mobile devices. The icon is automatically created based on the type of the selected file, but you can also paste any graphic into this field.
- **File type**: The type of the selected file. If you have selected a folder instead of a single file, “Batch upload” is displayed.

- **File size**: The size of the file in bytes.
- **Version**: The version of the file. This is a freeform string, so you can enter the version in any way that makes sense in your organization.
- **Author**: The author of the file.
- **Description**: A description of the file for the mobile users. This description is displayed in LANrev Safe.
- **Passphrase**: When you enter text into this field, the media file is only displayed when the user enters the same text on the mobile device.
- **Verify passphrase**: Repeat the passphrase to guard against typos.
- **Media file can leave LANrev Safe**: If you check this option, users of mobile devices can open the file in an app other than LANrev Safe, for example, to view it in a PDF reader or to mail it to somebody else.
  Two other options become available:
  - **User can e-mail file**: If this option is checked, a button for sending this file by e-mail appears in LANrev Safe.
  - **User can print file**: If this option is checked, a button for printing this file appears in LANrev Safe.

  If this option is unchecked, mobile users can view the file only in LANrev Safe.
  If you have selected an entire folder of files (instead of a single file), this setting does not apply to files that cannot be displayed in LANrev Safe (see “Supported media types” on page 222 for a complete list): These files are always allowed to leave LANrev Safe because otherwise there would be no way for the mobile users to view them.
  Note: While unchecking this option reliably prevents the file from leaving LANrev Safe, the same is not necessarily true for the information contained in the file. For example, a mobile user still could take screenshots of the file and send those to other persons.
- **Download file only over WiFi**: If you check this option, LANrev Safe will download the file only if the mobile device is on a WiFi-connection, not when it is connected over a mobile data connection such as 3G (UMTS) or LTE.
  This setting is ignored by versions of LANrev Safe earlier than 1.1.

Clicking **OK** saves the media file in LANrev. It can then be assigned to a policy to make it available to mobile users.

Duplicate Media File

This command creates a duplicate of the selected media file record, removes the media file from it, and opens the **Mobile Media File** dialog.

In the dialog, the **Category**, **Description**, and **Media file can leave LANrev Safe** settings are preserved. You can select a new media file to fill the other fields and enter a new name for the duplicated media file object.

For a description of the **Mobile Media File** dialog, see above.

New Smart Group: Media Files

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile media files.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Media Files

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile media files that have been installed using the **Install Media File** command.

For details, see “New Smart Group” on page 522.

New Smart Group: Installed Media File Statistics

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile media file statistics.

For details, see “New Smart Group” on page 522.

New Smart Group: Mobile Devices by Installed Media Files

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group to list devices depending on which mobile media files have been installed on them.

For details, see “New Smart Group” on page 522.

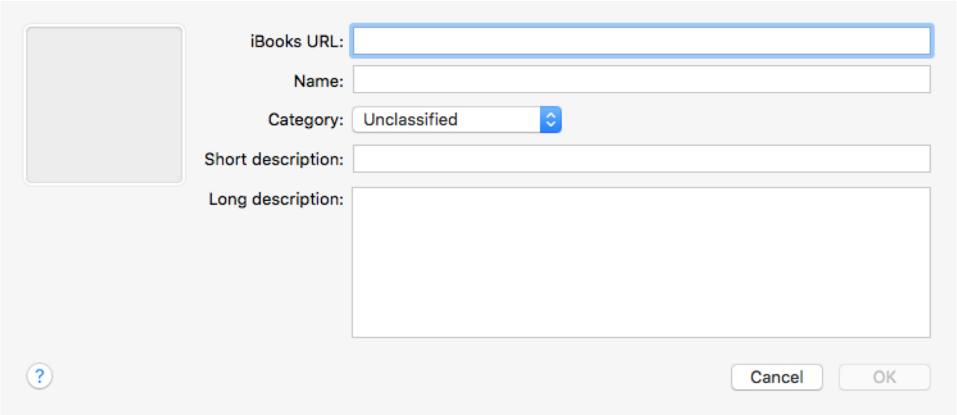
Books

The **Books** submenu contains commands for working with iBooks Store book objects:

- “New iBooks Book” on page 569
- “Duplicate iBooks Book” on page 569
- “New Smart Group: iBooks Books” on page 569

New iBooks Book

This command opens the **iBooks Book** dialog in which you can specify a book from the iBooks Store file that is to be made available to managed mobile devices:



The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the book store URL is specified, but you can paste in a custom graphic.
- **iBooks URL**: The URL of the iBooks Store page for this book. You can obtain the URL by right-clicking the book’s icon anywhere in the book store and choosing **Copy Link** from the context menu.
  Entering the URL and leaving this field fills in some of the other fields with information downloaded from the book store.
- **Name**: The name of the book. This name is displayed for the book in LANrev.
- **Category**: The book store category to which the book belongs.
- **Short description**: A brief description of the book.
- **Long description**: A more extensive description of the application.

Clicking **OK** saves the book in LANrev.

Duplicate iBooks Book

This command creates a duplicate of the selected book record, appends “ copy” to the name, and opens the **iBooks Book** dialog.

For a description of the **iBooks Book** dialog, see above.

New Smart Group: iBooks Books

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for iBooks Store books.

For details, see “New Smart Group” on page 522.

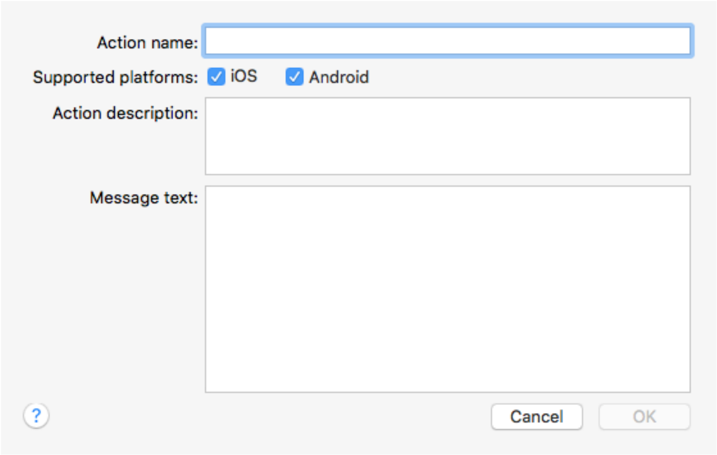
Actions

The **Actions** submenu contains commands for working with actions that can be assigned to smart policies:

- “New Send Message Action” on page 571
- “New Send E-Mail Action” on page 572
- “New Send SMS (Text Message) Action” on page 573
- “New Set Roaming Options Action” on page 574
- “New Set Activation Lock Options Action” on page 575
- “New Enable Activation Lock Action” on page 576
- “New Set Wallpaper Action” on page 577
- “New Set Device Name Action” on page 578
- “New Install iOS Update Action” on page 579
- “New Validate Applications Action” on page 580
- “New Set Custom Field Value Action” on page 581
- “New Update Device Information Action” on page 582
- “New Set Attention Mode Action” on page 583
- “New Set Lost Mode Action” on page 584
- “New Set Passcode Lock Grace Period Action” on page 585
- “New Configure Diagnostic Data Transmission Action” on page 586
- “New Freeze Device Action” on page 587
- “New Clear Passcode Action” on page 588
- “New Register User in VPP Action” on page 588
- “New Send VPP Invitation Action” on page 590
- “New Retire User from VPP Action” on page 592
- “New Remove Configuration Profile Action” on page 593
- “New Demote to Unmanaged Device Action” on page 593
- “New Configure Devices for Current Classroom Setup Action” on page 594
- “Duplicate Action” on page 595
- “New Smart Group: Actions” on page 595

New Send Message Action

This command opens the **Send Message Action** dialog in which you can specify a message that is to be sent to mobile devices that become members of a policy:



Supported platforms: ☑ iOS ☑ Android

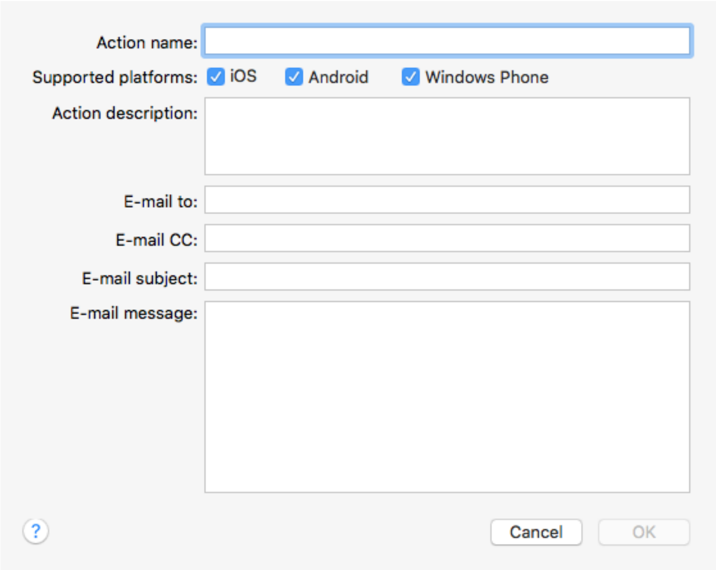
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Message text**: The text that is sent to managed mobiled evices that trigger the action. The message appears on-screen on the devices.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Send E-Mail Action

This command opens the **Send E-Mail Action** dialog in which you can specify an e-mail that is to be sent when mobile devices become members of a policy:



The dialog contains these elements:

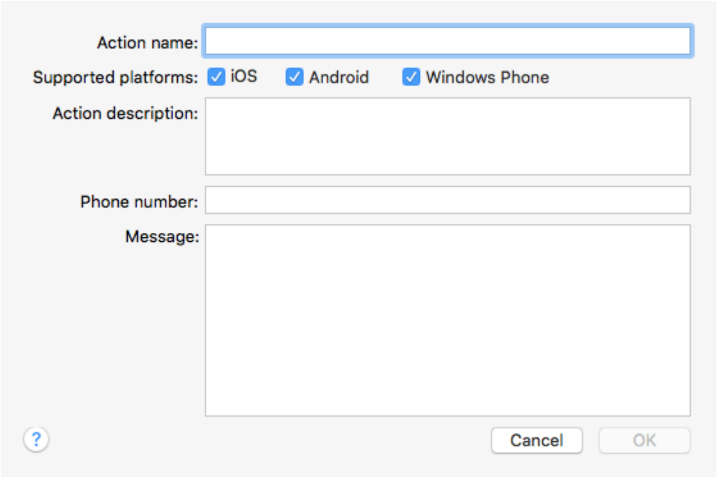
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **E-mail to**: The e-mail address to which the e-mail is to be sent.
- **E-mail cc**: The e-mail addresses to which the e-mail is to be copied, if any.
- **E-mail subject**: The subject of the e-mail.
- **E-mail message**: The body of the e-mail.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

Note that LANrev can send e-mails only when the SMTP information in the **Notification** tab of the **Server Settings** is filled in.

New Send SMS (Text Message) Action

This command opens the **Send SMS Action** dialog in which you can specify an SMS text message that is to be sent when mobile devices become members of a policy:



Action name:

Supported platforms: ☑ iOS ☑ Android ☑ Windows Phone

Action description:

Phone number:

Message:

The dialog contains these elements:

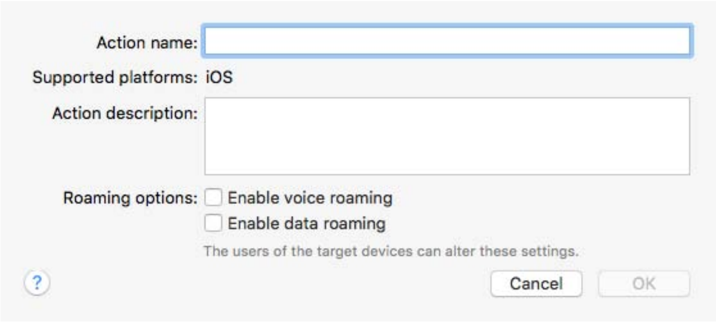
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Phone number**: The telephone number to which the SMS text message is to be sent. When you enter multiple phone numbers separated by commas, the text message is sent to all of them.
- **Message**: The message that is going to be sent. The message may be up to 140 characters long.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458. Note that the limit of 140 characters applies after the variables have been substituted with the actual values.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

Note that LANrev can send texts only when the SMS information in the **Notification** tab of the **Server Settings** is filled in.

New Set Roaming Options Action

This command opens the **Set Roaming Options Action** dialog in which you can specify roaming options that are to be applied to mobile devices that become members of a policy:



Action name:

Supported platforms: iOS

Action description:

Roaming options: □ Enable voice roaming

□ Enable data roaming

The users of the target devices can alter these settings.

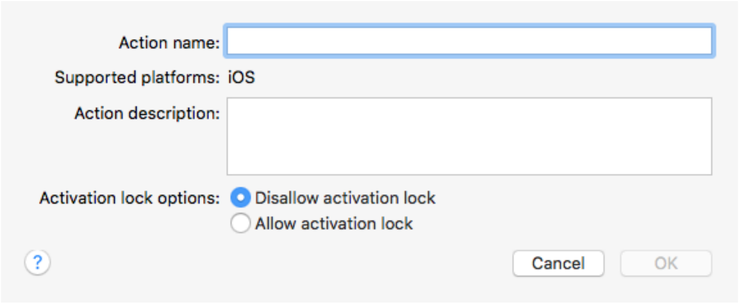
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Roaming options**: Whether to enable or disable voice and data roaming, respectively, on managed mobile devices entering a policy. Checking an option enables the respective kind on roaming on all devices, unchecking the option, disables the kind of roaming, and setting the option to the third state (⊟) leaves the roaming setting unchanged.
  Note that the local users of the managed mobile devices can change the roaming settings at any time.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Set Activation Lock Options Action

This command opens the **Set Activation Lock Options Action** dialog in which you can create an action that switches on or off the activation lock on affected computers:



Action name:

Supported platforms: iOS

Action description:

Activation lock options: ● Disallow activation lock ○ Allow activation lock

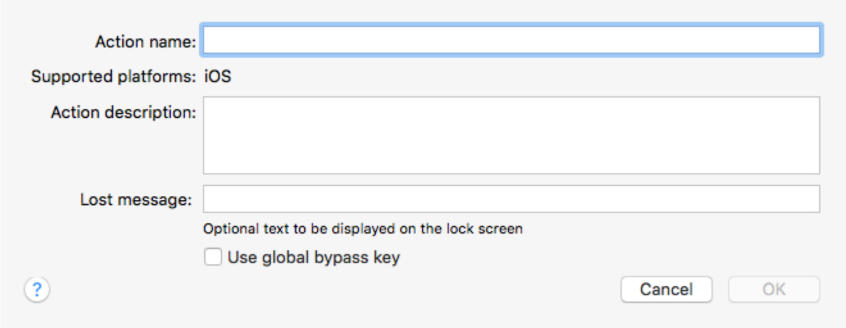
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
  Activation lock actions can only be applied to supervised devices running iOS 7 and up.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Activation lock options**: Whether the activation lock can be enabled on the selected devices via the "Find My iPhone" (or "Find My iPad") setting:
  - If you allow the activation lock to be enabled, the feature will be automatically activated when "Find my iPhone" is switched on.
  - If you disallow the activation lock, it will not be switched on together with "Find My iPhone".
    Note, however, that this does not disable an activation lock feature that is already activated. The activation lock setting remains in effect until "Find My iPhone" is next disabled, which automatically switches it off. Thereafter, it will not be enabled again, even if "Find my iPhone" is switched on again.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Enable Activation Lock Action

This command opens the **Enable Activation Lock Action** dialog in which you can enable the activation lock of a shared device:



Action name:

Supported platforms: iOS

Action description:

Lost message:

Optional text to be displayed on the lock screen

□ Use global bypass key

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply. This action can only be applied to iOS devices.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Lost message**: The message that is displayed on the locked devices.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458.
- **Use global bypass key**: If this option is checked, a universal bypass key is generated that unlocks all devices that have been locked with this option. If it is unchecked, a unique key is generated for each locked device. For more details, see “Enable Activation Lock” on page 472.

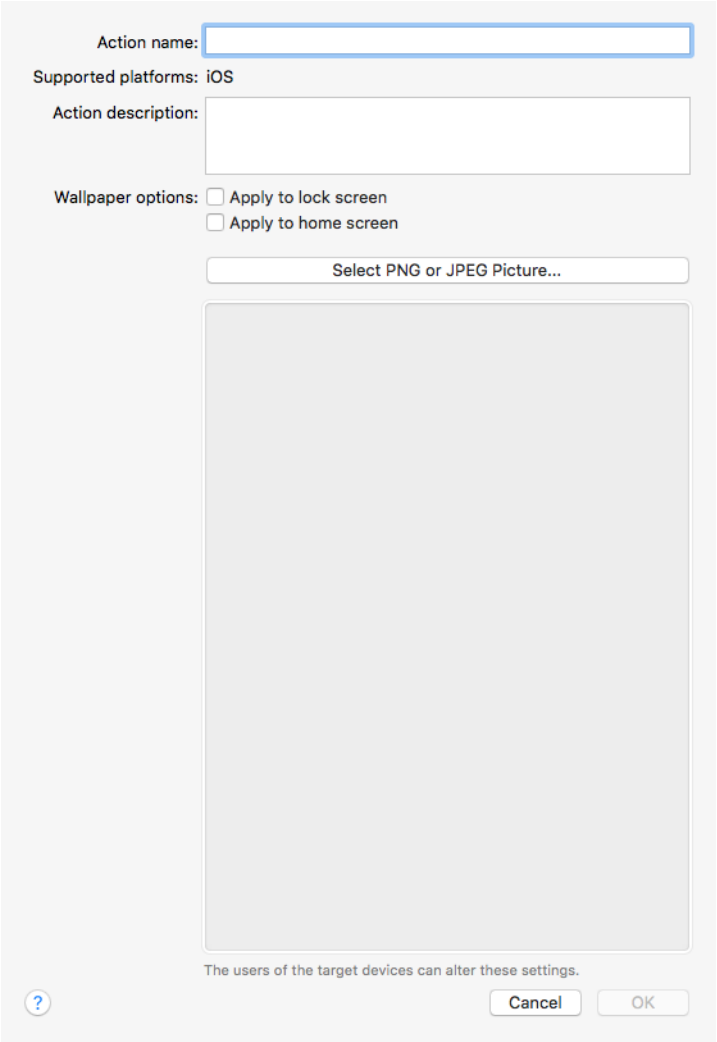
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev enables the activation lock on the device, which means that they can be activated in future only with the generated bypass code (which can be displayed using **Show Activation Lock Bypass Code** command).

This action affects only shared devices that are enrolled in Apple School Manager.

New Set Wallpaper Action

This command opens the **Set Wallpaper Action** dialog in which you can specify wallpaper to be set on mobile devices that become members of a policy:



Action name:

Supported platforms: iOS

Action description:

Wallpaper options: □ Apply to lock screen
□ Apply to home screen

The users of the target devices can alter these settings.

The dialog contains these elements:

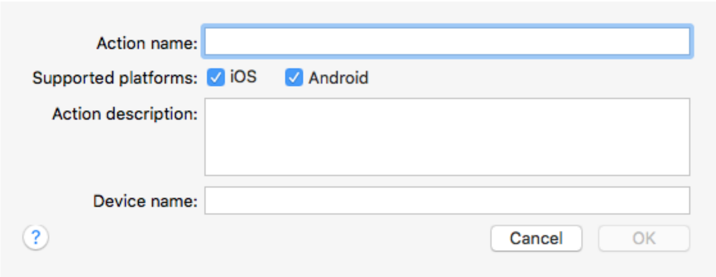
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
  Wallpaper actions can only be applied to supervised devices running iOS 7.1 and up.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Wallpaper options**: Which image to set where as wallpaper.

- **Apply to lock screen**: If this option is checked, the selected devices display the chosen image as the screen background as long as the device is locked.
- **Apply to home screen**: If this option is checked, the selected devices display the chosen image as the screen background of the device’s home screen.
- **Select PNG or JPEG Picture**: Clicking this button opens a standard Open dialog in which you can choose the image that you want to use as the wallpaper on the selected devices.
- The main part of the dialog displays the currently chosen image, if any.
  Instead of using the **Select PNG or JPEG Picture** button, you can also drag an image here.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

New Set Device Name Action

This command opens the **Set Device Name Action** dialog in which you can specify that a device is renamed when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android

Action description:

Device name:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Device name**: The new device name.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458.

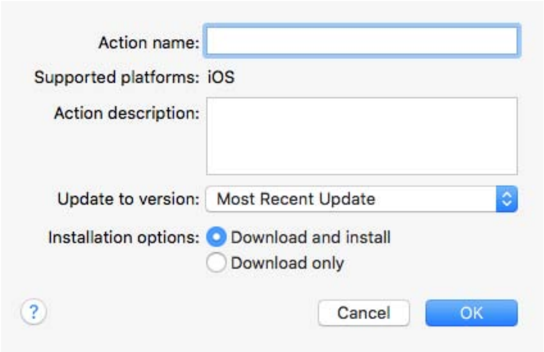
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev renames the device according to the specifications in the action. This action can be applied only to iOS devices running iOS 8 and above and Android devices.

New Install iOS Update Action

This command opens the **Install iOS Update Action** dialog in which you can specify that iOS on a device is updated to a particular version when it becomes the member of a smart policy.

The action created in this dialog applies only to devices that run iOS 9 and up, have been enrolled through Apple's device enrollment program, and also are supervised.



Action name:

Supported platforms: iOS

Action description:

Update to version: Most Recent Update

Installation options: ● Download and install

○ Download only

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Update to version**: The desired target version to update the device to. The pop-up menu contains the **Most Recent Update** entry and all versions that are available on Apple's servers and that apply to the selected devices.
  If you choose a specific version, the devices are updated to that version when the action is executed (unless they already contain a newer version).
  If you choose **Most Recent Update**, the devices are updated to the newest version available at the time the action is executed.
- **Installation options**: Whether to just download the updater or install it as well:
  - **Download and install**: The updater is downloaded and executed immediately afterwards. If the updater is already available on the device (for example, because it has been downloaded earlier using the **Download only** setting), it is executed immediately.

Note that some updaters give the user the option to postpone the update, but some do not. Also, some updaters require a device restart.
You can display the properties of the updater using the information items in the **Available OS Updates** category.

- **Download only**: The updater is downloaded to the device but not executed.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev triggers the device to download and install the update according to the specifications in the action. This action can be applied only to iOS devices running iOS 9 and up.

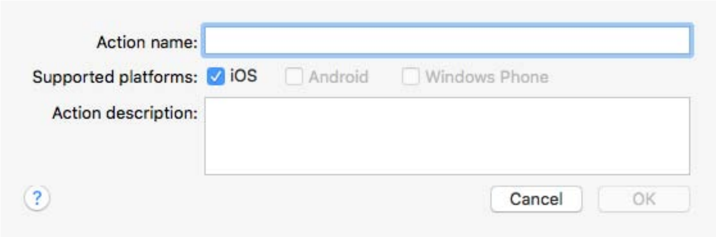
New Validate Applications Action

This command opens the **Validate Applications Action** dialog in which you can specify that all apps on the device that have been installed with enterprise certificates are validated.

iOS 9.2 and up requires this validation every few weeks to allow applications that have been installed with enterprise certificates to continue running. The validation fails if there is no Internet connection.

If a device will be without Internet contact for prolonged periods of time, you can use this action to reset the interval for the next validation, allowing any affected apps to be used for a few weeks before the next validation is required.

The action created in this dialog applies only to devices that run iOS 9.2 and up.



Action name:

Supported platforms: ☑ iOS □ Android □ Windows Phone

Action description:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is

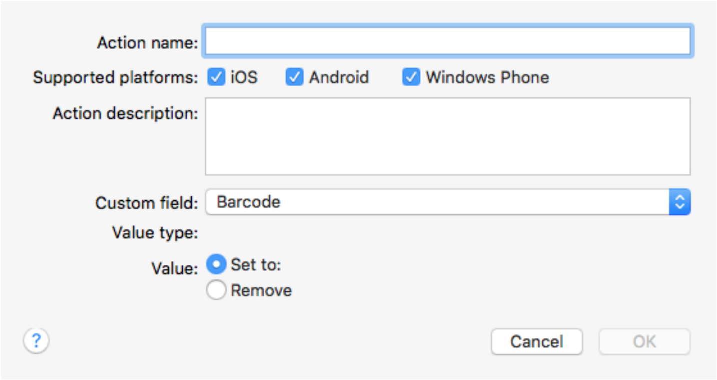
intended for your own reference and that of other administrators.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev triggers the device to download and install the update according to the specifications in the action. This action can be applied only to iOS devices running iOS 9.2 and up.

New Set Custom Field Value Action

This command opens the **Set Custom Field Value Action** dialog in which you can specify the value for a custom field that is set for the device when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android ☑ Windows Phone

Action description:

Custom field: Barcode

Value type:

Value: ● Set to: ○ Remove

The dialog contains these elements:

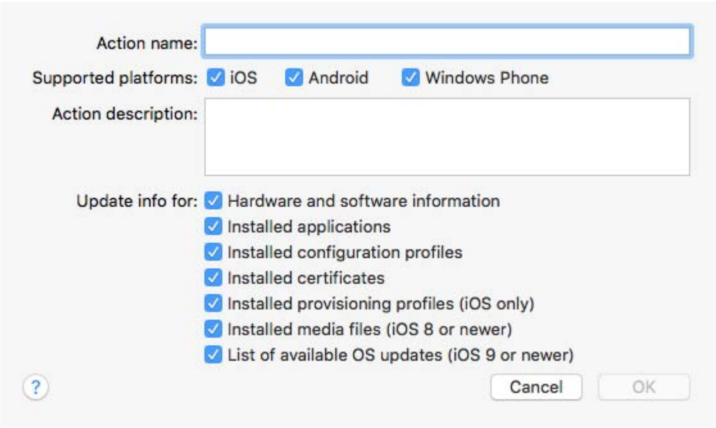
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Custom field**: The field for which the value is set.
  The pop-up menu contains all manual custom information fields that have been defined on the server.
- **Value type**: The data type that the field value must have.
- **Value**: The value to which the field is set on the device on which the action is executed.
  If you choose the **Remove** option, any existing value is removed from the field.
  When you specify a value (choosing the **Set to** option), you can use the variables described in “Variables for mobile devices” on page 458.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev renames the device according the specifications in the action. This action can be applied only to iOS devices running iOS 8 and above and the Android devices.

New Update Device Information Action

This command opens the **Update Device Information Action** dialog in which you can specify that the information stored on LANrev Server for a device is updated when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android ☑ Windows Phone

Action description:

Update info for:
☑ Hardware and software information
☑ Installed applications
☑ Installed configuration profiles
☑ Installed certificates
☑ Installed provisioning profiles (iOS only)
☑ Installed media files (iOS 8 or newer)
☑ List of available OS updates (iOS 9 or newer)

The dialog contains these elements:

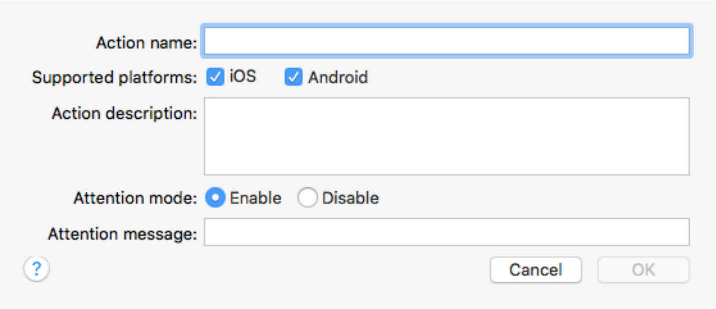
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Update info for**: The information categories that can be updated. Some of the categories apply only to certain devices, as noted beside those options.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev updates all information on the device that is stored on the server. This is similar to applying the **Update Device Information** command to the device.

New Set Attention Mode Action

This command opens the **Set Attention Mode Action** dialog in which you can specify that the attention mode on a device is enabled or disabled when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android

Action description:

Attention mode: ● Enable ○ Disable

Attention message:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Attention mode**: Whether you want the action to enable or disable the attention mode.
- **Attention message**: The message that is displayed on the screen of the device while the attention mode is enabled.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all applicable devices (see below) that are currently members of the policy. It will also be applied to any applicable device that becomes a member of the policy when it becomes a member.

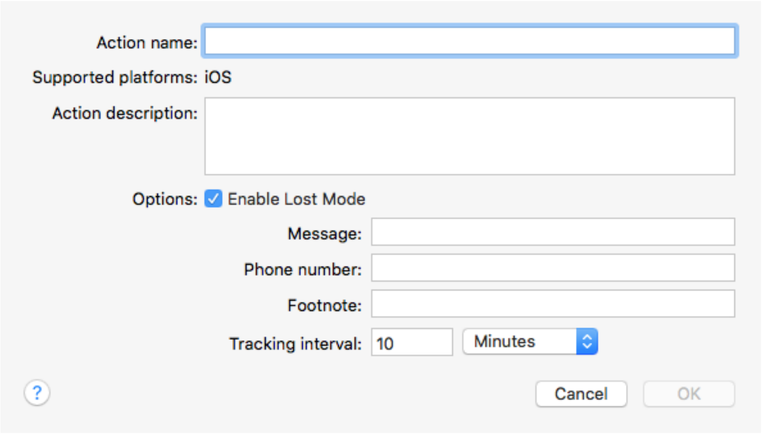
The action applies only to these devices:

- iOS: Any supervised device.(Devices can be put into supervised mode with the Apple Configurator. Devices that are part of Apple's device enrollment program can be put into supervised mode in the enrollment profile, as described in "New Device Enrollment Profile" on page 640.)
- Android: Devices on which LANrev Apps 2.0.9 or up is installed or running Samsung SAFE on which LANrev Apps 2.0.5 or up is installed.

When the action is applied to an applicable device, LANrev sets the attention mode as specified. This is similar to applying the **Enable Attention Mode** or **Disable Attention Mode** command, respectively, to the device.

New Set Lost Mode Action

This command opens the **Set Lost Mode Action** dialog in which you can specify that the lost mode on a device is enabled or disabled when it becomes the member of a smart policy:



Action name:

Supported platforms: iOS

Action description:

Options: ☑ Enable Lost Mode

Message:

Phone number:

Footnote:

Tracking interval: 10 Minutes

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Enable Lost Mode**: If this checkbox is checked, the Lost mode will be enabled on the on the selected device; if it is unchecked, the mode will be disabled.
  If this checkbox is unchecked, the following fields are ignored.
- **Message**: The message that is displayed on the lock screen of the device. This information is optional.
  You can use the variables described in "Variables for mobile devices" on page 458.
- **Phone number**: The phone number that is displayed on the lock screen. If the device is capable of making phone calls, this number can be called from the locked device. This information is optional.
- **Footnote**: This text is displayed at the bottom of the lock screen. This information is optional.
  You can use the variables described in "Variables for mobile devices" on page 458.
- **Tracking interval**: The frequency with which the position of the device is determined and recorded in the LANrev database. This information is optional.

Note that Lost mode is persistent: Erasing and re-enrolling the device will not take it out of Lost mode.

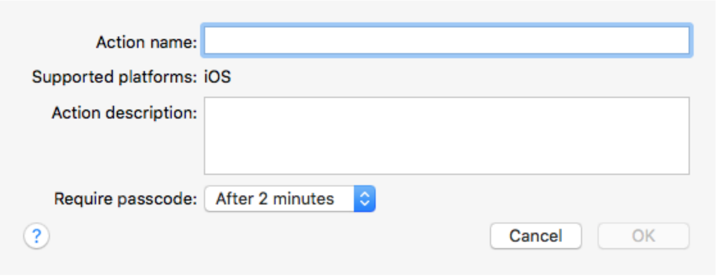
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all applicable devices (see below) that are currently members of the policy. It will also be applied to any applicable device that becomes a member of the policy when it becomes a member.

The action applies only to supervised iOS devices running iOS 9.3 and up.

When the action is executed on a device, LANrev sets the lost mode as specified. This is similar to applying the **Set Lost Mode** command to the device.

New Set Passcode Lock Grace Period Action

This command opens the **Set Passcode Lock Grace Period Action** dialog in which you can specify the passcode lock grace period on a device when it becomes the member of a smart policy:



Action name:

Supported platforms: iOS

Action description:

Require passcode: After 2 minutes

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply. This is always iOS for this action.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Require passcode**: The passcode lock grace period from this menu.
  The grace period is the amount of time between the moment when the device locks (the screen is deactivated) and the moment when unlocking it again requires entering the passcode or, if the device has Touch ID, providing a fingerprint.

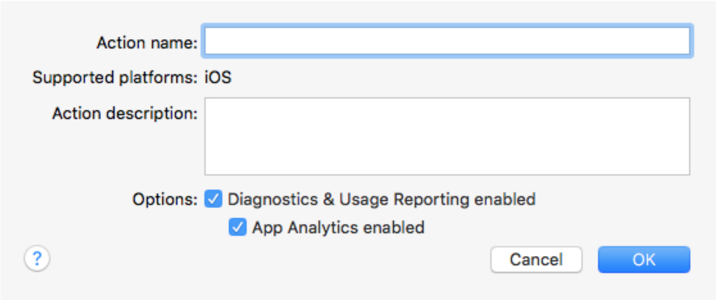
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all applicable devices (see below) that are currently members of the policy. It will also be applied to any applicable device that becomes a member of the policy when it becomes a member.

This action can only be applied to devices running iOS 9.3.2 and up.

When the action is applied to an applicable device, LANrev sets the grace period as specified. This is similar to applying the **Set Passcode Lock Grace Period** command to the device.

New Configure Diagnostic Data Transmission Action

This command opens the **Configure Diagnostic Data Transmission Action** dialog in which you can specify which types of diagnostic information a device that becomes the member of a smart policy sends back to Apple:



Action name:

Supported platforms: iOS

Action description:

Options: ☑ Diagnostics & Usage Reporting enabled

☑ App Analytics enabled

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply. This is always iOS for this action.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Diagnostics & Usage Reporting enbled**: If this option is checked, devices send daily diagnostic and usage data to Apple.
- **App Analytics enbled**: If this option is checked, devices send crash and usage data to Apple for forwarding to the app's developers.

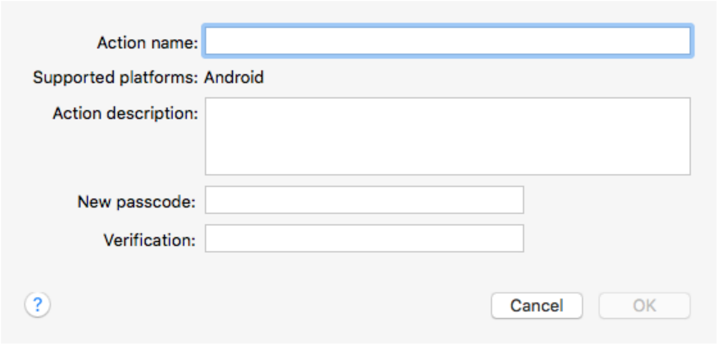
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all applicable devices (see below) that are currently members of the policy. It will also be applied to any applicable device that becomes a member of the policy when it becomes a member.

This action can only be applied to devices running iOS 9.3.2 and up.

When the action is applied to an applicable device, LANrev sets the diagnostic reporting as specified. This is similar to applying the **Configure Diagnostic Data Transmission** command to the device.

New Freeze Device Action

This command opens the **Freeze Device Action** dialog in which you can specify that a device is locked and given a new passcode when it becomes the member of a smart policy:



Action name:

Supported platforms: Android

Action description:

New passcode:

Verification:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **New passcode**: The new passcode for the device. This replaces any existing passcode that there may be on the device.
- **Verification**: Repeat the new passcode.

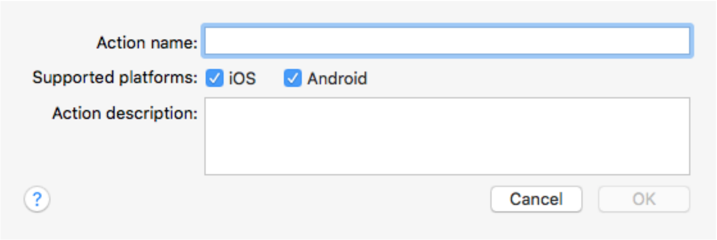
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, the device will be locked so that it is no longer accessible. At the same time the passcode is changed so that the user of the device must contact you to regain access to it.

NOTE It may be possible to circumvent the lock by resetting the device to its factory state. However, this usually deletes all data on the device.

New Clear Passcode Action

This command opens the **Clear Passcode Action** dialog in which you can specify that the passcode of a device is removed when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android

Action description:

The dialog contains these elements:

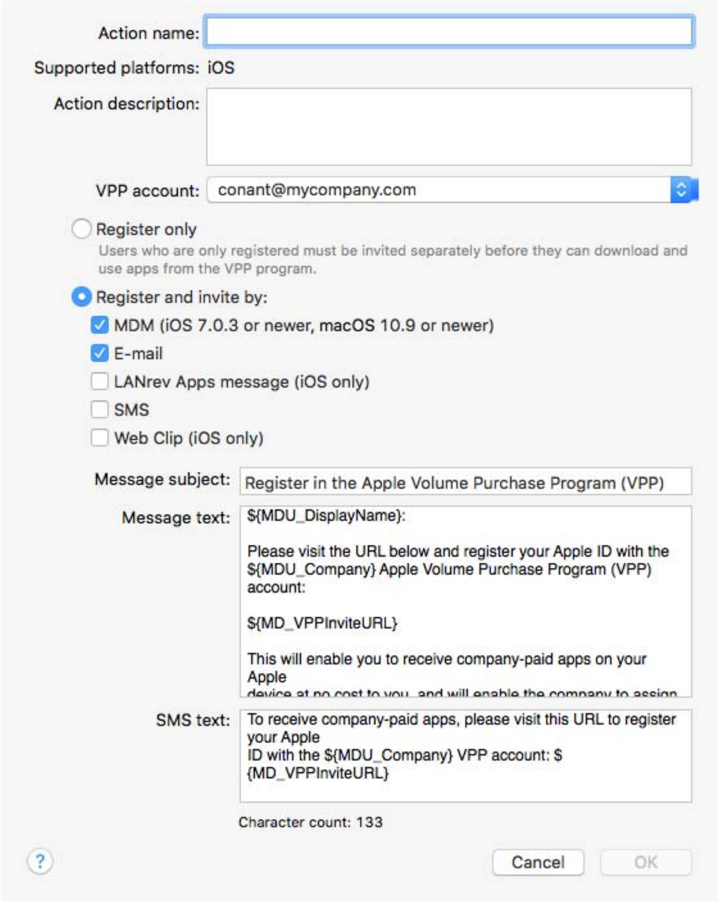
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, any existing passcode will be removed from the device. No new passcode will be required, so it is up to the user whether to set a new passcode (unless a configuration profile on the device makes a passcode mandatory).

New Register User in VPP Action

This command opens the **Register User in VPP Action** dialog in which you can specify a VPP account to which to add devices on which the action is executed as well as whether to send an invitation message at the same time and, if so, what message to send:



Action name:

Supported platforms: iOS

Action description:

VPP account: conant@mycompany.com

○ Register only

Users who are only registered must be invited separately before they can download and use apps from the VPP program.

● Register and invite by:

☑ MDM (iOS 7.0.3 or newer, macOS 10.9 or newer)

☑ E-mail

☐ LANrev Apps message (iOS only)

☐ SMS

☐ Web Clip (iOS only)

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text:

```
${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the
${MDU_Company} Apple Volume Purchase Program (VPP)
account:

${MD_VPPInviteURL}

This will enable you to receive company-paid apps on your
Apple
device at no cost to you, and will enable the company to assign
```

SMS text:

```
To receive company-paid apps, please visit this URL to register
your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}
```

Character count: 133

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: The account in which you want to register the users of the devices. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
- **Register only**: If this option is checked, the users affected by this action are registered for your VPP account, but not invited to link their Apple ID to the account. This invitation has to happen later through the **New Send VPP Invitation Action** action or the **Send VPP Invitation** command.
  This two-step process is faster on Apple's back-end then immediately inviting users and is therefore recommended if you expect to process large numbers of users in one go.
- **Register and invite by**: Check all channels over which you want to send the registration notice to the users. (Users need to complete the registration themselves by entering their personal Apple ID on Apple's VPP website.)

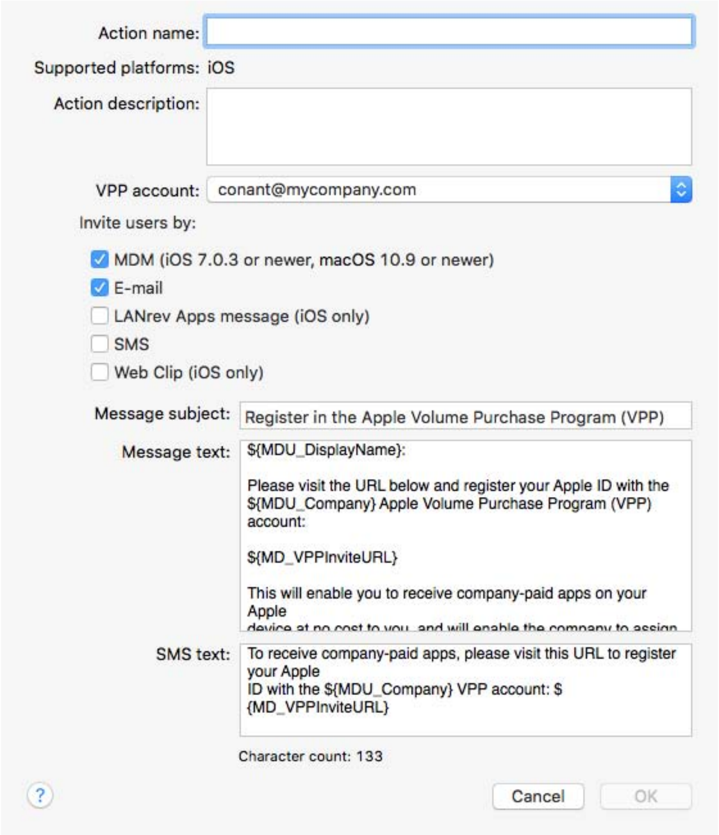
Invitations via MDM can only be sent to clients running iOS 7.0.3 and above; LANrev Apps messages can be sent only to mobile devices on which LANrev Apps is installed.
If invitations are sent via web clip, the icon and label of the clip can be configured by editing the predefined “VPP Invite Web Clip” configuration profile. (Do not change the URL in the profile.)
For registering a large number of users, this option can be slower than choosing **Register only**.

- **E-Mail subject**: The subject text for the invitation e-mail.
In this text, you can use the variables described in “Variables for mobile devices” on page 458.
- **Message text**: The text of the message sent via e-mail or LANrev Apps message.
In this text, you can use the variables described in “Variables for mobile devices” on page 458.
In addition, you can use the MD_VPPInviteURL variable, which is displayed as a link to the web page in the App Store where the users have to enter her or his Apple ID to register for the VPP account of your organization.
- **SMS text**: The text of the message sent via SMS.
You can use the same variables as for **Message text**.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Send VPP Invitation Action

This command opens the **Send VPP Invitation Action** dialog in which you can specify a VPP account to which devices on which the action is executed are added. You can also specify the invitation message to send:



Action name:

Supported platforms: iOS

Action description:

VPP account: conant@mycompany.com

Invite users by:

☑ MDM (iOS 7.0.3 or newer, macOS 10.9 or newer)
☑ E-mail
☐ LANrev Apps message (iOS only)
☐ SMS
☐ Web Clip (iOS only)

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text: ${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

${MD_VPPInviteURL}

This will enable you to receive company-paid apps on your Apple
device at no cost to you, and will enable the company to assign

SMS text: To receive company-paid apps, please visit this URL to register your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}

Character count: 133

The dialog contains these elements:

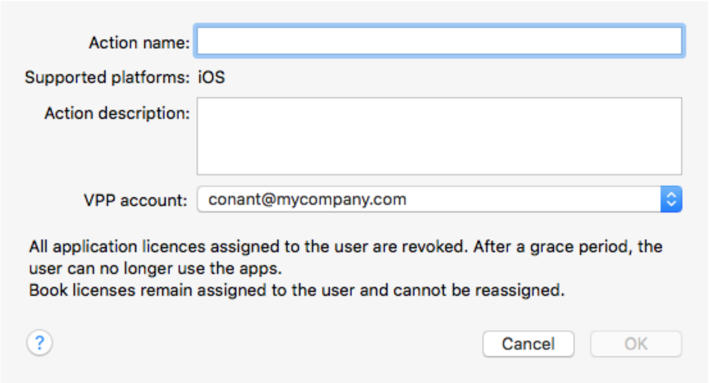
- **Action name**: The name under which the action is stored in LANrev.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: The account in which you want to register the users of the devices. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
- **Invite users by**: Check all channels over which you want to send the registration notice to the users. (Users need to complete the registration themselves by entering their personal Apple ID on Apple’s VPP website.)
  Invitations via MDM can only be sent to clients running iOS 7.0.3 and above; LANrev Apps messages can be sent only to mobile devices on which LANrev Apps is installed.
  If invitations are sent via web clip, the icon and label of the clip can be configured by editing the predefined “VPP Invite Web Clip” configuration profile. (Do not change the URL in the profile.)
- **Message subject**: The subject text for the invitation e-mail. In this text, you can use the variables described in “Variables for mobile devices” on page 458.

- **Message text**: The text of the message sent via e-mail or LANrev Apps message.
  In this text, you can use the variables described in "Variables for mobile devices" on page 458.
  In addition, you can use the MD_VPPInviteURL variable, which is displayed as a link to the web page in the App Store where the users have to enter her or his Apple ID to register for the VPP account of your organization.
- **SMS text**: The text of the message sent via SMS.
  You can use the same variables as for **Message text**.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Retire User from VPP Action

This command opens the **Retire User from VPP Action** dialog in which you can specify the VPP account from which to remove devices:



Action name:

Supported platforms: iOS

Action description:

VPP account: conant@mycompany.com

All application licences assigned to the user are revoked. After a grace period, the user can no longer use the apps.
Book licenses remain assigned to the user and cannot be reassigned.

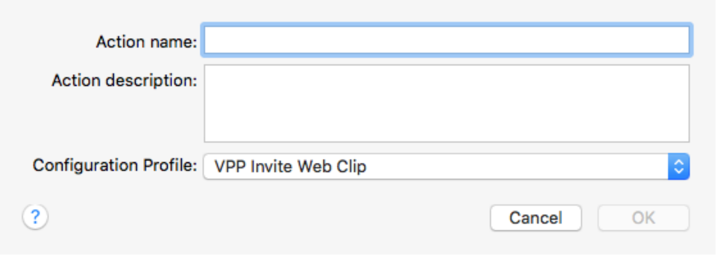
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: A list of all available VPP accounts. The target devices will be removed from the selected account when the action is triggered.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Remove Configuration Profile Action

This command opens the **Remove Configuration Profile Action** dialog in which you can specify a configuration profile that is to be removed from a mobile device when it becomes a member of a policy:



Action name:

Action description:

Configuration Profile: VPP Invite Web Clip

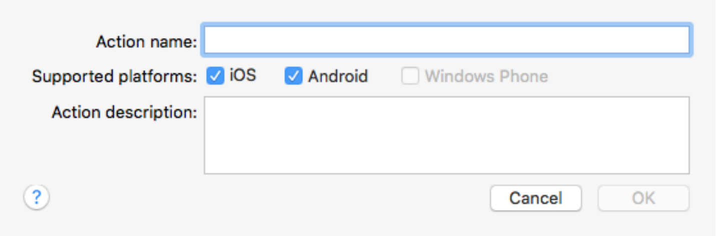
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Configuration profile**: A list of all available configuration profiles. The chosen profile will be removed from the target devices when the action is triggered.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which executes it automatically when a device becomes a member of the policy.

New Demote to Unmanaged Device Action

This command opens the **Demote to Unmanaged Device Action** dialog in which you can specify that a device is removed from MDM management when it becomes the member of a smart policy:



Action name:

Supported platforms: ☑ iOS ☑ Android □ Windows Phone

Action description:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply.

- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.

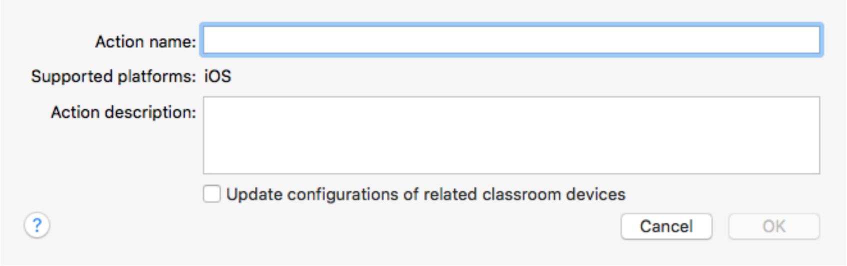
Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev removes the device from MDM management. This action cannot be reversed inside LANrev; the device must first be enrolled anew.

Note that removing a device from MDM management may prevent you from performing actions on the device that have MDM management as a prerequisite. For example, the device is automatically removed from classroom management.

New Configure Devices for Current Classroom Setup Action

This command opens the **Configure Devices for Current Classroom Setup Action** dialog in which you can specify that a device is updated for the classroom configuration current at the time the action is executed:


Action name:
Supported platforms: iOS
Action description:
□ Update configurations of related classroom devices

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The mobile device platforms to which you want the action to apply. This action can only be applied to iOS devices.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Update configurations of related classroom devices**: If this option is checked, not only will the configurations of devices added to a policy be updated, but also those of related devices, such as the teacher’s device in a class to which student devices are added.

Unless you have a specific reason to update only the devices on which the action is executed, we recommend that you check this option to avoid inconsistent configurations.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart policy, which applies it automatically to all devices that are currently members of the policy. It will also be applied to any device that becomes a member of the policy when it becomes a member.

When the action is applied to a device, LANrev updates the device configuration according to the settings in the **Classroom Management**. Note that the configuration that is current at the time of the execution of the action is applied, not the configuration as it is when you define the action.

This action affects only devices that are enrolled in Apple School Manager.

Duplicate Action

This command duplicates the selected action and opens the dialog for editing it. Which dialog it opens depends on the type of the duplicated action. See "Actions" on page 570 for an overview of the available dialogs.

New Smart Group: Actions

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that includes all actions meeting the specified criteria. See "Working with actions" on page 232 for more information on actions.

For details on the **Smart Group** dialog, see "New Smart Group" on page 522.

Policies

The **Policies** submenu contains commands for working with configuration profiles:

- "New Policy" on page 596
- "New Smart Policy: Mobile Devices" on page 596
- "New Smart Policy: Mobile Devices by Installed Applications" on page 596
- "New Smart Policy: Mobile Devices by Installed Configuration Profiles" on page 596

New Policy

This command opens the **New Mobile Device Policy** dialog in which you can specify a name for a new policy.

A policy groups administered mobile with permitted and prohibited applications as well as required and prohibited configuration profiles. See “Working with policies” on page 245 for more information.

New Smart Policy: Mobile Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy that includes all mobile devices meeting the specified criteria. See “Working with policies” on page 245 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 522.

New Smart Policy: Mobile Devices by Installed Applications

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy in which you can specify mobile devices by applications that are installed or not installed on them. See “Working with policies” on page 245 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 522.

New Smart Policy: Mobile Devices by Installed Configuration Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart mobile device policy in which you can specify mobile devices by configuration profiles that are installed or not installed on them. See “Working with policies” on page 245 for more information.

For details on the **Smart Group** dialog, see “New Smart Group” on page 522.

Device Enrollment Profiles

The **Device Enrollment Profiles** submenu contains commands for working with device enrollment profiles:

- “New Enrollment Profile” on page 597
- “New Smart Group: Enrollment Profiles” on page 603

New Enrollment Profile

This command lets you create a new device enrollment profile for iOS and macOS devices that are part of Apple’s device enrollment program (ADEP). Choosing the command opens the **Device Enrollment Profile Editor** dialog, described below.

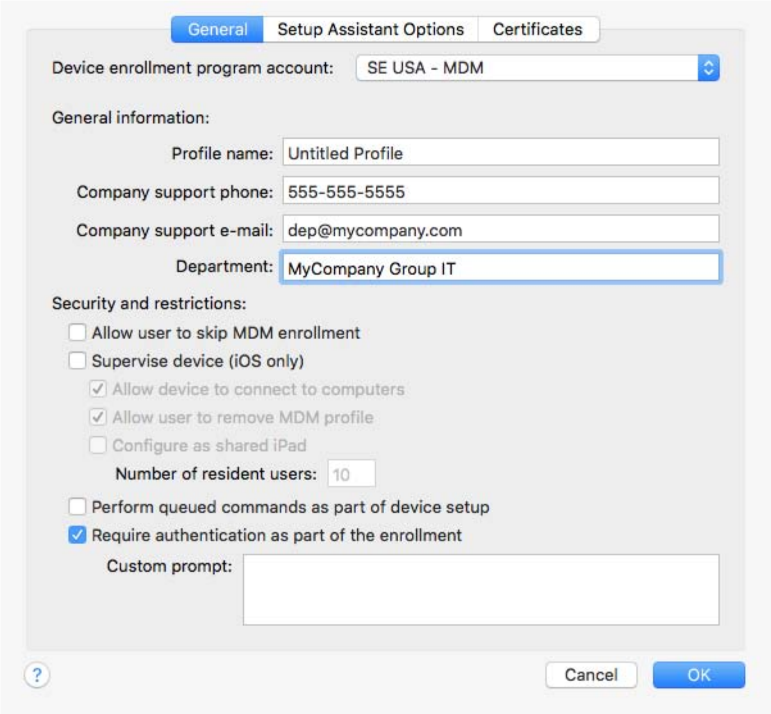
The **Device Enrollment Profile Editor** dialog lets you create enrollment profiles for devices that are part of Apple’s device enrollment program (ADEP). Such profiles let you specify setup steps to skip as well as some basic access and security settings.

The dialog has three panes:

- General
- Setup Assistant Options
- Certificates

General

The **General** pane of the **Device Enrollment Profile Editor** dialog lets you specify the enrollment account and set basic enrollment options.



Device enrollment program account: SE USA - MDM

General information:

Profile name: Untitled Profile

Company support phone: 555-555-5555

Company support e-mail: dep@mycompany.com

Department: MyCompany Group IT

Security and restrictions:

- □ Allow user to skip MDM enrollment
- □ Supervise device (iOS only)
  - ☑ Allow device to connect to computers
  - ☑ Allow user to remove MDM profile
  - □ Configure as shared iPad
  - Number of resident users: 10
- □ Perform queued commands as part of device setup
- ☑ Require authentication as part of the enrollment

Custom prompt:

The pane contains these elements:

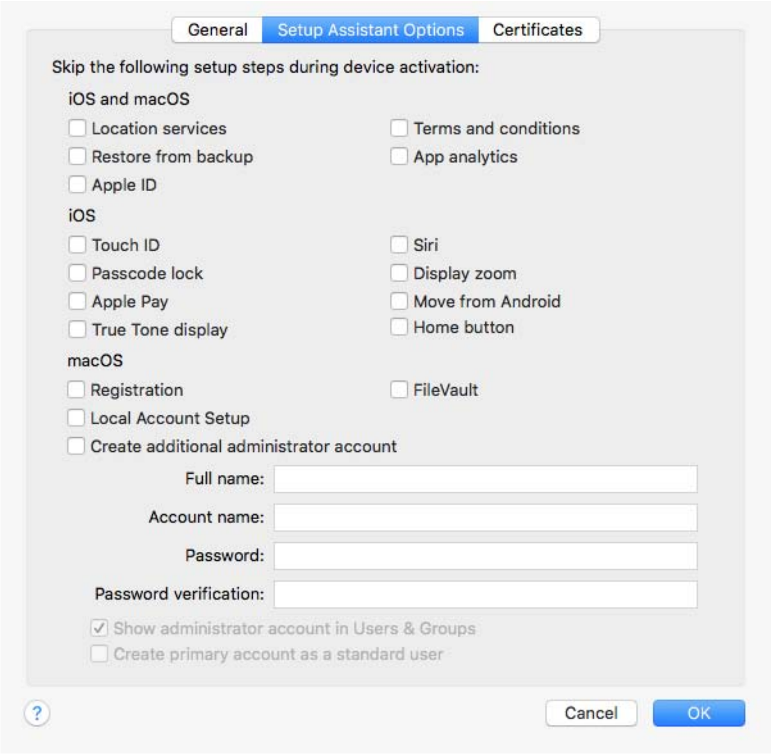
- **Device enrollment program account**: This list contains all device enrollment accounts that have been configured in the **MDM** tab of the server settings.
- **General information**: Free-form information for the profile.
  - **Profile name**: The name under which the profile is listed in LANrev.
  - **Company support phone**: The phone number that users should call for any MDM-related support issues. (This field may be left empty.)
  - **Company support e-mail**: The e-mail address that users should contact for any MDM-related support issues. (This field may be left empty.)
  - **Department**: The department of your organization which manages the devices set up through this profile.
- **Security and restrictions**: This section lets you set some fundamental security- and access-related options:
  - **Allow user to skip MDM enrollment**: If this option is checked, users can decide during the setup process whether to allow their device to be managed through MDM.
    If the option is unchecked, the user may choose not to enroll the device in MDM. In this case, most of the other settings in this dialog have no effect, except for **Supervise device** and **Allow device to connect to computers**.

- **Supervise device**: If this option is checked, the device becomes a supervised device. Supervised devices allow more management options, such as setting the state of the personal hotspot.
- **Allow device to connect to computers**: If this option is checked, the device can be connected to any desktop computer over USB, for example, for iTunes synchronization or to download photos.
  If the option is unchecked, such connection is possible only with computers for which a pairing certificate is installed on the device, as described in "Certificates", below.
  This option is always checked for unsupervised devices. In other words, only supervised devices can be prevented from connecting to computers.
- **Allow user to remove MDM profile**: If this option is checked, the user of the enrolled device may delete the MDM profile at some point after enrollment. Doing so removes the device from MDM and disables any restrictions that may have been configured on it.
  If the option is unchecked, the user cannot remove the device from MDM.
  This option is always checked for unsupervised devices. In other words, the user can only be prevented from removing the profile on supervised devices.
- **Configure as shared iPad**: If this option is checked, the enrolled device can be shared by multiple users. If it is not checked, the device has only one user.
  This option is available only for iPads running iOS 9.3 or up. The devices must be set to be supervised, and the **Perform queued commands as part of device setup** option (see below) is automatically checked.
- **Number of resident users**: Specify how many users can keep their data on this shared device (space permitting). if more users log into the device, data for the longest-dormant user is automatically removed, although it is being kept in iCloud.
  This option applies only to devices being set up as a shared device.
- **Perform queued commands as part of device setup**: If this option is checked, any commands that are queued for the device are executed on the device during the setup process. The user cannot start using the device before all these commands are excuted.
  Queued commands come from policies to which the device belongs. Some of these commands that are not setup commands (for example, application installations) are executed after the setup process even if this option is checked.
  This option is always checked when **Configure as shared iPad** (see above) is checked.
- **Require authentication as part of the enrollment**: If this option is checked, a user must specify an Active Directory account as part of the setup process. This requires LANrev Server to be connected to an Active Directory server.

- **Custom prompt**: The prompt in this field is displayed instead of the default prompt specified by Apple when users are requested to enter their credentials during device activation.

Setup Assistant Options

The **Setup Assistant Options** pane of the **Device Enrollment Profile Editor** dialog lets you specify which steps to skip during the first launch setup procedure on the device. Users cannot specify any settings for these modules.



Skip the following setup steps during device activation:

iOS and macOS

□ Location services
□ Restore from backup
□ Apple ID
□ Terms and conditions
□ App analytics

iOS

□ Touch ID
□ Passcode lock
□ Apple Pay
□ True Tone display
□ Siri
□ Display zoom
□ Move from Android
□ Home button

macOS

□ Registration
□ Local Account Setup
□ Create additional administrator account
□ FileVault

Full name:
Account name:
Password:
Password verification:

☑ Show administrator account in Users & Groups
□ Create primary account as a standard user

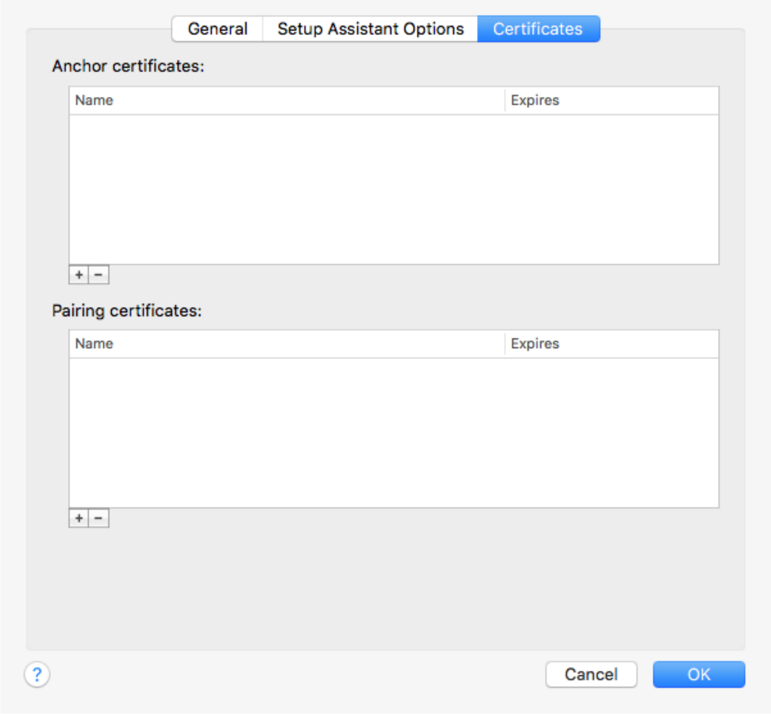
The pane contains these elements:

- **iOS and macOS**: Options that affect both iOS and macOS devices.
  - **Location services**: Whether to activate location services on the device.
  - **Restore from backup**: Whether to set up the device from an existing backup (instead of from scratch).
  - **Apple ID**: Whether and which Apple ID to specify for the user of the device.
  - **Terms and conditions**: Whether the user accepts Apple’s terms and conditions.
  - **App analytics**: Whether the user wants to allow the device send device analytics data to Apple.
- **iOS**: Options that affect only iOS devices.
  - **Touch ID**: Whether to activate and train Touch ID.
  - **Passcode lock**: Whether to specify a passcode that is required for unlocking the device.
  - **Apple Pay**: Whether to enable the device for making payments using Apple Pay.

  - **True Tone display**: Whether to enable the True Tone display on the device. This affects only devices that have a True Tone display.
  - **Siri**: Whether to enable Siri on the device.
  - **Display zoom**: Whether to enable the Display Zoom function on the device.
  - **Move from Android**: Whether to transfer data from an Android device as part of the setup process.
  - **Home button**: Whether to set up the function of the home button.
- **macOS**: Options that affect only macOS devices.
  - **Registration**: Whether to provide registration information to Apple.
  - **FileVault**: Whether to activate FileVault on the device.
  - **Local account setup**: Whether the screen to set up a local account is skipped.
    If you set the device to skip this step, you must set up an administrator account (see below). Also, users will not be able to use the device unless they have a network account for it.
  - **Create additional administrator account**: Whether to set up an administrator account on the computer, in addition to any user account created through the setup screen. You must specify the name and password for the account.
    If the local account setup screen is skipped, you must create an administrator account.
    - **Full name**: The full name of the administrator account.
    - **Account name**: The short name of the account. This is the name for the home folder. It can also be used as the login name (instead of the full account name).
    - **Password** and **Password verification**: The password for the account.
    - **Show administrator account in Users & Groups**: Whether the additional administrator account is visible in the Users & Groups system settings. This setting has no effect on a local user account created in the setup screen, even if that account is an administrator account.
    - **Create primary account as a standard user**: If this option is checked, the local user can only create an account that has no administrator access. If it is unchecked, the account is created as normal as an administrator account.

Certificates

The **Certificates** pane of the **Device Enrollment Profile Editor** dialog lets you manage the certificates for fallback MDM verification and iOS computer device pairing.



The pane contains these elements:

- **Anchor certificates**: These SSL certificates will be installed on the mobile devices to which this enrollment profile is assigned. They are intended to allow the device to verify the identity of the MDM server in situations where it cannot verify the entire trust chain.
  Usually, this field can be left empty.
  Clicking the **+** button below the list lets you import a new certificate; clicking the **–** button removes the selected certificates from the list.
- **Pairing certificates**: This is a list of certificates from Macs that are allowed to configure the mobile devices through the Apple Configurator utility.
  Only Macs authorized through a certificate in this list can access the mobile devices if the **Allow computers to connect with device** option (see above) is unchecked. If the option is checked, the **Pairing certificates** list is ignored.
  The certificates for inclusion in this list can be generated in Apple Configurator when it is run on the Mac that is to be authorized.
  Clicking the **+** button below the list lets you import a new certificate; clicking the **–** button removes the selected certificates from the list.

New Smart Group: Enrollment Profiles

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that includes all enrollment profiles meeting the specified criteria.

For details on the **Smart Group** dialog, see “New Smart Group” on page 522.

New Group: Mobile Devices

This command is the **New Group** command standard to all browser windows. It creates a group for mobile devices.

New Smart Group: Mobile Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for mobile devices.

For details, see “New Smart Group” on page 522.

New Smart Group: Command Queue

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for entries in the command queue.

For details, see “New Smart Group” on page 522.

New Smart Group: Command History

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for entries in the command history.

For details, see “New Smart Group” on page 522.

New Category

This command is the **New Category** command standard to all browser windows.

For details, see “New Category” on page 523.

Rename <item>

This command lets you edit the name of the selected item in the sidebar of the **Mobile Devices** window.

Edit <item>

This command lets you edit the selected items from the **Mobile Devices** window. The items are opened in the dialog in which they were created; see these dialogs’ descriptions for details.

Remove <item>

This command lets you remove the selected items from the Mobile Devices window. Not all objects can be removed.

Table context menu

The context menus for the table area of the **Mobile Devices** window contains commands for working with the items displayed and controlling mobile devices.

Depending on the content displayed in the table area, different commands are included in the context menu.

These commands may appear:

- “Copy” on page 607
- “Copy “<information item>”” on page 607
- “New Smart Mobile Device Group from “<information item>”” on page 608
- “New Smart Policy from “<information item>”” on page 608
- “New Smart Application Group from “<information item>”” on page 608
- “New Smart Configuration Profiles Group from “<information item>”” on page 609
- “New Smart Device Enrollment Profiles Group from “<information item>”” on page 609
- “New Smart Provisioning Profiles Group from “<information item>”” on page 609
- “New Smart Media Files Group from “<information item>”” on page 610
- “New Command Queue Smart Group from “<information item>”” on page 610
- “New Command History Smart Group from “<information item>”” on page 610
- “New Policy with Selected Devices” on page 611
- “Install Configuration Profile” on page 611
- “Install Provisioning Profile” on page 611
- “Install Application” on page 611

- “Install Media File” on page 611
- “Change Application Configuration” on page 611
- “Validate Managed Applications” on page 611
- “Validate Selected Applications” on page 612
- “Issue Device Lock” on page 612
- “Issue Clear Passcode” on page 612
- “Issue Clear Restrictions Passcode” on page 612
- “Erase Device” on page 612
- “Set Roaming Options” on page 612
- “Send Message to Device” on page 612
- “Set Wallpaper” on page 613
- “Install iOS Update” on page 613
- “Set Device Name” on page 613
- “Request AirPlay Mirroring” on page 613
- “Stop AirPlay Mirroring” on page 613
- “Change Personal HotSpot State” on page 613
- “Enable Attention Mode” on page 614
- “Disable Attention Mode” on page 614
- “Set Lost Mode” on page 614
- “Set Organization Information” on page 614
- “Set Activation Lock Options” on page 614
- “Enable Activation Lock” on page 614
- “Remove Activation Lock” on page 614
- “Show Activation Lock Bypass Code” on page 614
- “Log Out User” on page 614
- “Delete User Data” on page 615
- “Set Passcode Lock Grace Period” on page 615
- “Set Passcode Lock Grace Period” on page 615
- “Delete Application” on page 616
- “Update Device Information” on page 617
- “Make Device Contact Server” on page 617
- “Remote Control” on page 617
- “Create KNOX Workspace” on page 617
- “Remove KNOX Workspace” on page 617
- “Lock KNOX Workspace” on page 617
- “Unlock KNOX Workspace” on page 617
- “Reset KNOX Workspace Password” on page 618
- “Register Device User in VPP” on page 618
- “Send VPP Invitation” on page 619
- “Retire Device Users from VPP” on page 621
- “Assign Application Licenses to Device Users” on page 621
- “Assign Application Licenses to Devices” on page 622
- “Revoke Application Licenses” on page 624
- “Assign Book Licenses to Device Users” on page 626
- “Assign Book Licenses to Devices” on page 627
- “Remove Users from Server” on page 627
- “Register Users in VPP” on page 627
- “Retire Users from VPP” on page 627
- “Assign Device Enrollment Profile” on page 627
- “Unassign Device Enrollment Profile” on page 628
- “Reload Device Enrollment Data” on page 629
- “Configure Devices for Current Classroom Setup” on page 629
- “Manage Personal Device Assignment” on page 629
- “Delete Profile” on page 629
- “Show Detail View” on page 629

- “Create Home Screen Layout Configuration Profile” on page 630
- “Synchronize Records” on page 630
- “Enter Custom Field Data” on page 630
- “Import Custom Field Data” on page 630
- “Ignore Devices” on page 631
- “Reset All Ignored Devices” on page 631
- “Re-execute All Actions for This Device” on page 631
- “Re-execute This Action for This Device” on page 631
- “Retry All Failed Profiles” on page 631
- “Retry All Failed Applications” on page 632
- “Retry All Failed Books” on page 632
- “Remove from Group” on page 632
- “Remove from Policy” on page 632
- “Track Device” on page 632
- “Get Device Geolocation” on page 632
- “Reset Tracking Passphrase” on page 633
- “Show Location on Google Maps” on page 633
- “Show Location on Bing Maps” on page 633
- “Set Device Ownership” on page 633
- “Set Enrollment User” on page 634
- “Update AD User Information” on page 634
- “Send Re-enrollment Message to Device” on page 634
- “Update Installed Application Statistics” on page 635
- “Show User Details” on page 635
- “Show Mobile Application Package Details” on page 635
- “New Mobile Application Package” on page 636
- “New iOS App Store Application Package” on page 636
- “New Google Play Application Package” on page 636
- “Edit Mobile Application Package” on page 636
- “Duplicate Mobile Application Package” on page 636
- “Remove Mobile Application Package” on page 636
- “Assign Application Licenses to Users” on page 637
- “Revoke Application Licenses” on page 638
- “Show Book Details” on page 638
- “New iBooks Book” on page 639
- “Edit Book” on page 639
- “Duplicate Book” on page 639
- “Remove Book” on page 639
- “Show Configuration Profile Details” on page 640
- “New Configuration Profile” on page 640
- “Edit Configuration Profile” on page 640
- “Remove Configuration Profile” on page 640
- “Remove Configuration Profile from Policy” on page 640
- “Show Device Enrollment Profile Details” on page 640
- “New Device Enrollment Profile” on page 640
- “Edit Device Enrollment Profile” on page 640
- “Duplicate Device Enrollment Profile” on page 641
- “Remove Device Enrollment Profile” on page 641
- “Show Provisioning Profile Details” on page 641
- “Show Media File Details” on page 641
- “Set Availability Time” on page 642
- “New Media File” on page 643
- “Edit Media File” on page 643
- “Remove Media File” on page 643

- “Show Action Details” on page 643
- “Duplicate Action” on page 643
- “Edit Action” on page 643
- “Remove Action” on page 643
- “Re-execute This Action for All Devices” on page 644
- “Re-execute This Action for This Policy” on page 644
- “New Send Message Action” on page 644
- “New Send E-Mail Action” on page 644
- “New Send SMS (Text Message) Action” on page 644
- “New Set Roaming Options Action” on page 644
- “New Set Activation Lock Options Action” on page 645
- “New Enable Activation Lock Action” on page 645
- “New Set Wallpaper Action” on page 645
- “New Set Device Name Action” on page 645
- “New Set Custom Field Value Action” on page 645
- “New Install iOS Update Action” on page 645
- “New Validate Applications Action” on page 645
- “New Update Device Information Action” on page 645
- “New Set Attention Mode Action” on page 646
- “New Set Lost Mode Action” on page 646
- “New Set Passcode Lock Grace Period Action” on page 646
- “New Configure Diagnostic Data Transmission Action” on page 646
- “New Freeze Device Action” on page 646
- “New Clear Passcode Action” on page 646
- “New Retire User from VPP Action” on page 647
- “New Remove Configuration Profile Action” on page 647
- “New Demote to Unmanaged Device Action” on page 647
- “New Configure Devices for Current Classroom Setup Action” on page 647
- “Change Action Schedule” on page 647
- “Remove Action from Policy” on page 648
- “Show Policy Members” on page 648
- “Remove Policy” on page 648

Copy

This command is the **Copy** command from the **Edit** menu.

For details, see “Copy” on page 392.

Copy “<information item>”

This command is the **Copy “<information item>”** command standard to all browser windows.

For details, see “Copy “<information item>”” on page 525.

New Smart Mobile Device Group from "<information item>"

This command is the **New Smart Group from "<information item>"** command standard to all browser windows.

For details, see "New Smart Group from "<information item>"" on page 525.

New Smart Policy from "<information item>"

Choosing this command lets you create a mobile device policy with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart policy.

For details on the dialog, see "New Smart Group" on page 522. For more information on policies, see "Working with policies" on page 245.

New Smart Application Group from "<information item>"

Choosing this command lets you create a smart group for application packages with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see "New Smart Group" on page 522.

New Smart Configuration Profiles Group from “<information item>”

Choosing this command lets you create a smart group for configuration profiles with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Smart Device Enrollment Profiles Group from “<information item>”

Choosing this command lets you create a smart group for device enrollment profiles with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Smart Provisioning Profiles Group from “<information item>”

Choosing this command lets you create a smart group for provisioning profiles with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Smart Media Files Group from “<information item>”

Choosing this command lets you create a smart group for media files with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Command Queue Smart Group from “<information item>”

Choosing this command lets you create a smart group for command queue entries with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Command History Smart Group from “<information item>”

Choosing this command lets you create a smart group for command history entries with prefilled criteria.

Choosing the command opens the **New Smart Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

For details on the dialog, see “New Smart Group” on page 522.

New Policy with Selected Devices

Choosing this command lets you create a new policy that already contains the selected mobile devices.

Choosing the command opens the **New Mobile Device Policy** dialog in which you can specify the name for the new policy.

Install Configuration Profile

This is the same command as **Install Configuration Profile** on page 459.

Install Provisioning Profile

This is the same command as **Install Provisioning Profile** on page 460.

Install Application

This is the same command as **Install Application** on page 461.

Install Media File

This is the same command as **Install Media File** on page 463.

Change Application Configuration

This is the same command as **Change Application Configuration** on page 464.

Validate Managed Applications

Choosing the **Validate Managed Applications** command causes LANrev to trigger a validation of all managed applications on the selected devices that have been installed with enterprise certificates.

iOS 9.2 and up requires this validation every few weeks to allow applications that have been installed with enterprise certificates to continue running. The validation fails if there is no Internet connection.

If a device will be without Internet contact for prolonged periods of time, you can use this command to reset the interval for the next validation, allowing any affected apps to be used for a few weeks before the next validation is required.

For devices with regular Internet contact, this command is not needed.

Validate Selected Applications

Choosing the **Validate Selected Applications** command causes LANrev to trigger a validation of all selected managed applications that have been installed with enterprise certificates.

The command is otherwise similar to **Validate Managed Applications**, described above.

Issue Device Lock

This is the same command as **Issue Device Lock** on page 464.

Issue Clear Passcode

This is the same command as **Issue Clear Passcode** on page 465.

Issue Clear Restrictions Passcode

This is the same command as **Issue Clear Restrictions Passcode** on page 466.

Erase Device

This is the same command as **Erase Device** on page 466.

Set Roaming Options

This is the same command as **Set Roaming Options** on page 467.

Send Message to Device

This is the same command as **Send Message to Device** on page 468.

Set Wallpaper

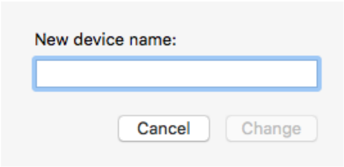
This is the same command as **Set Wallpaper** on page 468.

Install iOS Update

This is the same command as **Install iOS Update** on page 469.

Set Device Name

Choosing this command opens the **New Mobile Device Name** dialog in which you can assign a name to a selected mobile device:



New device name:

The dialog contains this element:

- **New device name**: The name in this field will be assigned to the device.
  In this text, you can use the variables described in “Variables for mobile devices” on page 458.

This command applies only to iOS devices running iOS 8 and above and Android devices.

Request AirPlay Mirroring

This is the same command as **Request AirPlay Mirroring** on page 470.

Stop AirPlay Mirroring

This is the same command as **Stop AirPlay Mirroring** on page 471.

Change Personal HotSpot State

This is the same command as **Change Personal HotSpot State** on page 471.

Enable Attention Mode

This is the same command as **Enable Attention Mode** on page 473.

Disable Attention Mode

This is the same command as **Disable Attention Mode** on page 473.

Set Lost Mode

This is the same command as **Set Lost Mode** on page 474.

Set Organization Information

This is the same command as **Set Organization Information** on page 475.

Set Activation Lock Options

This is the same command as **Set Activation Lock Options** on page 471.

Enable Activation Lock

This is the same command as **Enable Activation Lock** on page 472.

Remove Activation Lock

This is the same command as **Remove Activation Lock** on page 472.

Show Activation Lock Bypass Code

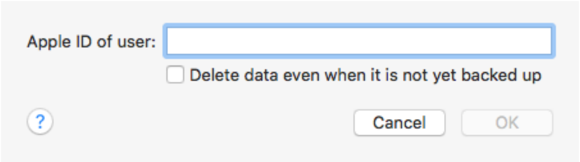
This is the same command as **Show Activation Lock Bypass Code** on page 472.

Log Out User

Choosing this command logs out the currently logged-in user on shared mobile devices. The command applies only to supervised shared devices running iOS 9.3 and up.

Delete User Data

Choosing this command removes the data of a user of a shared device from the device. The command applies only to supervised shared devices running iOS 9.3 and up.



Apple ID of user:

□ Delete data even when it is not yet backed up

The dialog contains these elements:

- **Apple ID of user**: The Apple ID of the user whose data you want to delete.
- **Delete data even when it is not yet backed up**: By default, this command will only delete user data when it has been fully synchronized with iCloud. If you check this checkbox, the user data is removed even if it has not yet been synchronized.

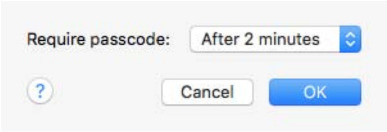
IMPORTANT Deleting user data that has not yet been backed up may lead to irrecoverable data loss. Use this option only when you are certain that no important data can be lost.

Clicking **OK** deletes the data of the selected user from the device, but leaves it available in iCloud.

Note that the data of a user who is still logged in cannot be deleted.

Set Passcode Lock Grace Period

Choosing this command lets you specify the passcode lock grace period for an administered device. The command applies only to supervised shared devices running iOS 9.3.2 and up.



Require passcode: After 2 minutes

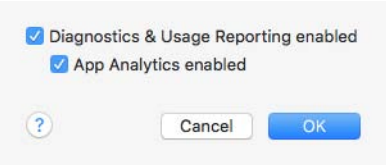
The dialog contains these elements:

- **Require passcode**: Choose the passcode lock grace period from this menu.
  The grace period is the amount of time between the moment when the device locks (the screen is deactivated) and the moment when unlocking it again requires entering the passcode or, if the device has Touch ID, providing a fingerprint.

Clicking **OK** sets the grace periods of the selected devices to the specified value.

Configure Diagnostic Data Transmission

Choosing this command lets you view and specify which diagnostic data the selected devices are transmitting to Apple. The command applies only to devices running iOS 9.3.2 and up.



☑ Diagnostics & Usage Reporting enabled

☑ App Analytics enabled

The dialog contains these elements:

- **Diagnostics & Usage Reporting enbled**: If this option is checked, the device sends daily diagnostic and usage data to Apple.
- **App Analytics enbled**: If this option is checked, the device sends crash and usage data to Apple for forwarding to the app‘s developers.

The two options correspond to settings found in the **Privacy** part of the Settings app in iOS.

Clicking **OK** sets the reporting of the selected devices to specified settings.

Delete Application

Choosing this command removes the selected applications from the mobile devices on which they are installed.

If the app has been running with a VPP device license, LANrev automatically removes that license from the device. (User licenses are not automatically removed, because the same user may use that app on other devices with the same license.)

This command can be used only to delete installed applications, such as when the list of applications on a particular device or the list of all applications are displayed.

Which applications can be removed depends on the mobile OS:

- iOS 4.x: No applications can be removed.
- iOS 5.0 and later: Managed applications can be removed, that is, applications that have been installed through the MDM system. No user confirmation is required.
- Android: Any application can be removed. The local user must confirm the removal, except on devices that support persistence.
- Windows Phone: Deleting applications is not supported.

Update Device Information

This is the same command as **Update Device Information** on page 475.

Make Device Contact Server

This command sends push notifications to all selected devices. Upon receipt of these notifications, the devices contact the MDM server.

This is useful in trouble-shooting scenarios or when a push notification may have been lost. For example, if a device was offline for a long time (several weeks or months), push notifications for the device may have been removed from the Apple or Google server because their time-out expired. In this case, making the device contact the MDM server will allow that server to execute all actions that were scheduled for the device while it was offline.

Remote Control

Choosing this command establishes a screen sharing session with the selected device and opens an **LANrev Remote** window in which the screen of the device is displayed (if the user of the device accepts the connection).

This command works only with mobile devices on which the LANrev Remote app is installed.

Create KNOX Workspace

This is the same command as **Create KNOX Workspace** on page 476.

Remove KNOX Workspace

This is the same command as **Remove KNOX Workspace** on page 476.

Lock KNOX Workspace

This is the same command as **Lock KNOX Workspace** on page 477.

Unlock KNOX Workspace

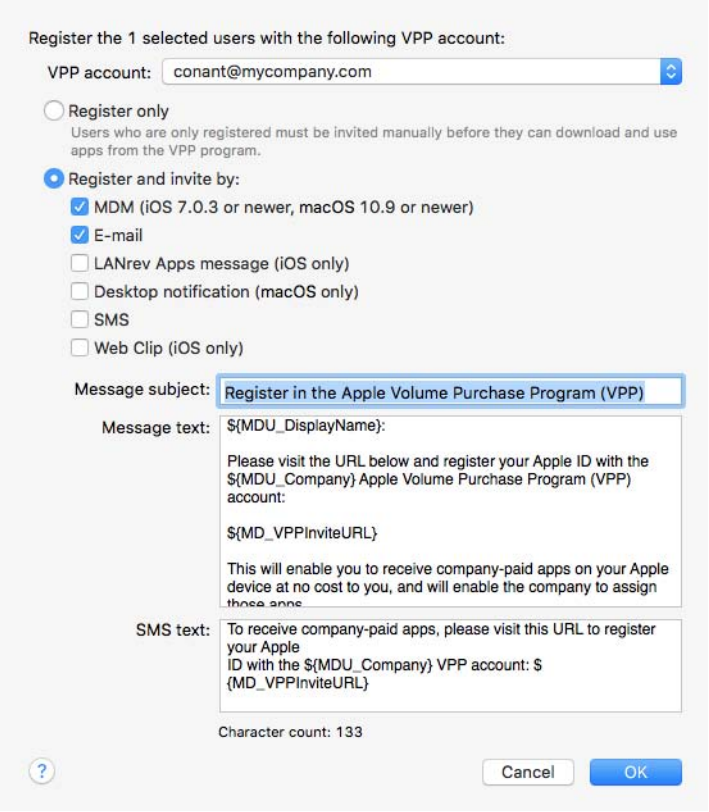
This is the same command as **Unlock KNOX Workspace** on page 477.

Reset KNOX Workspace Password

This is the same command as **Reset KNOX Workspace Password** on page 477.

Register Device User in VPP

Choosing this command opens the **Register Users in VPP** dialog, in which you can assign the selected users to an account of your company in Apple’s volume purchasing program (VPP):



Register the 1 selected users with the following VPP account:

VPP account: conant@mycompany.com

○ Register only

Users who are only registered must be invited manually before they can download and use apps from the VPP program.

● Register and invite by:

- ☑ MDM (iOS 7.0.3 or newer, macOS 10.9 or newer)
- ☑ E-mail
- □ LANrev Apps message (iOS only)
- □ Desktop notification (macOS only)
- □ SMS
- □ Web Clip (iOS only)

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text: ${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

${MD_VPPInviteURL}

This will enable you to receive company-paid apps on your Apple device at no cost to you, and will enable the company to assign those apps

SMS text: To receive company-paid apps, please visit this URL to register your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}

Character count: 133

The dialog contains these elements:

- **VPP account**: The account in which you want to register the users. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
- **Register only**: If this option is checked, the users affected by this action are registered for your VPP account, but not invited to link their Apple ID to the account. This invitation has to happen later through the **New Send VPP Invitation Action** action or the **Send VPP Invitation** command.
  This two-step process is faster on Apple’s servers than immediately inviting users and is therefore recommended if you expect to process large numbers of users in one go.
- **Register and invite by**: Check all channels over which you want to send the registration notice to the users. (Users need

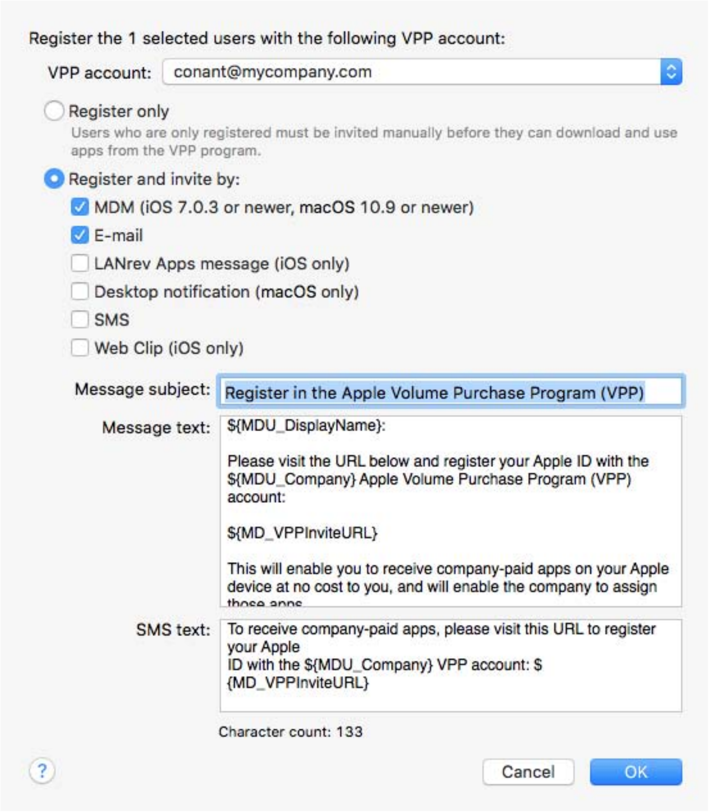
to complete the registration themselves by entering their personal Apple ID on Apple's VPP website.)
Invitations via MDM can only be sent to clients running iOS 7.0.3 and above; LANrev Apps messages can be sent only to mobile devices on which LANrev Apps is installed.
If invitations are sent via web clip, the icon and label of the clip can be configured by editing the predefined "VPP Invite Web Clip" configuration profile. (Do not change the URL in the profile.)
For registering a large number of users, this option can be slower than choosing **Register only**.

- **Message subject**: The subject text for the invitation e-mail.
  In this text, you can use the variables described in "Variables for mobile devices" on page 458.
- **Message text**: The text of the message sent via e-mail or LANrev Apps message.
  In this text, you can use the variables described in "Variables for mobile devices" on page 458.
  In addition, you can use the `MD_VPPInviteURL` variable, which is displayed as a link to the web page in the App Store where the users have to enter her or his Apple ID to register for the VPP account of your organization.
- **SMS text**: The text of the message sent via SMS.
  You can use the same variables as for **Message text**.

Clicking **OK** in this dialog sends the message to the users. To complete the registration, each user has to visit the App Store page and enter her or his Apple ID.

Send VPP Invitation

Choosing this command opens the **Send VPP Invitation** dialog, in which you can send a message to a user to take part in Apple's volume purchasing program (VPP). The user must already be registered with your VPP account, for example with the **Register Device User in VPP** command:



Register the 1 selected users with the following VPP account:

VPP account: conant@mycompany.com

○ Register only
Users who are only registered must be invited manually before they can download and use apps from the VPP program.

● Register and invite by:

☑ MDM (iOS 7.0.3 or newer, macOS 10.9 or newer)
☑ E-mail
□ LANrev Apps message (iOS only)
□ Desktop notification (macOS only)
□ SMS
□ Web Clip (iOS only)

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text:
${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

${MD_VPPInviteURL}

This will enable you to receive company-paid apps on your Apple device at no cost to you, and will enable the company to assign those apps

SMS text: To receive company-paid apps, please visit this URL to register your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}

Character count: 133

The dialog contains these elements:

- **VPP account**: The account to which you want to invite the users. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
  The user must already be registered in this account.
- **Send invite via**: Check all channels over which you want to send the registration notice to the users. (Users need to complete the registration themselves by entering their personal Apple ID on Apple's VPP website.)
  Some ways of sending the invitation apply only to some target devices, as noted in parentheses behind the options.
  If invitations are sent via web clip, the icon and label of the clip can be configured by editing the predefined "VPP Invite Web Clip" configuration profile. (Do not change the URL in the profile.)
- **Message subject**: The subject text for the invitation e-mail.
  In this text, you can use the variables described in "Variables for mobile devices" on page 458.
- **Message text**: The text of the message sent via e-mail or LANrev Apps message.
  In this text, you can use the variables described in "Variables for mobile devices" on page 458.
  In addition, you can use the `MD_VPPInviteURL` variable, which is displayed as a link to the web page in the App Store

where the users have to enter her or his Apple ID to link it to the VPP account of your organization.

- **SMS text**: The text of the message sent via SMS.
  You can use the same variables as for **Message text**.

Clicking **OK** in this dialog sends the message to the users. To be able to access the VPP account, each user has to visit the App Store page and enter her or his Apple ID.

Retire Device Users from VPP

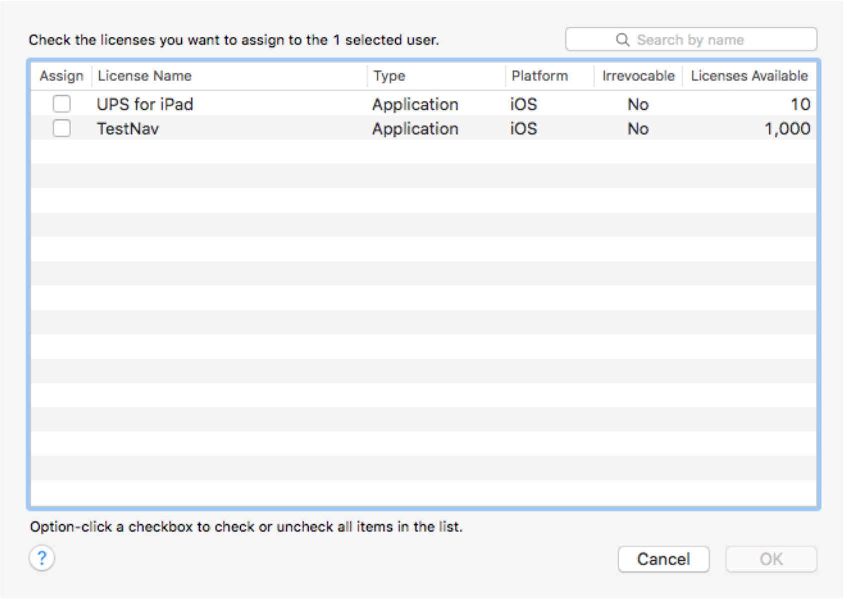
Choosing this command removes the selected users from the VPP account to which they were assigned.

Any apps purchased through this account remain on the users' devices but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

Any books purchased through the account remain available to the users, and the licenses do not become available for reassignment to other users.

Assign Application Licenses to Device Users

Choosing this command opens the **Assign Application Licenses to Users** dialog, in which you can assign application licenses from your organization's VPP account to the user of the selected device:



Check the licenses you want to assign to the 1 selected user.

Assign	License Name	Type	Platform	Irrevocable	Licenses Available
☐	UPS for iPad	Application	iOS	No	10
☐	TestNav	Application	iOS	No	1,000

Option-click a checkbox to check or uncheck all items in the list.

The dialog lists all app licenses that are still available (purchased but not yet assigned) in the VPP account in which the user is registered. In the list, the licenses that are to be assigned to the user can be checked.

Entering text in the search field in the top left filters the list by license name.

Clicking **OK** assigns all licenses with a checkmark in the **Assign** column to the selected users.

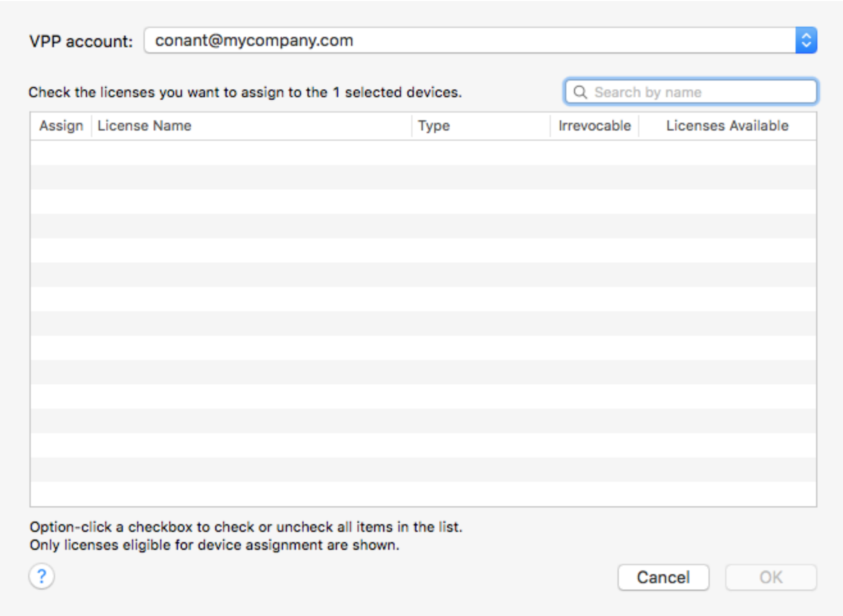
Assign Application Licenses to Devices

Choosing this command opens the **Assign Application Licenses to Devices** dialog, in which you can assign application licenses from your organization’s VPP account to devices.

There are two variants of the dialog, described separately below, depending on whether you right-click app store apps or devices.

When devices are selected

Choosing the command with devices selected opens the dialog with a list of licenses that you can assign to the selected devices:



VPP account: conant@mycompany.com

Check the licenses you want to assign to the 1 selected devices.

Assign	License Name	Type	Irrevocable	Licenses Available

Option-click a checkbox to check or uncheck all items in the list.
Only licenses eligible for device assignment are shown.

The **VPP account** pop-up menu lets you select a VPP account from which to assign licenses.

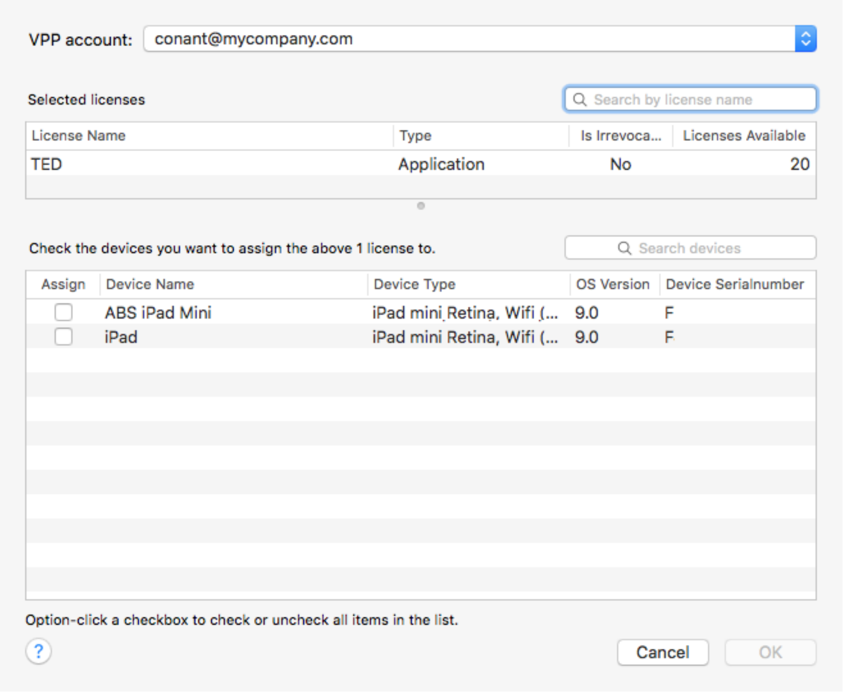
The main list contains all application licenses that are still available (purchased but not yet assigned) in the chosen VPP account. Only licenses for applications that support assignment to devices (as opposed to users) are shown. The licenses that are to be assigned to the user can be checked.

Entering text in the search field in the top left filters the list by license name.

Clicking **OK** assigns all licenses with a checkmark in the **Assign** column to the selected devices.

When apps are selected

Choosing the command with apps selected opens the dialog with a list of devices to which you can assign the selected licenses:



VPP account: conant@mycompany.com

Selected licenses

License Name	Type	Is Irrevoca...	Licenses Available
TED	Application	No	20

Check the devices you want to assign the above 1 license to.

Assign	Device Name	Device Type	OS Version	Device Serialnumber
□	ABS iPad Mini	iPad mini Retina, Wifi (...	9.0	F
□	iPad	iPad mini Retina, Wifi (...	9.0	F

Option-click a checkbox to check or uncheck all items in the list.

The **VPP account** pop-up menu lets you select a VPP account from which to assign licenses. The menu lists only accounts which contain licenses for at least one selected application.

The **Selected licenses** field displays the apps for which licenses are available in the chosen account, together with basic information on each app.

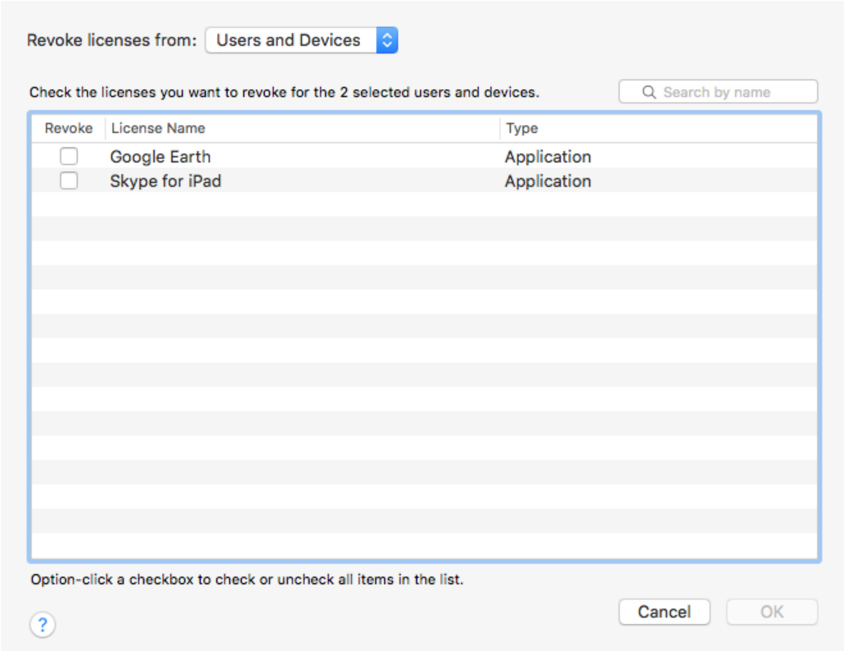
The main list contains all devices to which app licenses can be assigned (that is, all devices running iOS 9 and up). Devices that are to receive licenses must be checked in the **Assign** column.

Entering text in the search field in the top left filters the list by device name.

Clicking **OK** assigns to each checked device one license of each type displayed in the **Selected licenses** field.

Revoke Application Licenses

This command opens the **Revoke Application Licenses** dialog, in which you can revoke application licenses that have been assigned to the selected users or to their devices.



Revoke licenses from: Users and Devices

Check the licenses you want to revoke for the 2 selected users and devices.

Revoke	License Name	Type
□	Google Earth	Application
□	Skype for iPad	Application

Option-click a checkbox to check or uncheck all items in the list.

The pop-up menu at the top lets you choose whether to revoke licenses that have been assigned to users, licenses assigned to devices, or both.

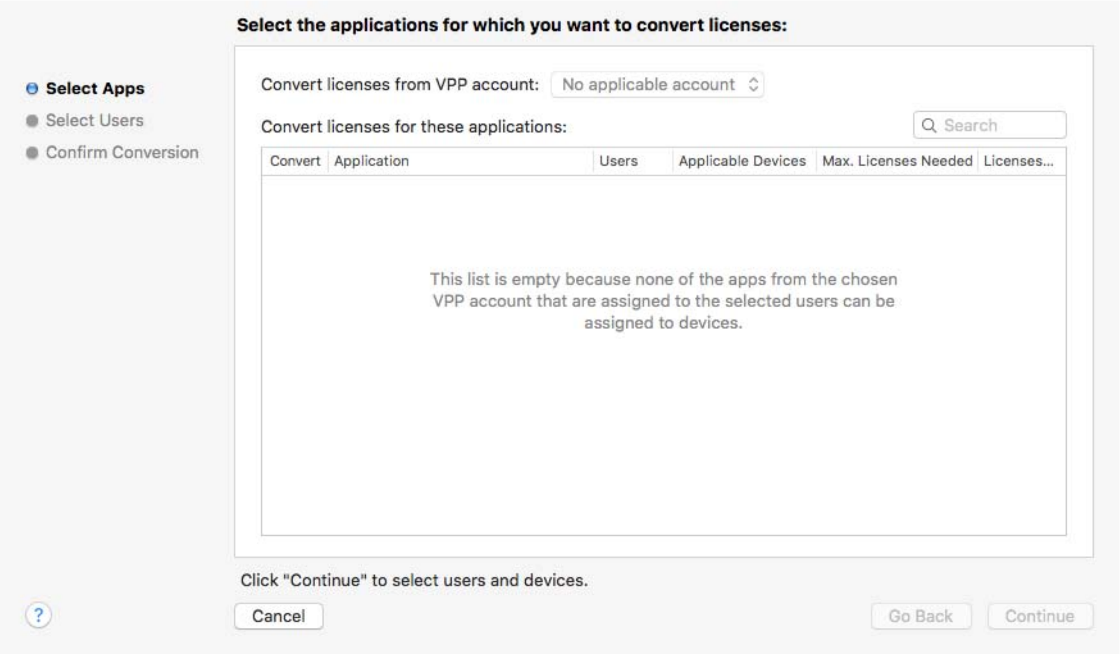
The list includes all VPP apps for which licenses have been assigned to at least one selected user. Apps can be marked for revocation in the **Revoke** column.

Clicking **OK** revokes the licenses for the marked apps. They remain on the users' devices but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

Convert Application Licenses from Users to Devices

This command opens the license conversion assistant, in which you can convert licenses from application licenses to device license and reassign them from users to devices of those users.

Only licenses for application that support device licensing can be converted.



Select the applications for which you want to convert licenses:

Convert licenses from VPP account: No applicable account

Convert licenses for these applications:

Convert	Application	Users	Applicable Devices	Max. Licenses Needed	Licenses...

This list is empty because none of the apps from the chosen VPP account that are assigned to the selected users can be assigned to devices.

Click "Continue" to select users and devices.

The assistant contains these elements:

- On the first screen:
  - **Convert licenses from VPP account**: This pop-up menu lets you specify the VPP account to which the licenses belong that you want to convert.
  - **Convert licenses for these applications**: This list contains the applications that meet all of these conditions:
    - The application has been licensed through the selected VPP account.
    - A license for the application has been assigned to at least one user of a selected device.
    - The application supports device-assigned licenses.

    The list displays the number of additional licenses that will be needed according to the current conversion settings. This number can be negative when devices are reassigned from users to devices that already have the specified license assigned to them. In that case, the conversion frees up licenses.

    Licenses for applications that are checked in this list can be reassigned in the following steps.
- On the second screen:
  - **Convert the licenses for these users**: This list contains all users with at least one license for an application that was selected in the previous screen.

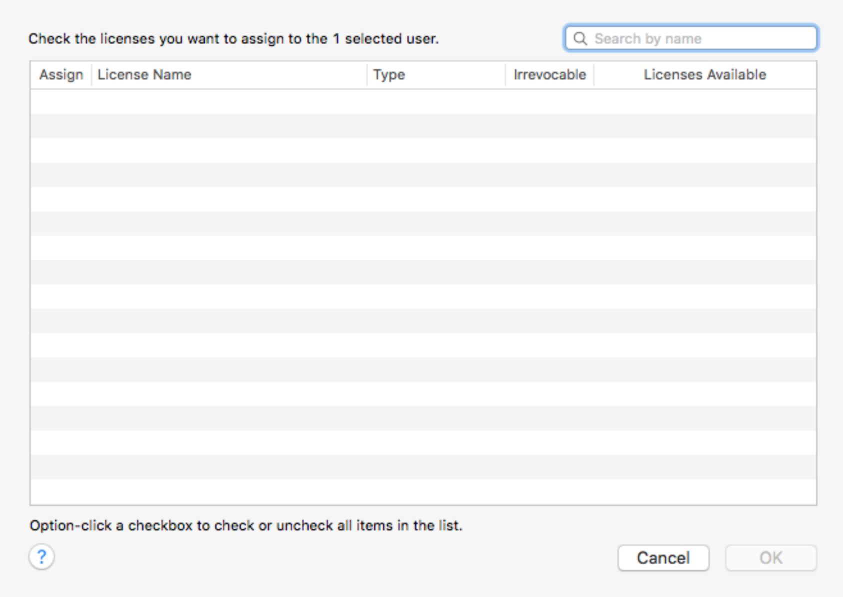
    For all users checked in this list, the licenses for the specified applications will be converted to device licenses.
  - **Reassign the licenses to these devices of the selected user**: The list contains all devices in the MDM system that

belong to the selected user and that support device-assigned licenses (that is, devices running iOS 9 and up). All converted licenses for this user will be assigned to all devices that are checked in this list. If multiple devices are selected, additional licenses from the VPP license pool will be used (in addition to the converted license that was originally assigned to the user).

- The third screen collects the choices from the previous two screens and gives you a chance to review them.
  Clicking **Convert Licenses** on this screen starts the conversion process.

Assign Book Licenses to Device Users

Choosing this command opens the **Assign Book Licenses to Users** dialog, in which you can assign book licenses from your organization's VPP account to the user:


Check the licenses you want to assign to the 1 selected user.

Assign	License Name	Type	Irrevocable	Licenses Available

Option-click a checkbox to check or uncheck all items in the list.

The dialog lists all book licenses that are still available (purchased but not yet assigned) in the VPP account in which the user is registered. In the list, the licenses that are to be assigned to the user can be checked.

Entering text in the search field in the top left filters the list by license name.

Clicking **OK** assigns all licenses with a checkmark in the **Assign** column to the selected users.

Assign Book Licenses

This is the same command as **Assign Book Licenses to Device Users**, described above. The command's title changes in the context menu for users.

Assign Book Licenses to Devices

Choosing this command opens the **Assign Book Licenses to Devices** dialog, in which you can assign application licenses from your organization's VPP account to the selected devices. The command is similar to **Assign Application Licenses to Devices**.

Remove Users from Server

Choosing this command removes mobile device users from LANrev. It can only be applied to users that are neither associated with a device nor registered in a VPP program.

This is a clean-up command that let's you get rid of user records that are no longer needed.

Register Users in VPP

This command is similar to the **Register Device User in VPP** command, which is described on page 618.

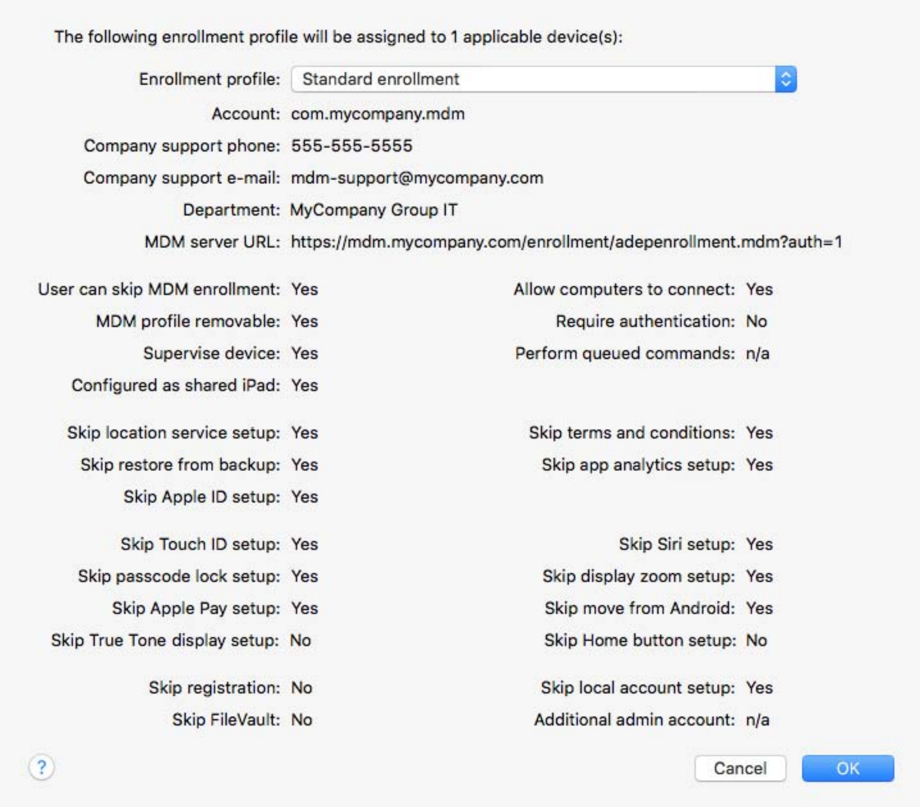
Retire Users from VPP

This command is similar to the **Retire Device Users from VPP** command, which is described on page 618.

Assign Device Enrollment Profile

This command lets you assign one of the device enrollment profiles that have been defined in LANrev to the selected devices.

The command can only be applied to devices that are part of a device enrollment program. Choosing it opens the **Assign Enrollment Profile** dialog:



The following enrollment profile will be assigned to 1 applicable device(s):

Enrollment profile: Standard enrollment

Account: com.mycompany.mdm

Company support phone: 555-555-5555

Company support e-mail: mdm-support@mycompany.com

Department: MyCompany Group IT

MDM server URL: https://mdm.mycompany.com/enrollment/adepenrollment.mdm?auth=1

User can skip MDM enrollment:	Yes	Allow computers to connect:	Yes
MDM profile removable:	Yes	Require authentication:	No
Supervise device:	Yes	Perform queued commands:	n/a
Configured as shared iPad:	Yes		
Skip location service setup:	Yes	Skip terms and conditions:	Yes
Skip restore from backup:	Yes	Skip app analytics setup:	Yes
Skip Apple ID setup:	Yes		
Skip Touch ID setup:	Yes	Skip Siri setup:	Yes
Skip passcode lock setup:	Yes	Skip display zoom setup:	Yes
Skip Apple Pay setup:	Yes	Skip move from Android:	Yes
Skip True Tone display setup:	No	Skip Home button setup:	No
Skip registration:	No	Skip local account setup:	Yes
Skip FileVault:	No	Additional admin account:	n/a

The **Enrollment profile** pop-up menu lets you choose the profile to assign.

The rest of the dialog displays the information contained in the chosen profile.

Unassign Device Enrollment Profile

This command removes the assigned device enrollment profile from all selected devices.

Removing the profile does not immediately change any settings on the device. For example, if it was set to be a supervised device, it remains supervised.

However, when the device is next reset to its factory conditions, it can be reactivated without any restrictions, and none of the setup screens specified in the profile are skipped.

If the device has not yet been activated for the first time, none of the settings in the unassigned profile will apply to the device activation.

Reload Device Enrollment Data

This command reloads the enrollment information for the selected devices from Apple's enrollment servers.

This should not normally be necessary but may be helpful if you suspect that the enrollment information that is cached locally on the LANrev server has failed to keep in sync with Apple's data.

Configure Devices for Current Classroom Setup

The **Configure Devices for Current Classroom Setup** command applies the current configuration specified in the Classroom Management window to the selected devices.

It is the same command as **Configure Devices for Current Classroom Setup** in the **Classroom Management** window.

Manage Personal Device Assignment

The **Manage Personal Device Assignment** command opens a dialog in which you can assign a classroom device to a user as a personal device, or – if the device is already assigned – unassign it.

It is the same command as **Manage Personal Device Assignment** in the **Classroom Management** window.

Delete Profile

Choosing this command removes the selected configuration or provisioning profiles from the mobile devices on which they are installed.

This command can be used only to delete installed profiles, such as when the list of configuration profiles on a particular device or the list of all installed provisioning profiles are displayed.

Applying this command to a Windows Phone device removes its current EAS policy. This means that the default EAS policy specified on the Exchange server is applied to the device.

This command cannot be used to remove profiles from iOS 4 devices.

Show Detail View

This command is the **Show Detail View** command standard to all browser windows. These commands are also similar:

- **Show Mobile Application Package Details**

- **Show Configuration Profile Details**
- **Show Provisioning Profile Details**
- **Show Media File Details**
- **Show Action Details**

These commands have the same effect as the **Details** command described on page 396.

Create Home Screen Layout Configuration Profile

This command is very similar to the **New Configuration Profile** command when the **iOS home screen layout configuration profile** option is chosen in that command’s dialog.

The difference between these two ways to create a configuration profile for home screen layouts is that choosing **Create Home Screen Layout Configuration Profile** prepopulates the editor with the apps installed on the selected devices (in addition to the system apps).

For further information, see “New Configuration Profile” on page 561.

Synchronize Records

This command is the **Synchronize Records** command standard to all browser windows.

It has the same effect as the **Synchronize Selected Records** command described on page 481.

Enter Custom Field Data

The **Enter Custom Field Data** command lets you edit the content of manual custom information fields for multiple mobile devices in one step.

The command is similar to the **Enter Custom Field Data** command of browser windows, described on page 526.

Import Custom Field Data

The **Import Custom Field Data** command lets you import data from text files into manual (that is, non-dynamic) custom information fields that have been defined for mobile devices.

The command is the same as the **Custom Field Data for Mobile Devices** command, described on page 383.

Ignore Devices

Choosing this command removes the selected iOS devices from the **Mobile Devices** window. Ignored devices and the applications, on them are not listed in any of the groups in the window.

This command applies only to iOS devices found because they are connected to administered computers. It does not apply to mobile devices managed through an MDM server.

Devices will be redisplayed the next time that their agents send inventory information to the server.

Reset All Ignored Devices

Choosing this command ‘unignores’ all devices that have previously been removed from the **Mobile Devices** window using the **Ignore Devices** command described above.

Re-execute All Actions for This Device

Choosing this command treats the selected device as if it was just entering all the smart policies to which it belongs. All actions specified in these policies for new devices are re-executed for this device. Any delays and repetitions specified for the actions still apply.

Choosing the command opens an alert in which you can choose between re-executing the actions when the device next checks in and immediately re-executing them. Immediate execution sends a push notification to the device to check in with the MDM server.

Re-execute This Action for This Device

Choosing this command re-executes the selected action on the displayed device. Any delays and repetitions specified for the actions still apply.

Choosing the command opens an alert in which you can choose between re-executing the action when the device next checks in and immediately re-executing it. Immediate execution sends a push notification to the device to check in with the MDM server.

Retry All Failed Profiles

Choosing this command tries to install configuration and provisioning profiles on the selected device that failed during an earlier installation attempt. It tries to reinstall all profiles that are assigned to any policy to which the device belongs and that are not yet present on the device.

This command is intended to make it easier to install profiles that could not be installed in an earlier attempt, for example, because they were incompatible with a device. In that case, you can fix all profiles that generated error messages and then choose **Retry All Failed Profiles** from the context menu for the device.

Retry All Failed Applications

Choosing this command tries to install applications on the selected device that failed during an earlier installation attempt. It tries to reinstall all applications that are assigned to any policy to which the device belongs and that are not yet present on the device.

Retry All Failed Books

Choosing this command tries to install books on the selected device that failed during an earlier installation attempt. It tries to reinstall all books that are assigned to any policy to which the device belongs and that are not yet present on the device.

Remove from Group

This command is the **Remove from Group** command standard to all browser windows. It is not available when a smart group is being displayed.

For details, see “Remove from Group” on page 528.

Remove from Policy

This command is similar to the **Remove from Group** command standard to all browser windows. Choosing it removes the selected devices from the policy. It is not available when a smart policy is being displayed.

Track Device

This is the same command as **Track Device** on page 477.

Get Device Geolocation

This is the same command as **Get Device Geolocation** on page 479.

Reset Tracking Passphrase

This is the same command as **Reset Tracking Passphrase** on page 479.

Show Location on Google Maps

This command displays the location of a tracked mobile device in Google Maps.

Choosing the command opens a new window in your default web browser and displays the selected location in Google Maps. If a device (instead of a recorded location of a device) is selected before choosing the command, the last known location is displayed.

This command does not support Windows Phone devices.

Show Location on Bing Maps

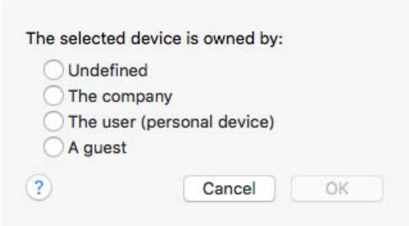
This command displays the location of a tracked mobile device in Bing Maps.

Choosing the command opens a new window in your default web browser and displays the selected locations in Bing Maps. If a device (instead of a recorded location of a device) is selected before choosing the command, the last known location is displayed.

This command does not support Windows Phone devices.

Set Device Ownership

Choosing this command opens the **Set Device Ownership** dialog. Using it, administrators with the “Modify Enrollment Users” privilege can specify to which ownership class the device belongs:


The selected device is owned by:

○ Undefined
○ The company
○ The user (personal device)
○ A guest

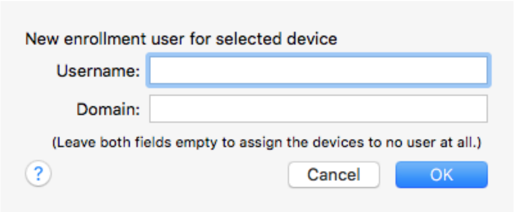
The options in the dialog have the following meanings:

- **Undefined**: No statement is made about the ownership of the device.
- **The company**: The device belongs to your organization.
- **The user (personal device)**: The device is the personal device of its user.

- **A guest**: The device belongs to a visitor to your network, that is, a person that is permitted to have access to your network but is not an employee.

Set Enrollment User

Choosing this command opens the **Set Device Enrollment User** dialog. Using it, administrators with the "Modify Enrollment Users" privilege can specify the directory account of the device's user:



New enrollment user for selected device

Username:

Domain:

(Leave both fields empty to assign the devices to no user at all.)

The dialog contains these elements:

- **Username**: The username of the Active Directory or Open Directory account you want to specify.
- **Domain**: The domain to which the account belongs. This information is not required for Open Directory accounts.

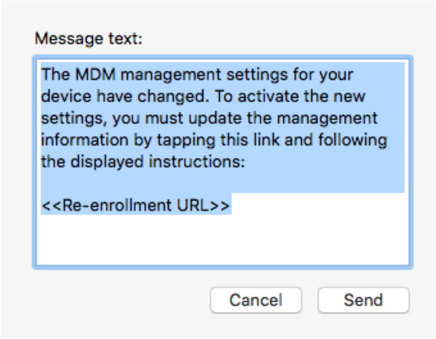
If the username is left empty, the device is marked as belonging to no user, but remains under MDM management.

Update AD User Information

Choosing this command makes LANrev retrieve the information for the users of the selected devices from the Active Directory server. The command applies only to devices with an Active Directory user.

Send Re-enrollment Message to Device

Choosing this command opens the **Message** dialog. Using it, you can prompt users of managed mobile devices to re-enroll their devices, which is necessary when you have changed the MDM privileges in the **MDM** tab of the server settings:



Message text:

The MDM management settings for your device have changed. To activate the new settings, you must update the management information by tapping this link and following the displayed instructions:

<<Re-enrollment URL>>

The dialog contains this element:

- **Message text**: The text in this field will be sent to the users of the managed devices. The URL placeholder will be replaced by an individualized enrollment URL in the actual message. (Do not remove the placeholder or enrollment will not be possible.) In this text, you can use the variables described in “Variables for mobile devices” on page 458.

This command applies only to iOS devices.

Update Installed Application Statistics

Choosing this command updates the summary information displayed in the Installed Software Statistics smart group (see “Sidebar” on page 546) to reflect the current information available on the inventory server.

This command is available only when the **Installed Software Statistics** smart group is displayed.

Show User Details

This command displays the details on the selected mobile device user in the main part of the window. Choosing it is the same as clicking on the user in the sidebar of the **Mobile Devices** window.

Show Mobile Application Package Details

This command displays the details on the selected mobile application package in the main part of the window. Choosing it is the same as clicking on the package in the sidebar of the **Mobile Devices** window.

New Mobile Application Package

This command is the same command as **New Enterprise Application Package**, described on page 553.

New iOS App Store Application Package

This command is the same command as **New iOS App Store Application Package**, described on page 554.

New Google Play Application Package

This command is the same command as **New Google Play Application Package**, described on page 558.

Edit Mobile Application Package

This command lets you edit the selected application package in the **Mobile Application** dialog.

See “New Enterprise Application Package” on page 553 for details.

Duplicate Mobile Application Package

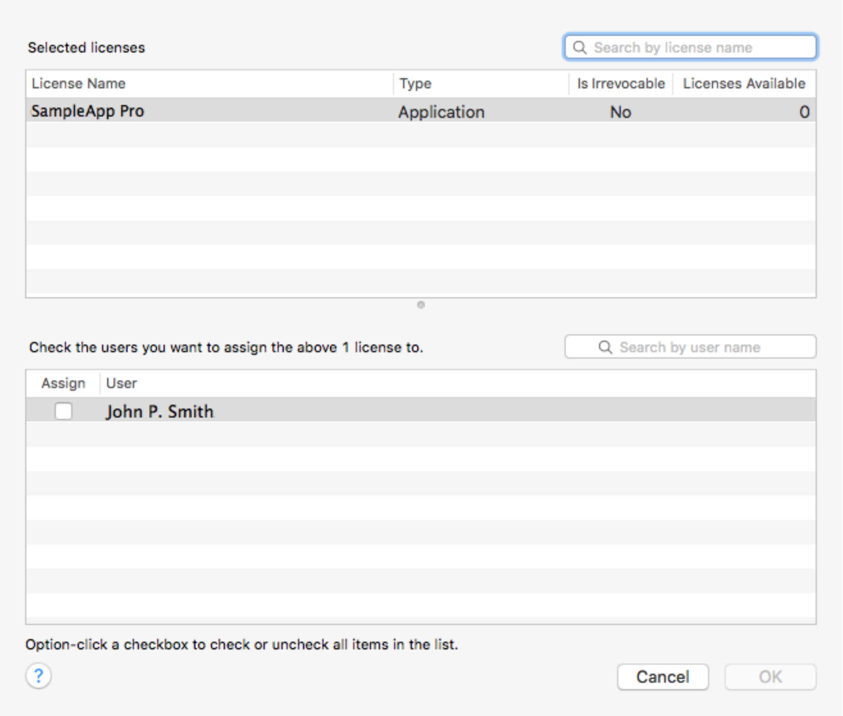
This is the same command as **Duplicate Application Package**, described on page 559.

Remove Mobile Application Package

This command removes the selected application packages from LANrev. Choosing the command when a policy is displayed removes the application only from the policy.

Assign Application Licenses to Users

This command opens the **Assign Application Licenses to Users** dialog, in which you can assign a VPP license for the selected app or book to one or more users.


Selected licenses

License Name	Type	Is Irrevocable	Licenses Available
SampleApp Pro	Application	No	0

Check the users you want to assign the above 1 license to.

Assign	User
□	John P. Smith

Option-click a checkbox to check or uncheck all items in the list.

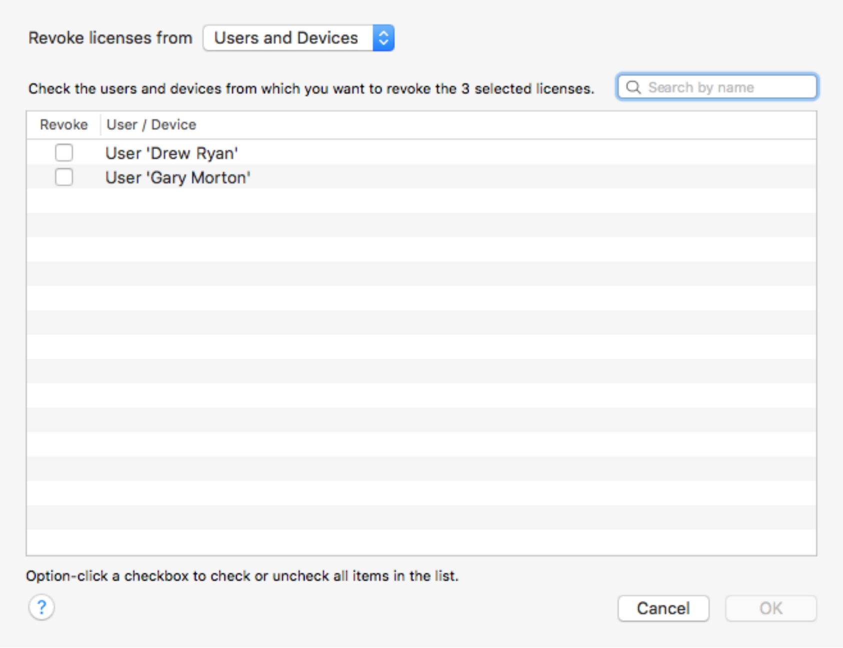
The dialog lists the selected licenses in the upper half and the users in the lower half.

Option-clicking a user in the lower list selects or deselects all users.

Clicking **OK** assigns the listed licenses to all users marked with a checkmark in the **Assign** column.

Revoke Application Licenses

This command opens the **Revoke Application Licenses** dialog, in which you can revoke the VPP license for the selected app from one or more of the users or devices to which it has been assigned.



Revoke licenses from: Users and Devices

Check the users and devices from which you want to revoke the 3 selected licenses.

Revoke	User / Device
□	User 'Drew Ryan'
□	User 'Gary Morton'

Option-click a checkbox to check or uncheck all items in the list.

The list in the dialog includes all users to whom a license for this app is currently assigned.

Option-clicking a user selects or deselects all users.

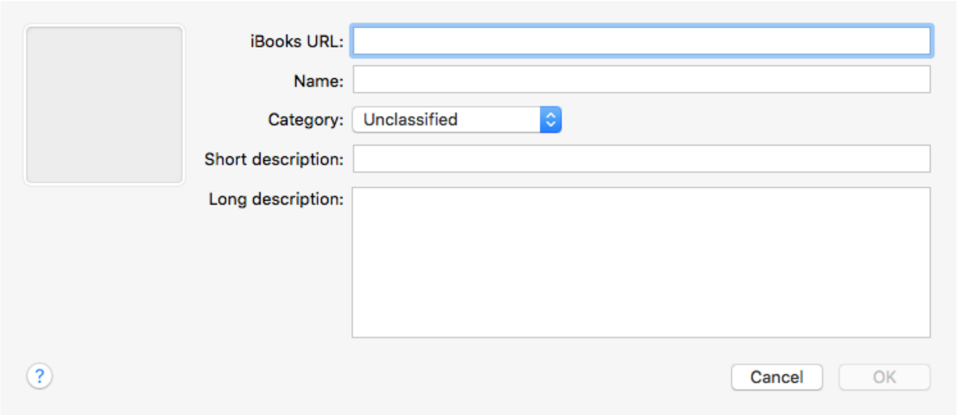
Clicking **OK** revokes the license from all users or their devices (depending on the setting at the top of the dialog) with a checkmark in the **Revoke** column. They remain on the user's device but can only be used for the grace period specified by Apple. After that grace period, the apps no longer function.

Show Book Details

This command displays the details on the selected book in the main part of the window. Choosing it is the same as clicking on the book in the sidebar of the **Mobile Devices** window.

New iBooks Book

This command opens the **iBooks Book** dialog in which you can enter the information for a book from the iBooks Store that you want to make available to users of managed mobile devices:



The dialog contains these elements:

- Cover field: You can paste a graphic in this field that is displayed as the books cover.
- **iBooks URL**: The URL of the book in the iBooks Store. If you enter the URL in this field and leave the field, in the other fields are automatically filled in with data from the store.
- **Name**: The title of the book.
- **Category**: The genre of the book.
- **Short description**: A brief description of the book’s content.
- **Long description**: A longer description of the book’s content.

Clicking **OK** creates an entry for the book in LANrev.

Edit Book

This command opens the LANrev entry for the book in the **iBooks Book** dialog (see above).

Duplicate Book

This command duplicates the LANrev entry for the book and opens the duplicate in the **iBooks Book** dialog (see above).

Remove Book

This command deletes the entry for the selected books from LANrev. This has no effect of copies of the book that are installed on managed mobile devices.

Show Configuration Profile Details

This command displays the details on the selected configuration profile in the main part of the window. Choosing it is the same as clicking on the profile in the sidebar of the **Mobile Devices** window.

New Configuration Profile

This is the same command as **New Configuration Profile**, described on page 561.

Edit Configuration Profile

This command lets you edit the selected application package in the **iOS Configuration Profile** dialog.

See “New Configuration Profile” on page 561 for details.

Remove Configuration Profile

This command removes the selected configuration profile from LANrev.

Remove Configuration Profile from Policy

This command removes the selected configuration profile from the currently displayed policy.

Show Device Enrollment Profile Details

This command displays the details on the selected device enrollment profile in the main part of the window. Choosing it is the same as clicking on the profile in the sidebar of the **Mobile Devices** window.

New Device Enrollment Profile

This command lets you create a new device enrollment profile. Choosing the command opens the **Device Enrollment Profile Editor** dialog, described in “New Enrollment Profile” on page 597.

Edit Device Enrollment Profile

This command lets you change the settings in a device enrollment profile, provided that the profile has not yet been assigned to a device.

If you choose the command for a profile that has not yet been assigned, the profile is opened in the **Device Enrollment Profile Editor** dialog where you can edit it. See “New Enrollment Profile” on page 597 for details.

If you choose the command for a profile that has already been assigned to a device, an error message is displayed. The structure of Apple‘s enrollment servers does not support changing assigned profiles. Therefore, to change enrollment settings for a device, you need to create a new enrollment profile (for example, with the **Duplicate Device Enrollment Profile** command) with the desired settings and assign that profile to the device.

Duplicate Device Enrollment Profile

This command duplicates the selected device enrollment profile and opens the duplicate in the **Device Enrollment Profile Editor** dialog where you can edit it.

See “New Device Enrollment Profile” on page 640 for details.

Remove Device Enrollment Profile

This command removes the selected device enrollment profile from LANrev.

This also removes the profile from all devices to which it has been assigned. Doing so does not immediately change the settings from the **Security and restrictions** section of the profile, which are described in “New Device Enrollment Profile” on page 640. (That is, a device that has been put into supervised mode is still supervised when the enrollment profile is removed.) However, performing a factory reset of the device removes all of these settings.

Show Provisioning Profile Details

This command displays the details on the selected provisioning profile in the main part of the window. Choosing it is the same as clicking on the profile in the sidebar of the **Mobile Devices** window.

Show Media File Details

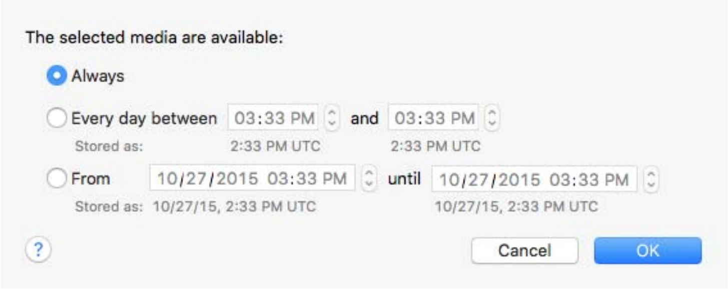
This command displays the details on the selected media file in the main part of the window. Choosing it is the same as clicking on the media file in the sidebar of the **Mobile Devices** window.

Set Availability Time

This command lets you restrict the availability of a media file or configuration profile within a policy. (It is not available when you display the media files or profiles in a subgroup of **Assignable Items**.)

The availability time set in this dialog is always specific to the policy to which the media file or profile is assigned. It does not affect the same media file or profile in other policies; and if the media file or profile is moved to a different policy, the availability time is reset.

Choosing **Set Availability Time** opens the **Set Availability Time** dialog:



The selected media are available:

● Always

○ Every day between 03:33 PM and 03:33 PM
Stored as: 2:33 PM UTC 2:33 PM UTC

○ From 10/27/2015 03:33 PM until 10/27/2015 03:33 PM
Stored as: 10/27/15, 2:33 PM UTC 10/27/15, 2:33 PM UTC

The dialog contains these elements:

- **Always**: If this option is chosen, the media file is available to the members of this policy at any time.
- **Every day between**: If this option is chosen, the media file is available to the members of this policy only during a certain time of the day (for example, during office hours). The specified times refer to the local time of the LANrev server. Note that you can set the start time to be later than the end time. In that case, the availability is from the beginning of the day to the end time and from the start time to the end of the day. (Think of this as a wrap-around interval crossing midnight.) For example, a start time of 9:00 and an end time of 8:00 would result in the profile being available from midnight to 8:00 and from 9:00 to midnight.
- **From**: If this option is chosen, the media file is available to the members of this policy only for the specified interval, not before or after.

NOTE Times are entered by you as local times and stored as UTC (Coordinated Universal Time, similar to GMT or Greenwich Mean Time). This means that you have to take into account any time differences between the server and mobile clients. You also have to manually compensate for daylight saving time (DST), if desired, because DST does not apply to UTC.

New Media File

This is the same command as **New Media File**, described on page 566.

Edit Media File

This command lets you edit the selected media file in the **Mobile Media File** dialog.

See “New Media File” on page 566 for details.

Remove Media File

This command removes the selected media file from LANrev.

Show Action Details

This command displays the details on the selected action in the main part of the window. Choosing it is the same as clicking on the action in the **Actions** group in the sidebar of the **Mobile Devices** window.

Duplicate Action

This command opens the selected action in the appropriate **New ... Action** dialog with a new name. You can edit the settings as desired and save the duplicate.

The various action editing dialogs are described in “Actions” on page 570.

Edit Action

This command lets you edit the selected action in the appropriate **New ... Action** dialog.

The various action editing dialogs are described in “Actions” on page 570.

Remove Action

This command removes the selected action from LANrev. This also removes it from any policy to which it has been assigned.

If you want to remove an action only from the policy the actions of which you are displaying, use the **Remove Action from Policy** command, described on page 648.

Re-execute This Action for All Devices

Choosing this command treats the selected action as if it has just been assigned to all the smart policies to which it is assigned. It is re-executed on all devices belonging to these policies. Any delays and repetitions specified for the action still apply.

Choosing the command opens an alert in which you can choose between re-executing the action when the devices next check in and immediately re-executing it. Immediate execution sends push notifications to the devices to check in with the MDM server.

Re-execute This Action for This Policy

Choosing this command treats the selected action as if it has just been assigned to the displayed policy. It is re-executed on all devices belonging to the policy. Any delays and repetitions specified for the action still apply.

Choosing the command opens an alert in which you can choose between re-executing the action when the devices next check in and immediately re-executing it. Immediate execution sends push notifications to the devices to check in with the MDM server.

New Send Message Action

This is the same command as **New Send Message Action**, described on page 571.

New Send E-Mail Action

This is the same command as **New Send E-Mail Action**, described on page 572.

New Send SMS (Text Message) Action

This is the same command as **New Send SMS (Text Message) Action**, described on page 573.

New Set Roaming Options Action

This is the same command as **New Set Roaming Options Action**, described on page 574.

New Set Activation Lock Options Action

This is the same command as **New Set Activation Lock Options Action**, described on page 575.

New Enable Activation Lock Action

This is the same command as **New Enable Activation Lock Action**, described on page 576.

New Set Wallpaper Action

This is the same command as **New Set Wallpaper Action**, described on page 577.

New Set Device Name Action

This is the same command as **New Set Device Name Action**, described on page 578.

New Set Custom Field Value Action

This is the same command as **New Set Custom Field Value Action**, described on page 581.

New Install iOS Update Action

This is the same command as **New Install iOS Update Action**, described on page 579.

New Validate Applications Action

This is the same command as **New Validate Applications Action**, described on page 580.

New Update Device Information Action

This is the same command as **New Update Device Information Action**, described on page 582.

New Set Attention Mode Action

This is the same command as **New Set Attention Mode Action**, described on page 583.

New Set Lost Mode Action

This is the same command as **New Set Lost Mode Action**, described on page 584.

New Set Passcode Lock Grace Period Action

This is the same command as **New Set Passcode Lock Grace Period Action**, described on page 585.

New Configure Diagnostic Data Transmission Action

This is the same command as **New Configure Diagnostic Data Transmission Action**, described on page 586.

New Freeze Device Action

This is the same command as **New Freeze Device Action**, described on page 587.

New Clear Passcode Action

This is the same command as **New Clear Passcode Action**, described on page 588.

New Register User in VPP Action

This is the same command as **New Register User in VPP Action**, described on page 588.

New Send VPP Invitation Action

This is the same command as **New Send VPP Invitation Action**, described on page 590.

New Retire User from VPP Action

This is the same command as **New Retire User from VPP Action**, described on page 592.

New Remove Configuration Profile Action

This is the same command as **New Remove Configuration Profile Action**, described on page 593.

New Demote to Unmanaged Device Action

This is the same command as **New Demote to Unmanaged Device Action**, described on page 593.

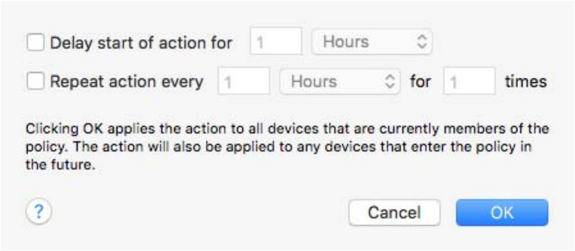
New Configure Devices for Current Classroom Setup Action

This is the same command as **New Configure Devices for Current Classroom Setup Action**, described on page 594.

Change Action Schedule

This command lets you change the delay and repetition settings for a particular action in a policy.

Choosing **Change Action Schedule** opens the **Action Assignment Options** dialog:



☐ Delay start of action for 1 Hours

☐ Repeat action every 1 Hours for 1 times

Clicking OK applies the action to all devices that are currently members of the policy. The action will also be applied to any devices that enter the policy in the future.

The dialog contains these elements:

- **Delay start of action for**: If this option is chosen, the action will not be performed immediately when a device enters the policy but the specified interval later.
- **Repeat action every**: If this option is chosen, the action is performed repeatedly on the device in the specified interval for the specified number of times. The initial execution is counted as the first repetition, so if you specify that the action is to be

repeated two times, the initial action will be executed plus one more execution.

Remove Action from Policy

This command removes the selected action from the policy the actions of which you are displaying.

Show Policy Members

This command displays the devices that belong to a policy in the main part of the window. Choosing it is the same as clicking on the policy in the sidebar of the **Mobile Devices** window.

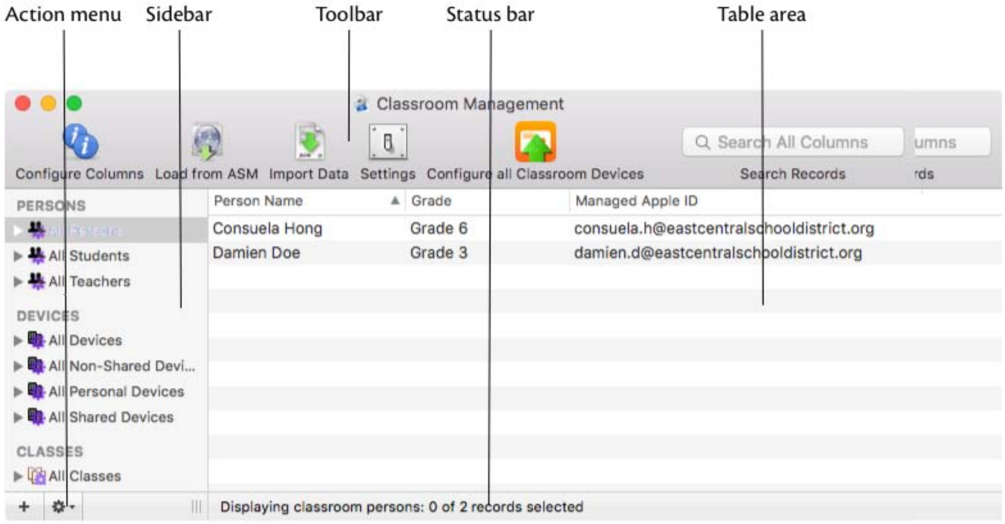
Remove Policy

This command removes the selected policy from LANrev.

Chapter 21 Classroom Management

The **Classroom Management** window lets you manage classes, students, teachers, and devices for use in education environments.

The window is opened by choosing **Window** > **Classroom Management**.



Person Name	Grade	Managed Apple ID
Consuela Hong	Grade 6	consuela.h@eastcentralschooldistrict.org
Damien Doe	Grade 3	damien.d@eastcentralschooldistrict.org

Displaying classroom persons: 0 of 2 records selected

The elements of a **Classroom Management** window are described below:

- **Toolbar** (page 650)
- **Status bar** (page 653)
- **Table columns** (page 654)
- **Drawer** (page 654)
- **Sidebar** (page 655)
- **Action menu** (page 657)
  - **Persons** (page 657)
    - **New Smart Group: Persons** (page 658)
    - **New Smart Group: Teachers** (page 658)
    - **New Smart Group: Students** (page 658)
    - **New Group: Persons** (page 658)
    - **New Person** (page 659)
  - **Classes** (page 660)
    - **New Smart Group: Classes** (page 660)
    - **New Group: Classes** (page 660)
    - **New Class** (page 661)
  - **Devices** (page 661)
    - **New Smart Group: Classes** (page 660)
    - **New Smart Group: Personal Devices** (page 661)
    - **New Smart Group: Shared Devices** (page 662)
    - **New Group: Devices** (page 662)
  - **Rename Group** (page 662)
  - **Edit …** (page 662)
  - **Remove …** (page 662)
  - **Remove … from Group** (page 663)

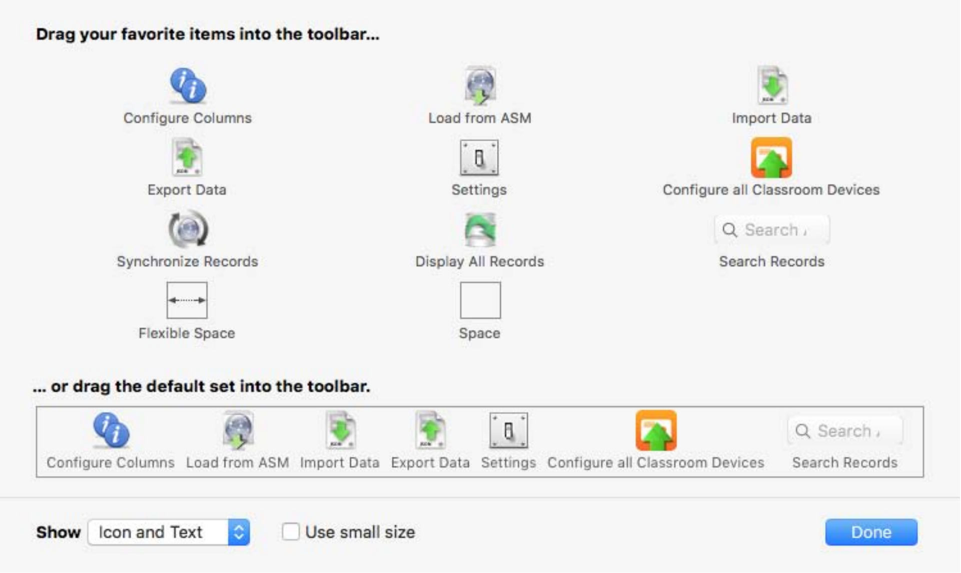
- **Context menu** (page 663)
  - **Classroom Management** (page 663)
    - **Configure Devices for Current Classroom Setup** (page 663)
    - **Configure All Devices Used in Selected Classes** (page 664)
    - **Manage Personal Device Assignment** (page 664)

The **+** button in the lower left-hand corner is not separately described. Clicking it creates a new person smart group as if you had chosen **New Smart Group: Persons**; clicking it with the Option key held down acts like you had chosen **New Group: Persons**.

Only administrators with the Classroom Management privilege can make changes in this window.

Toolbar

The **Classroom Management** window has a toolbar that allows quick access to common actions. It can contain these elements:



The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** and **Space**).

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Load from ASM

The **Load from ASM** button reloads data for all records related to classroom management (persons, classes, and devices) from the Apple School Manager server.

Clicking this button has the same effect as choosing **Server** > **Reload Apple School Management Data**.

Import Data

The **Import Data** button lets you import classroom-related records from a JSON file.

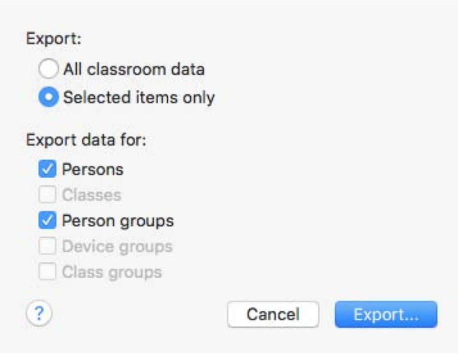
Clicking this button has the same effect as choosing **Server** > **Import Classroom Data**.

The file format of the import file is described in “Classroom data import file format” on page 486.

Export Data

The **Export Data** button lets you export classroom-related records as a JSON file. The file format of the export file is the same as the import file format, which is described in “Classroom data import file format” on page 486.

Clicking the button displays the **Export Classroom Data** dialog, in which you can specify the range and the kind of data to export:



Export:

○ All classroom data
● Selected items only

Export data for:

☑ Persons
□ Classes
☑ Person groups
□ Device groups
□ Class groups

The dialog contains these elements:

- **All classroom data**: If this option is chosen, LANrev exports all data from its database in the chosen categories (see below).
- **Selected items only**: If this option is chosen, LANrev exports only data for the selected items.
- **Export data for**: LANrev exports data for all categories that are checked in this section. Available categories include:
  - **Persons**: Person records.
  - **Classes**: Class records.

  - **Person groups**: Definitions of person groups from the **Classroom Management** window.
  - **Device groups**: Definitions of device groups from the **Classroom Management** window.
  - **Class groups**: Definitions of class groups window.
- **Export**: Clicking this button displays a standard Save dialog.

Settings

The **Settings** button lets you specify details about the importing process of classroom data.

Clicking this button opens the **Classroom Settings** dialog, which is described in "Classroom Settings" on page 652.

Configure All Classroom Devices

Clicking the **Configure All Classroom Devices** button applies the current configuration specified in the Classroom Management window to all devices displayed in the window.

Synchronize Records

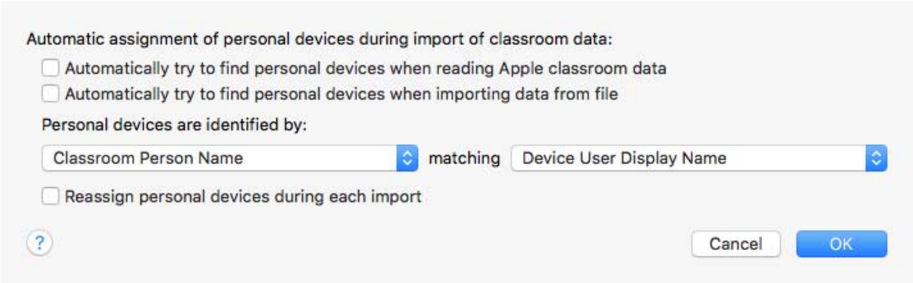
The **Synchronize Records** button downloads updated information for the selected records from the Apple School Manager server.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

Classroom Settings

The **Classroom Settings** dialog lets you specify processing steps for LANrev to perform when importing classroom data:



Automatic assignment of personal devices during import of classroom data:

□ Automatically try to find personal devices when reading Apple classroom data

□ Automatically try to find personal devices when importing data from file

Personal devices are identified by:

Classroom Person Name matching Device User Display Name

□ Reassign personal devices during each import

The dialog contains these elements:

- **Automatically try to find personal devices when reading Apple classroom data**: If this option is checked, LANrev tries to automatically assign personal devices to persons imported from Apple School Manager based on the assignment of users to devices that are already managed by LANrev.

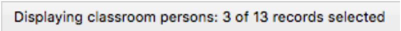
For example, if Madeleine DiFranco is the owner of an iPad that has been enrolled through the device enrollment program and is being managed in LANrev, and a person record for her is imported, that iPad will automatically be assigned to her as her personal device in the classroom.
How imported person records are matched with existing owners is governed by the setting in **Personal devices are identified by** (see below).

- **Automatically try to find personal devices when reading Apple classroom data**: This option is similar to the one above, but applies to importing classroom data from files.
- **Personal devices are identified by**: These two pop-up lists let you specify how to match imported person records with existing device users.
  The first list lets you choose a data field from the import file; the second an information item from the LANrev database. A device user is matched to an imported person record if the data in these two fields match exactly.
  Note that the data in the specified fields should be unique for each user (that is, no two users should have the same value in the field). While devices will still be assigned to users if the values aren’t unique, results will be unpredictable and likely incorrect.
- **Reassign personal devices during each import**: If this option is checked, LANrev assigns personal devices to all users when data is imported. If the option is unchecked, personal devices are assigned only to users who are newly imported. (That is, classroom persons who were unknown to LANrev before the current import.)
  - The manner of assignment is not influenced by this setting: LANrev assigns all devices that are indicated in the imported data as the personal device of a particular user to that user.
  - If one of these devices was previously the personal device of a different user, it is unassigned from that user.
  - If a device that is currently assigned to a particular user is no longer listed as a personal device of that user (but not listed as the device of a different user), it stays assigned to that user.

Status bar

The **Classroom Management** window has a status bar displaying information on the state of the window.

The status bar displays the number of records currently shown in the window. It also shows the kind of information displayed:



Displaying classroom persons: 3 of 13 records selected

If the window does not display all records from the server database table (because the number of records exceeds the initial display limit set in the **Preferences** dialog’s **General** pane), this is indicated with the addition “(more…)” after the record count in the status bar. Clicking **more** displays the additional records.

Table columns

The columns displayed in the **Classroom Management** window are completely configurable.

The columns display information items from the **Classroom Management** category. Information items are described in “Information items” on page 831.

Columns can be dragged around in the window to be rearranged. Dragging an item from the **Information Items** window into a browser window creates a new column at the right of the table.

Deleting columns is possible in the **Columns** drawer, in addition to rearranging and adding columns. This is described below.

Double-clicking a column title in the **Classroom Management** window sorts the table by that column or, if the column is already a sort column, reverses the sort order. If there already are sorting columns, double-clicking a new column makes it a subsorting column. Double-clicking while holding down the Command key unsorts a column.

Which columns are displayed depends on which sidebar entry is selected. The sidebar is described in “Sidebar” on page 655.

Drawer

The **Classroom Management** window contains a drawer for rearranging the columns in the window.

It is opened by choosing **Configure Columns** from the **View** menu.

The drawer contains the titles of all columns that are displayed in the browser window.

The order of the column titles is the same as that of the columns in the table in the window. Dragging a column title to another location in the drawer repositions the column in the window.

Dragging an information item into the drawer adds a corresponding column to the window. You can also drag columns from one window’s drawer to another or transfer them by copying and pasting.

Clicking the **Remove** button deletes the selected columns from the window.

Sidebar

The **Classroom Management** window contains a sidebar with a number of categories and predefined smart groups to which more can be added.

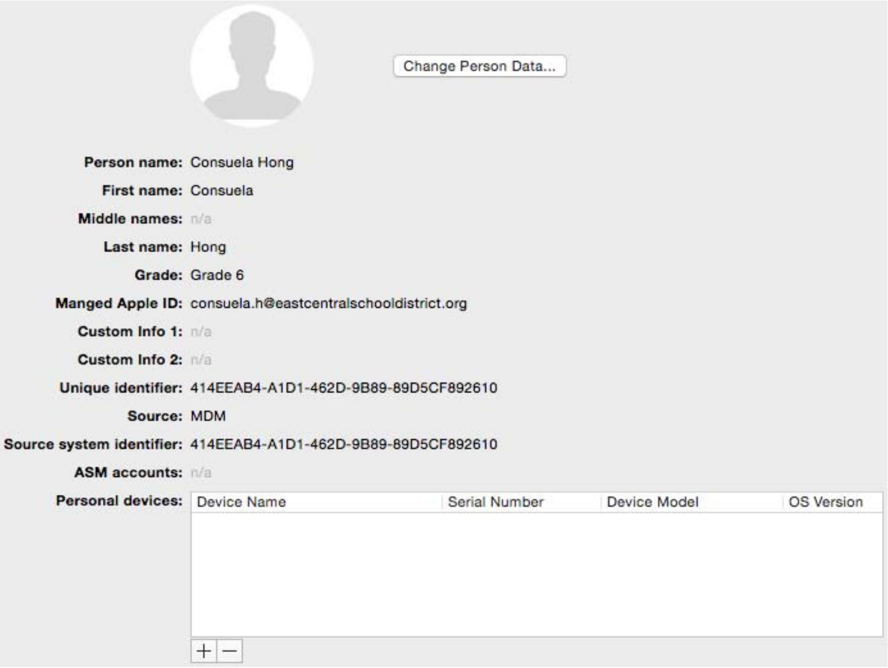
The categories display the various entities that have been defined for classroom management, such as teachers, students, classes, and devices.

Persons

The **Persons** category contains all teachers and students that have been defined in Apple School Manager, divided into subcategories:

- **All Persons**: All teachers and students.
- **All Students**: Just the students.
- **All Teachers**: Just the teachers.

Clicking a category displays its content in the table area; expanding it displays the members in the sidebar. Clicking a member in the sidebar displays detail information about that person in the main part of the window:



Person name: Consuela Hong
First name: Consuela
Middle names: n/a
Last name: Hong
Grade: Grade 6
Manged Apple ID: consuela.h@eastcentralschooldistrict.org
Custom Info 1: n/a
Custom Info 2: n/a
Unique identifier: 414EEAB4-A1D1-462D-9B89-89D5CF892610
Source: MDM
Source system identifier: 414EEAB4-A1D1-462D-9B89-89D5CF892610
ASM accounts: n/a
Personal devices:

Device Name	Serial Number	Device Model	OS Version

This detail view displays important data about the person.

The image can be changed by pasting or dragging a new image into the image area at the top left. Right-clicking the image and choosing **Edit** provides access to the macOS image editing capabilities.

Clicking the **+** button lets you add devices that are assigned to this person in the **Assign Personal Devices**, described in “Assign Personal

Devices" on page 656; clicking the – button removes the association to the selected devices.

Devices

The **Devices** category contains all managed devices that have been defined in Apple School Manager, divided into subcategories:

- **All Devices**: All devices under classroom management.
- **All Non-Shared Devices**: Devices that are under classromm management but have not been assigned to a person nor have been configured as shared devices.
- **All Personal Devices**: Devices that have been assigned to one person.
- **All Shared Devices**: Devices that have been set up as shared devices.

Clicking a category displays its content in the table area; expanding it displays the members in the sidebar. Clicking a member in the sidebar displays detail information about that device in the main part of the window.

Classes

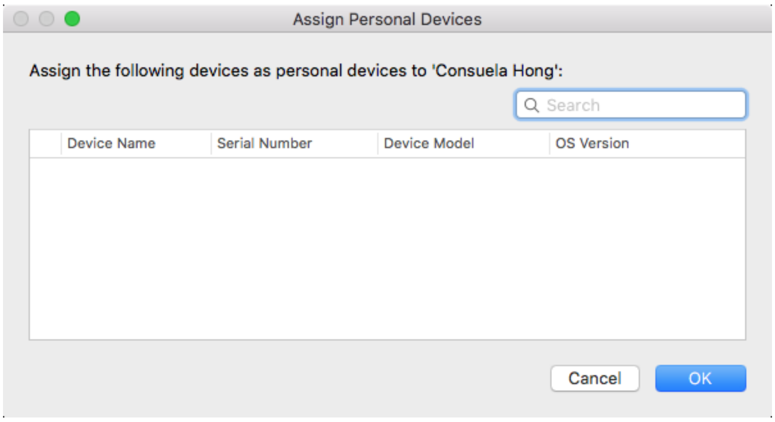
The **Classes** category contains all classes that have been defined in Apple School Manager.

Clicking a category displays its content in the table area; expanding it displays the members in the sidebar.

Clicking a member in the sidebar displays detail information about that class in the main part of the window. Expanding a class displays the teachers, students, and devices that have been assigned to it. Each of these entities can be clicked to display its details in the main part of the window.

Assign Personal Devices

The **Assign Personal Devices** window is opened by clicking the **+** button in the detail view of a person in the **Classroom Management** window. It lists devices that can be assigned to the person in question:



Assign the following devices as personal devices to 'Consuela Hong':

	Device Name	Serial Number	Device Model	OS Version

The window lists all personal devices (as opposed to shared devices) that are managed through the Apple School Manager account.

Typing text in the search field at the top right restricts display to only those devices matching the entered text.

Clicking **OK** assigns all selected devices to the person.

Action menu

The action and the context menus of the sidebar of the **Classroom Management** window contain commands for working with classes, teachers, students, devices, and other classroom-related items.

The commands are described in detail in the following sections.

- **Persons** (page 657)
  - **New Smart Group: Persons** (page 658)
  - **New Smart Group: Teachers** (page 658)
  - **New Smart Group: Students** (page 658)
  - **New Group: Persons** (page 658)
  - **New Person** (page 659)
- **Classes** (page 660)
  - **New Smart Group: Classes** (page 660)
  - **New Group: Classes** (page 660)
- **Devices** (page 661)
  - **New Smart Group: Devices** (page 661)
  - **New Smart Group: Personal Devices** (page 661)
  - **New Smart Group: Shared Devices** (page 662)
  - **New Group: Devices** (page 662)
- **Rename Group** (page 662)
- **Edit …** (page 662)
- **Remove …** (page 662)
- **Remove … from Group** (page 663)

For information on the rest of the commands in the context menu, see “Commands menu” on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Persons

The **Persons** submenu contains commands for working with teacher and student records:

- “New Smart Group: Persons” on page 658
- “New Smart Group: Teachers” on page 658
- “New Smart Group: Students” on page 658
- “New Group: Persons” on page 658
- “New Person” on page 659

New Smart Group: Persons

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for person records defined for classroom management.

For details, see “New Smart Group” on page 522.

New Smart Group: Teachers

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for teacher records defined for classroom management.

For details, see “New Smart Group” on page 522.

New Smart Group: Students

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for student records defined for classroom management.

For details, see “New Smart Group” on page 522.

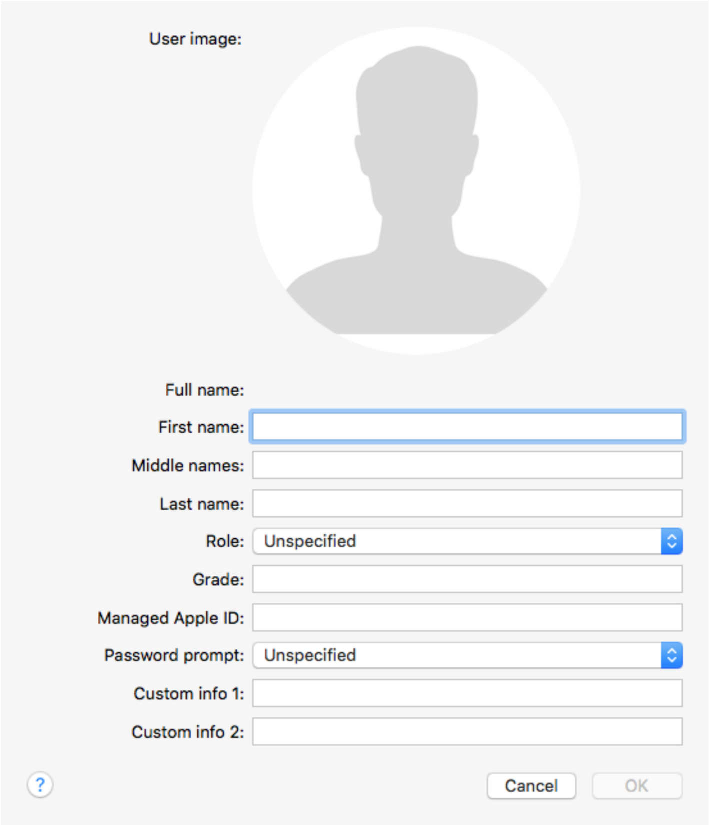
New Group: Persons

This command is the **New Group** command standard to all browser windows. It creates a group for person records defined for classroom management.

For details, see “New Group” on page 522.

New Person

The **New Person** command lets you specify new teachers or students for classroom management. Choosing the command opens the **Person** dialog:



User image:

Full name:

First name:

Middle names:

Last name:

Role: Unspecified

Grade:

Managed Apple ID:

Password prompt: Unspecified

Custom info 1:

Custom info 2:

The dialog contains these elements:

- **User image**: The photo or other representative image of the user.
  You can cut, copy, and paste, and delete images using the **Edit** menu or by right-clicking the image. You can also drag image files from the desktop to this field.
  Choosing **Edit** from the context menu lets you access macOS's image editing tools, including your computer's camera. See Apple's documentation for more information on these tools
- **First name**: The first name of the teacher or student.
- **Middle names**: The middle names or initials of the teacher or student, if any.
- **Last name**: The last name of the teacher or student.
- **Role**: The main role this person plays in the school, such as teacher or student.
  Note that this setting does not prevent the person to take alternate roles in a class. For example, if you specify the student role for a person, that person can still be assigned to a class as a teacher.

- **Grade**: The grade to which the person belongs. This information is optional.
- **Managed Apple ID**: The Apple ID used for this person in the classroom.
- **Password prompt**: The type of password for which the user is prompted on a shared device. (This setting has no effect on devices assigned exclusively to this user.) Available options include four-digit passcodes, six-digit passcodes, and alphanumeric passwords of no fixed length.
  Note that specifying a prompt that does not match the existing password of the user may prevent them from logging in. For example, specifying a six-digit code will present a keypad without letters, which makes it impossible to enter alphanumeric passwords.
- **Custom Info 1**: An arbitrary piece of information associated with the person. Whether and for what purpose this field is used must be decided individually for each LANrev installation.
- **Custom Info 2**: Another arbitrary piece of information associated with the person.

Clicking **OK** creates a record for the person in LANrev.

Classes

The **Classes** submenu contains commands for working with class records:

- "New Smart Group: Classes" on page 660
- "New Group: Classes" on page 660

New Smart Group: Classes

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for class records defined in LANrev.

For details, see "New Smart Group" on page 522.

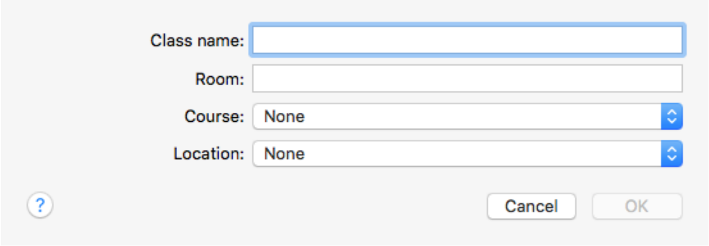
New Group: Classes

This command is the **New Group** command standard to all browser windows. It creates a group for class records defined in LANrev.

For details, see "New Group" on page 522.

New Class

The **New Class** command lets you specify new classes for classroom management. Choosing the command opens the **Class** dialog:


Class name:

Room:

Course: None

Location: None

The dialog contains these elements:

- **Class name**: The name of the class.
- **Room**: The room in which the class is held.
- **Course**: The course to which the class belongs. You can choose an existing cours eor define a new one.
- **Location**: The location of the class. You can choose an existign location or define a new one.

Clicking **OK** creates a record for the person in LANrev.

Devices

The **Devices** submenu contains commands for working with class records:

- "New Smart Group: Devices" on page 661
- "New Smart Group: Personal Devices" on page 661
- "New Smart Group: Shared Devices" on page 662
- "New Group: Devices" on page 662

New Smart Group: Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for device records defined for classroom management.

For details, see "New Smart Group" on page 522.

New Smart Group: Personal Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for personal device records defined for classroom management.

For details, see "New Smart Group" on page 522.

New Smart Group: Shared Devices

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for shared device records defined for classroom management.

For details, see “New Smart Group” on page 522.

New Group: Devices

This command is the **New Group** command standard to all browser windows. It creates a group for device records defined for classroom management.

For details, see “New Group” on page 522.

Rename Group

This command is the standard **Rename Group** command common to all browser windows.

For details, see “Rename Group” on page 523.

Edit ...

The various **Edit ...** commands let you edit groups and other items in the sidebar.

Choosing the command opens a dialog in which you can edit the item. For details about these dialogs, see the dialogs for creating the respective items.

Some items cannot be edited, in which case the command is disabled.

Remove ...

The various **Remove ...** commands let you delete groups and other items listed in the sidebar.

Choosing the command deletes the selected items.

Some items cannot be deleted, in which case the command is disabled.

Remove … from Group

The various **Remove … from Group** commands let you remove members from a group.

For example, choosing Remove Person from Group removes the selected person from the group that you are displaying. The person is not deleted from LANrev or from other groups, only from the current group.

The command applies only to standard (non-smart) groups and is disabled for smart groups.

Context menu

The commands from the context menu of the **Classroom Management** window are the same as described for the Mobile Devices window. For details, see "Table context menu" on page 604.

In addition, it contains these submenus and commands:

- **Classroom Management** (page 663)
    - **Configure Devices for Current Classroom Setup** (page 663)
    - **Configure Devices for Current Classroom Setup** (page 663)
    - **Manage Personal Device Assignment** (page 664)

Classroom Management

The **Classroom Management** submenu contains commands related to managing devices in a classroom setting:

- **Configure Devices for Current Classroom Setup** (page 663)
- **Configure All Devices Used in Selected Classes** (page 664)
- **Manage Personal Device Assignment** (page 664)

Configure Devices for Current Classroom Setup

The **Configure Devices for Current Classroom Setup** command applies the current configuration specified in the **Classroom Management** window to the selected devices.

Choosing the command displays a dialog where you can update just the selected devices or all related devices as well:

- **Update Selected**: This assigns users to the selected devices (if they are shared devices) and assigns them to classes, which in turn gives the teachers in the classes control of the devices.

- **Update Selected and Related**: This performs the same action as **Update Selected**. In addition, all other devices that are affected by the changes are updated as well. For example, if a device is added to a class, the device of that class's teacher is updated as well.

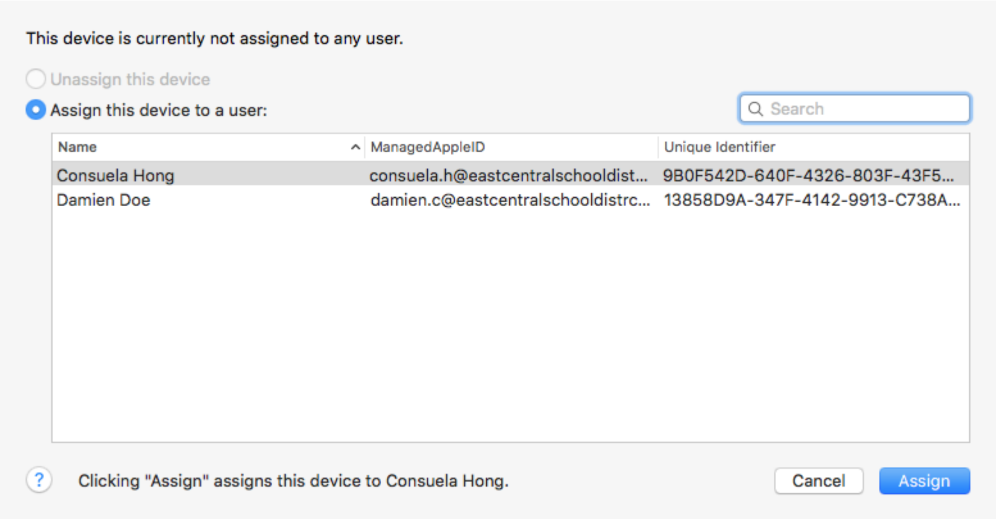
To avoid inconsistent configuration, we recommend that you use the **Update Selected and Related** button unless you have a specific reason to only update the selected devices.

Configure All Devices Used in Selected Classes

The **Configure All Devices Used in Selected Classes** command applies the current configuration specified in the **Classroom Management** window to all devices that are used in the selected classes.

Manage Personal Device Assignment

The **Manage Personal Device Assignment** command opens a dialog in which you can assign a classroom device to a user as a personal device, or – if the device is already assigned – unassign it:


This device is currently not assigned to any user.

○ Unassign this device

● Assign this device to a user:

Name	ManagedAppleID	Unique Identifier
Consuela Hong	consuela.h@eastcentralschooldist...	9B0F542D-640F-4326-803F-43F5...
Damien Doe	damien.c@eastcentralschooldistrc...	13858D9A-347F-4142-9913-C738A...

Clicking "Assign" assigns this device to Consuela Hong.

The dialog contains these elements:

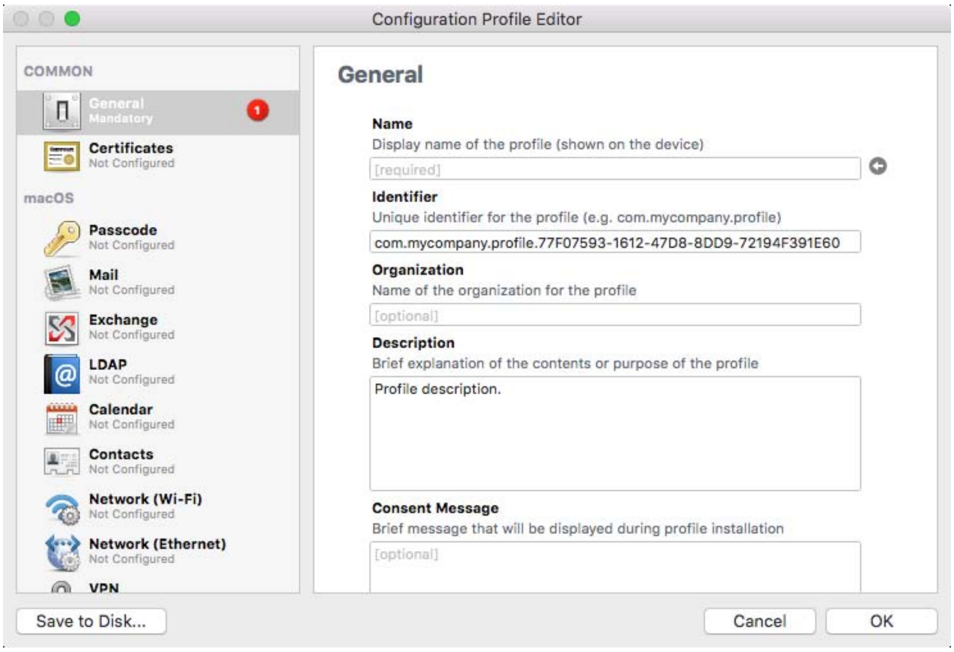
- **Unassign this device**: If this option is chosen, clicking the **Unassign** button turns the device into an unassigned device that is no longer assigned to any person.
  This option is not available when the device is already unassigned.
- **Assign this device to a user**: If this option is chosen, clicking the **Assign** button assigns the device to the person selected in the list.
  The list of person displayed in the list can be filtered by entering text in the search field above the list.

Clicking **Assign** or **Unassign**, respectively, performs the currently selected action.

Chapter 22 Configuration profile editor

The configuration profile editor lets you create new configuration profiles or edit existing ones without requiring external tools.

It is opened using the **New Configuration Profile** command in the **Mobile Device** window. The command presents you with a dialog in which you can choose from several types of profiles or open an existing profile from disk; the chosen profile is then opened in the configuration profile editor (the exact content of the window depends on the type of the profile):



General

Name
Display name of the profile (shown on the device)
[required]

Identifier
Unique identifier for the profile (e.g. com.mycompany.profile)
com.mycompany.profile.77F07593-1612-47D8-8DD9-72194F391E60

Organization
Name of the organization for the profile
[optional]

Description
Brief explanation of the contents or purpose of the profile
Profile description.

Consent Message
Brief message that will be displayed during profile installation
[optional]

Clicking **OK** in the profile editor window saves the new or edited profile to the **Configuration Profiles** section of the **Mobile Devices** window.

The **Save to Disk** button at the bottom of the window lets you export the profile as a text file to disk. This button is enabled only if at least one of these conditions is true:

- Exporting the profile was allowed by checking the Allow **save to disk** option (see “Common settings” on page 667).
- The current administrator has superadministrator privileges.

The other options available in the editor depend on the profile chosen. They are described in:

- “Common settings” on page 667
- “macOS profiles” on page 668
- “iOS profiles” on page 669
- “Android profiles” on page 669
- “Samsung KNOX profiles” on page 672
- “Windows Phone profiles” on page 673

- “LANrev Find profiles” on page 673
- “LANrev Safe SharePoint profiles” on page 674
- “LANrev Safe MDM URL profiles” on page 676
- “Third-Party app profiles” on page 676
- “LANrev Safe App configuration profiles” on page 677
- “LANrev Remote profiles” on page 678

NOTE Administrators can access this editor only if the **Modify Mobile Device Configuration Profiles** option has been activated for their account.

Common settings

The **Common** section of the configuration profile editor lets you specify and edit settings that each configuration profile has, independent of its type.

The section has two subsections:

- **General**
- **Certificates**

The settings from both sections are described below.

General

The **General** section contains mandatory settings for all kinds of configuration profiles:

- **Name**: The name of the profile. This is also the name that the profile will have in the **Mobile Devices** window.
- **Identifier**: A unique identifier for the profile, for example “com.mycompany.it.mdm.my-profile.421”.
- **Organization**: The name of your organization.
- **Description**: A brief text describing the purpose of the profile.
- **Consent Message**: A message that will be displayed on the target device when the user is prompted to allow the installation of the profile.
- **Security**: The options the user of the target device has for removing this profile:
  - **Always**: The user can remove the profile as desired.
  - **With Authorization**: The user can remove the profile when she or he enters a password that you specify in the **Authorization password** field. (The field is hidden unless you choose this option.)
  - **Never**: The profile cannot be removed, although it can be overwritten with a newer version.
- **Automatically Remove Profile**: At which point the profile is automatically removed from the device (that is, without requiring further action by you or the user):
  - **Never**: The profile is not automatically removed.

  - **On Date**: The profile is automatically removed at the specified date. (Choosing this option displays a field for entering the date.)
  - **After Interval**: The profile is automatically removed a set time after it has been installed. (Choosing this option displays a field for specifying the number of days.)
- **Allow save to disk**: If this option is checked, any administrator can save the profile to disk as a file (by clicking the **Save to Disk** button in the profile editor). If this option is unchecked, only superadministrators can export the profile in this manner.

Certificates

The **Certificates** section lets you specify which certificates will be installed with the profile on the target devices.

Clicking the **Configure** button will let you choose an X.509 certificate file from disk to attach to the profile.

Imported certificates have **+** and **-** buttons beside their names. Clicking **+** lets you import an additional certificate; clicking **-** removes the imported certificate from the profile.

Each imported certificate has two editable fields:

- **Credential Name**: The name of the certificate. By default, this is the file name, but you can edit it as desired.
- **Password**: If the certificate is protected by a password, you can enter it. If you do not do so, the user must enter the password during the installation of the profile; if it is not entered correctly, the installation fails. (This does not apply when no password is set for the profile.)

macOS profiles

The macOS section of the configuration profile editor contains settings for macOS computers that can be specified in profiles.

Custom setting

The settings in this section are the same as those in Apple’s Profile Manager (part of macOS Server), with one setting added by LANrev in the **Security & Privacy** section, on the **FileVault** tab:

If **Save personal FileVault recovery key on the LANrev server** is checked, the key is securely stored on the LANrev server (instead of with Apple) and can be retrieved from LANrev Admin by using the **Show FileVault Recovery Key** context menu command in a browser window.

Categories

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

iOS profiles

The iOS section of the configuration profile editor contains settings for iOS devices that can be specified in profiles.

Custom setting

The settings in this section are the same as those in Apple's Profile Manager (part of macOS Server), with one setting added by LANrev in the **Disable App Store** section:

If you add this payload to a configuration profile, it disables access to the App Store from any device on which it is installed. Note that the **Disable App Store** is always checked – the payload does not offer any other options.

If you want to re-enable App Store access, do so by removing the profile from the device.

If you create a profile with the **Disable App Store** payload, you must not add any other payloads to the profile.

Categories

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

Android profiles

The **Android** section of the configuration profile editor contains settings for Android devices that can be specified in profiles.

There are general settings that apply to all Android devices and specific settings that apply only to a subset. To find out what profile settings your managed Android devices support, see their documentation.

These categories of Android settings are available:

- "General Android settings" on page 670
- "Motorola Android settings" on page 672
- "Samsung Android settings" on page 672

- “NitroDesk TouchDown settings” on page 672

General Android settings

The **Android General** section of the configuration profile editor contains categories of configuration profile settings that apply to all Android devices:

- **Password**
- **Device Restrictions**
- **Wi-Fi**

The individual settings in the categories are described below.

Password

You can specify restrictions for the passwords that are set on the managed devices:

- **Password quality**: A general quality category required for any new device password.
  Most categories are straightforward; “weak biometric” means that the user may either specify a standard alphanumeric password or restrict access, usage of a low-security biometric access technology (such as facial recognition) is permitted.
  This setting works only on devices running Android 4.0.4 or newer.
- **Minimum password length**: How many characters the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Minimum number of letters**: How many letters (as opposed to digits or symbols) the password must at least contain.
- **Minimum number of uppercase letters**: How many uppercase letters the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Minimum number of lowercase letters**: How many lowercase letters the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Minimum number of non-letters**: How many digits and symbols combined the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Minimum number of digits**: How many digits the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Minimum number of symbols**: How many symbols (characters that are neother letters nor digits) the password must at least contain.
  This setting works only on devices running Android 3.0 or newer.
- **Maximum number of failed attempts**: After how many incorrect password entries the data on the device is erased.

- **Maximum auto-lock**: The time without user input after which the device locks itself.
- **Maximum password age**: How long a password may be used before it must be changed.
  This setting works only on devices running Android 3.0 or newer.
- **Password history**: How many different passwords a user must specify before he or she may reuse a password.
  This setting works only on devices running Android 3.0 or newer.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

Device Restrictions

Restrictions on how some device features may be used:

- **Allow use of camera**: If this option is unchecked, the user cannot use the built-in camera of the device.
  This setting works only on devices running Android 4.0 or newer.
- **Encrypt internal storage**: If this option is checked, data in the internal storage of the device must be encrypted.
  This setting works only on devices running Android 3.0 or newer.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

Wi-Fi

Settings specifying how the device may access Wi-Fi networks:

- **Network name (SSID)**: The name of the wireless network.
- **Hidden network**: If the specified network is hidden (not broadcasting its SSID), this option must be checked.
- **Security type**: The kind of security used by the specified network.
- **Password**: The password required for accessing this network.
  This option is shown when WEP security is chosen.
- **Preshared key**: The key required for accessing this network.
  This option is shown when WPA security is chosen.

Specified networks have **+** and **-** buttons beside their names. Clicking **+** lets you specify an additional network; clicking **-** removes the network specification from the profile.

Web Clips

Settings to create web page bookmarks on the device’s home screen:

- **Label**: The name for the bookmark.
- **URL**: The web address that is opened when the bookmark is clicked.

- **Icon**: The icon representing the bookmark on the home screen. Clicking the Choose button lets you open a graphics file to use as the icon.

Specified web clips have **+** and **-** buttons beside their names. Clicking **+** lets you specify an additional web clip; clicking **-** removes the web clip specification from the profile.

Motorola Android settings

The **Android (Motorola)** section of the configuration profile editor contains categories of configuration profile settings that apply to some Android devices from Motorola.

For details on the individual settings, see Motorola’s documentation on is mobile management extensions.

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

Samsung Android settings

The **Android (Samsung)** section of the configuration profile editor contains categories of configuration profile settings that apply to some Android devices from Samsung. (For Samsung KNOX-specific configuration profiles, see “Samsung KNOX profiles” on page 672.)

For details on the individual settings, see Samsung’s documentation on is mobile management extensions.

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

NitroDesk TouchDown settings

The **NitroDesk TouchDown** section of the configuration profile editor contains categories of configuration profile settings that apply to the TouchDown Exchange client solution from NitroDesk.

For details on the individual settings, see NitroDesk’s documentation on TouchDown.

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

Samsung KNOX profiles

The **Samsung KNOX** section of the configuration profile editor contains categories of configuration profile settings that apply to mobile devices running the Samsung KNOX extension of Android. (For other Samsung-specific configuration profiles, see "Samsung Android settings" on page 672.)

For details on the individual settings, see Samsung's documentation on KNOX configuration options.

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

Windows Phone profiles

The **Windows Phone 7** section of the configuration profile editor contains categories of configuration profile settings that apply to the mobile devices running the Windows Phone 7 operating system.

For details on the individual settings, see Microsoft's documentation on Windows Phone 7 configuration options.

Categories have **+** and **-** buttons or just **-** buttons beside their names. Clicking **+** lets you specify an instance of the category. Clicking **-** removes the category instance from the profile. If this was the last (or only) instance of the category, the profile no longer provides settings for this category.

LANrev Find profiles

The LANrev Find Settings section of the configuration profile editor contains settings for the LANrev Find geolocation display app that can be specified in profiles:

- **MDM server and port**: The DNS or IP address and port of the server from which LANrev Find is to retrieve the location data it displays.
- **Data refresh interval**: The interval before LANrev Find polls the server for new location data.
- **Maximum number of location entries**: How many locations LANrev Find is to download for a displayed device.
- **Log out automatically when idle after**: The interval of inactivity before the local user is automatically logged out of LANrev Find.
- **Log out automatically when closed**: If this option is checked, the local user will need to enter their credentials each time they return to LANrev Find after they have closed it or switched to a different app.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

LANrev Safe SharePoint profiles

The LANrev Safe section of the configuration profile editor contains settings for the LANrev Safe content access app that can be specified in profiles.

The section has two subsections:

- **LANrev Safe SharePoint**
- **LANrev Safe Settings**

The settings from both sections are described below.

Note that there are three different LANrev Safe profiles:

- Use the LANrev Safe SharePoint profile when you want to distribute media via a SharePoint server.
- Use the LANrev Safe MDM URL profile to specify the MDM server to use for LANrev Safe running on iOS 6. Do not use it for LANrev Safe 1.x for Android. See “LANrev Safe MDM URL profiles” on page 676 for details.
- Use the LANrev Safe App Configuration profile to specify the settings for LANrev Safe running on iOS 7 and above, and for LANrev Safe 2.0 and above running on Android. See “LANrev Safe App configuration profiles” on page 677 for details.

It is possible to assign multiple profiles related to LANrev Safe to the same device. If you do and they contain conflicting settings, the setting from the last assigned profile is used.

LANrev Safe SharePoint

The **LANrev Safe SharePoint** section contains settings for accessing a SharePoint server from LANrev Safe:

- **SharePoint name**: The name of this SharePoint configuration.
- **SharePoint URL**: The DNS name or IP address of the SharePooint server to use.
- **Domain**: The domain to which the SharePoint user account belongs.
- **User**: The username with which to access the SharePoint server.
- **Password**: The password for the user account.
- **User can change password**: If this option is checked, the user can change the password.
- **User can delete library**: If this option is checked, the user can delete SharePoint libraries from the account list.
- **SharePoint files can leave LANrev Safe**: If this option is unchecked, files that have been loaded from a SharePoint server cannot be taken out of LANrev Safe, whether by copying content, printing, or forwarding to other applications.
- **SharePoint files can be sent via e-mail**: If this option is checked, a button for sending files downloaded from a SharePoint server by e-mail appears in LANrev Safe.

- **SharePoint files can be printed**: If this option is checked, a button for printing files downloaded from a SharePoint server appears in LANrev Safe.
- **Download files only over Wi-Fi**: If this option is checked, LANrev Safe will download files from the SharePoint server only if the mobile device is on a WiFi-connection, not when it is connected over a mobile data connection such as 3G (UMTS) or LTE.

Availability: Choose when SharePoint access through this profile is available:

- **Always**: SharePoint access is available at any time.
- **Every day between**: SharePoint access is available only during a certain time of the day (for example, during office hours). The specified times refer to the local time of the LANrev server. Note that you can set the start time to be later than the end time. In that case, the availability is from the beginning of the day to the end time and from the start time to the end of the day. (Think of this as a wrap-around interval crossing midnight.) For example, a start time of 9:00 and an end time of 8:00 would result in the profile being available from midnight to 8:00 and from 9:00 to midnight.
- **From**: SharePoint access is available only for the specified interval, not before or after.

The individual SharePoint settings have **+** and **-** buttons beside their titles. Clicking **+** lets you specify an additional setting; clicking **-** removes the setting from the profile.

LANrev Safe Settings

The **LANrev Safe Settings** section contains general settings for using LANrev Safe:

- **Required free space**: When downloading a file would leave less than the specified amount of storage free on the mobile device, LANrev Safe will not download the file.
- **SharePoint folder refresh interval**: How often LANrev Apps checks the SharePoint server for new files.
  This setting applies to all SharePoint servers.
- **Add new SharePoint libraries**: If this option is checked, mobile users can add SharePoint libraries to their devices.
  This setting applies to all SharePoint servers.

Clicking **-** (at the upper right) removes all settings in this category from the profile.

LANrev Safe MDM URL profiles

The LANrev Safe section of the configuration profile editor lets you set the MDM server address for the LANrev Safe content access app in profiles:

- **LANrev Safe Application Bundle Identifier**: The identifier of the LANrev Safe application bundle.
  If you are using the App Store version of LANrev Safe, this is com.absolute.AbsoluteSafe. If you are using the enterprise version, this is the bundle identifier that you gave it. However, note that the identifier must end with “.lanrevsafe” in that case.
- **MDM server and port**: The DNS or IP address and port of the server from which LANrev Safe downloads media files.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

Note that there are three different LANrev Safe profiles:

- Use the LANrev Safe SharePoint profile when you want to distribute media via a SharePoint server. See “LANrev Safe SharePoint profiles” on page 674 for details.
- Use the LANrev Safe MDM URL profile described in this section to specify the MDM server to use for LANrev Safe running on iOS 6. Do not use it for LANrev Safe 1.x for Android.
- Use the LANrev Safe App profile to specify the settings for LANrev Safe running on iOS 7 and above, and for LANrev Safe 2.0 and above running on Android. See “LANrev Safe App configuration profiles” on page 677 for details.

It is possible to assign multiple profiles related to LANrev Safe to the same device. If you do and they contain conflicting settings, the setting from the last assigned profile is used.

Third-Party app profiles

The Third-Party App Config section of the configuration profile editor lets specify settings for compatible app store apps running on iOS 7 and above.

Settings are specified as key/value pairs. For information on which settings are available and which effects they have, see the documentation of the app in question.

- **Application Bundle Identifier**: The identifier of the application bundle.
  This identifier is displayed in the App Bundle Identifier information item.
- **Property List Values**: The list of settings. Each setting must be specified as a key, a data type, and a value.

To add a setting, right-click the list and choose **Add Row** from the context menu. To delete a setting, choose **Delete Selection**.

Clicking the **Load from File** button lets you load an existing plist file into the list. Doing so replaces any current content of the settings list. You can edit the imported content, for example, by deleting rows or changing values.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

LANrev Safe App configuration profiles

The LANrev Safe Settings section of the configuration profile editor contains settings for the LANrev Safe content access app that can be specified in profiles:

- **LANrev Safe Application Bundle Identifier**: The identifier of the LANrev Safe application bundle.
  If you are using the App Store version of LANrev Safe, this is com.absolute.AbsoluteSafe. If you are using the enterprise version, this is the bundle identifier that you gave it. However, note that the identifier must end with “.lanrevsafe” in that case.
- **MDM server and port**: The DNS or IP address and port of the server from which LANrev Safe downloads media files.
- **Required free space**: When downloading a file would leave less than the specified amount of storage free on the mobile device, LANrev Safe will not download the file.
- **SharePoint folder refresh interval**: How often LANrev Apps checks the SharePoint server for new files.
  This setting applies to all SharePoint servers.
- **Add new SharePoint libraries**: If this option is checked, mobile users can add SharePoint libraries to their devices.
  This setting applies to all SharePoint servers.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

Note that there are three different LANrev Safe profiles:

- Use the LANrev Safe SharePoint profile when you want to distribute media via a SharePoint server.
- Use the LANrev Safe MDM URL profile to specify the MDM server to use for LANrev Safe running on iOS 6. Do not use it for LANrev Safe 1.x for Android. See “LANrev Safe MDM URL profiles” on page 676 for details.
- Use the LANrev Safe App profile to specify the settings for LANrev Safe running on iOS 7 and above, and for LANrev Safe 2.0 and above running on Android.

It is possible to assign multiple profiles related to LANrev Safe to the same device. If you do and they contain conflicting settings, the setting from the last assigned profile is used.

LANrev Remote profiles

The LANrev Remote section lets you configure how the LANrev Remote host app on Android devices accepts and sets up connections and what capabilities the connection provides.

- **Enable incoming remote control sessions**: If this option is checked, LANrev Remote listens for incoming connection requests.
- **Enable outgoing remote control sessions**: If this option is checked, LANrev Remote reponds to requests from LANrev to initiate a connection to a viewer. This is required, for example, to allow remote connections when the device is behind a NAT router.
- **Authentication**: The type of authentication LANrev Remote requires before establishing a connection.
- **Control password**: The password a remote viewer must provide to establish a controlling session.
  If VNC authentication is specified and this field is left blank, controlling connections do not require a password.
  This field is visible only if VNC is chosen as the authentication method.
- **View-only password**: The password a remote viewer must provide to establish a viewing session without controlling access.
  If VNC authentication is specified and this field is left blank, no controlling connections are possible.
  This field is visible only if VNC is chosen as the authentication method.
- **Port**: The port on which LANrev Remote listens for connection requests.
- **Idle timeout**: When the viewer does not perform any actions for this amount of time, the connection is closed. The value must be at least 1 minute.
- **Allow only connections from LANrev (LANrev Remote)**: If this option is checked, LANrev Remote only accepts connections from LANrev (usually LANrev Admin). Connection requests from standard VNC viewers are rejected.
- **Allow clipboard transfer**: If this option is checked, the contents of the clipboard is transferred between the mobile device and the viewer.
- **User must confirmconnection requests**: If this option is checked, every connection request triggers an alert on the mobile device. The connection is opened only if the mobile user confirms the request.
- **Logging level**: This option lets you specify how detailed the LANrev Remote log on the mobile device should be.

Clicking **-** (in the upper right) removes all settings in this category from the profile.

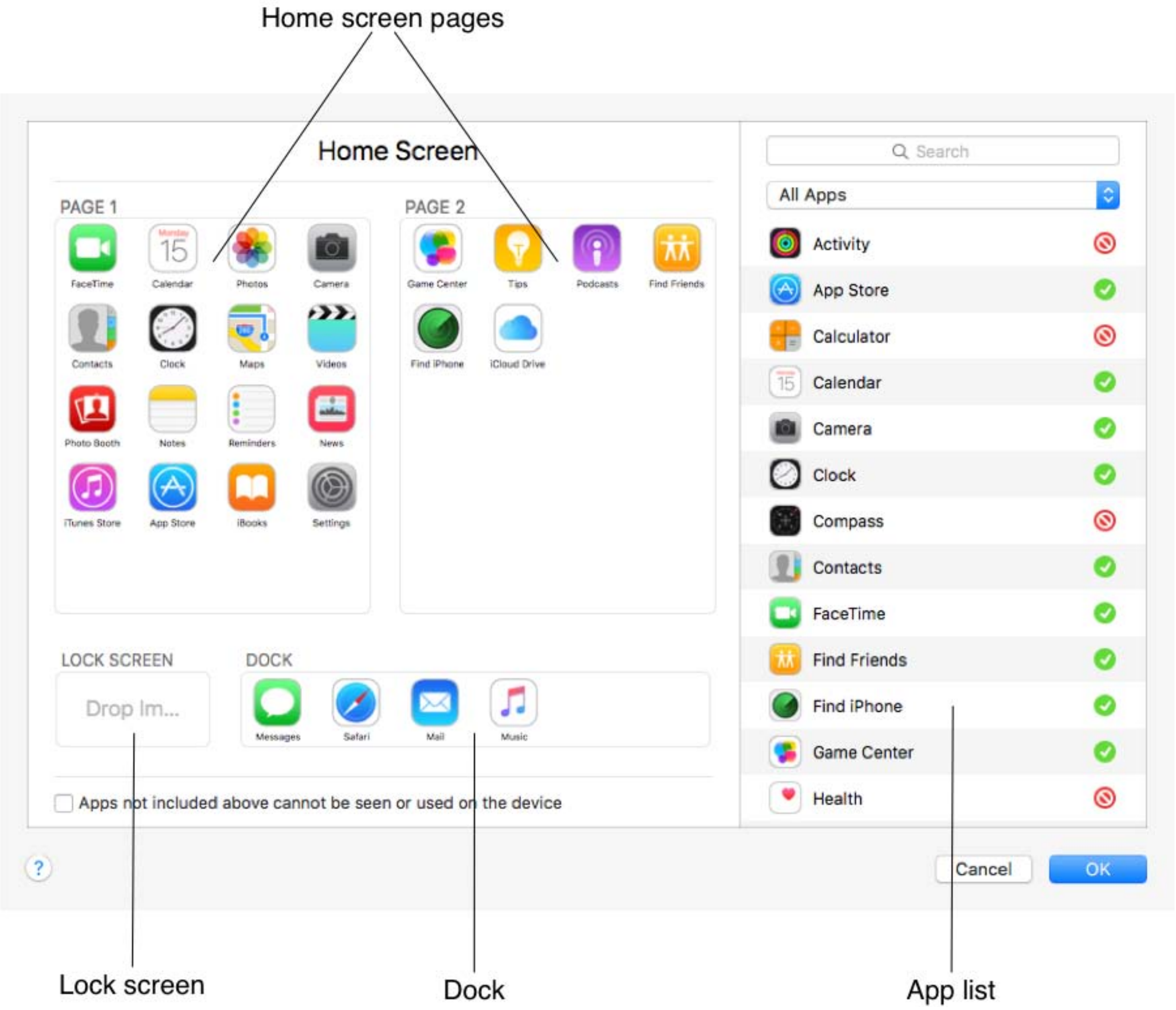
Chapter 23 Home screen layout editor

The home screen layout editor lets you create new configuration profiles for specifying the home screens of iOS devices.

NOTE Administrators can access this editor only if the **Modify Mobile Device Configuration Profiles** option has been activated for their account.

The dialog is opened using the **New Configuration Profile** command in the **Mobile Device** window, choosing the **iOS home screen layout configuration profile** option, and clicking **Continue;** or by double-clicking an existing home screen layout configuration profile.

Either action displays the Home Screen Layout Profile Settings dialog, described on page 562; clicking **Continue** in that dialog opens the home screen layout editor:



□ Apps not included above cannot be seen or used on the device

Activity	⊘
App Store	✓
Calculator	⊘
Calendar	✓
Camera	✓
Clock	✓
Compass	⊘
Contacts	✓
FaceTime	✓
Find Friends	✓
Find iPhone	✓
Game Center	✓
Health	⊘

Clicking **OK** in the profile editor window saves the new or edited profile to the **Configuration Profiles** section of the **Mobile Devices** window.

The configuration profile can be managed as usual. (For details, see "Working with configuration profiles" on page 181.) When the profile is applied to a device:

- Apps placed on a home screen page, in a folder, or in the dock are positioned on the device as specified if they are present.
- Apps that have been hidden the profile are hidden on the device and can no longer be used. If the same app is later installed on the device, it is automatically hidden as well.
- Apps that are present on the device but not specified in the profile are placed in empty spots left in the profile; if necessary, new home screen pages are added.
  If the **Apps not included above cannot be seen or used on the device** option in the layout editor was checked, apps not included in the profile are completely hidden on the device and cannot be launched, even if they are installed again after the home screen layout configuration profile has been installed.
- If a wallpaper image has been specified for the home screen or the lock screen, the wallpaper on the device is set accordingly.

The individual sections of the dialog are described in:

- **Home screen pages** (page 680)
- **App list** (page 681)
- **Lock Screen section** (page 682)
- **Dock section** (page 683)

The **Apps not included above cannot be seen or used on the device** option applies to the created configuration profile. As described above, it makes the profile an app whitelist: Only the apps that are explicitly included in the home screen layout can be used on the device. Other apps, whether installed before or after the profile, are neither shown on the device nor can be launched. They are, however, present and are shown again when the profile is removed.

NOTE Administrators can access this editor only if the **Modify Mobile Device Configuration Profiles** option has been activated for their account.

Home screen pages

The home screen pages section of the home screen layout editor displays all individual pages that have been configured for this layout.

Actions possible in this section:

- The section can be scrolled horizontally.
- Pages can be dragged by their names (for example, "Page 1") to reorder them.
- Dragging app icons from the app list to a page adds that app to the page.
- Dragging app icons between pages or between locations on one page moves them to the new location.

- Moving the mouse over an app icon displays an “X” badge on the icon. Clicking that “X” removes the icon.
  Clicking the “X” for a built-in app such as Settings does not remove it, but hides it (see below).
  If the icon is a folder, the folder contents is removed as well.
- Right-clicking an app icon and choosing **Hide** from the context menu removes the app from the home screen and prevents its installation by any means until it is made visible again, as described in “App list” on page 681 or it has been added back to a home screen page by dragging it from the app list.
  Note that you can use this feature to hide most built-in apps, but some elementary apps, such as Settings and Phone, cannot be hidden.
- Right-clicking a folder icon and choosing **Remove** deletes the folder.
  Deleting a folder moves the apps in it to the app list and deletes any web clips it may contain.
- Pressing Command-A selects all icons on the most recently clicked page.
- Dragging an app icon on top of another app icon creates a folder with both apps. See below for a list of folder-related actions.
  Note that folders can only be created on home screen pages or in the dock, not inside other folders.
- Scrolling to the right and adding app icons to the New Page section adds another page to the layout.
- Dragging an image to a page sets that image as the home screen wallpaper.
  All pages and folders have the same wallpaper.
- When a wallpaper has been set, right-clicking a page and choosing **Remove Wallpaper** removes the wallpaper image for all pages.

Actions possible with folders:

- Dragging an icon on top of a folder icon moves it to the folder.
  It is not possible to move a folder to another folder.
- Double-clicking a folder displays its contents.
- App icons and app pages can be added to folders as described above for the main home screen pages.
- Dragging an app icon from the folder page to the “< Home Screen” label above the page lets you move the icon back to the main home screen page.
  When the last app is moved out of a folder, the folder is automatically removed.
- Double-clicking the folder name displayed above the folder pages lets you edit the name.

App list

The app list in the home screen layout editor displays all apps that can be added to the layout.

Apps with a green checkmark ✓ besides their names is used in the current layout. A red stop sign ⊘ can signify two things:

- The app has been hidden using the **Hide** command (see "Home screen pages" on page 680).
  Dragging an app marked for this reason to the home screen places it as usual and unhides it, as if the **Make Visible** context menu command had been chosen.
- The app is not applicable to the device chosen for the home screen configuration profile in the Home Screen Layout Profile Settings dialog.
  For example, when a layout for an iPad is created, Apple apps that do not run on iPads are marked with a stop sign.
  Dragging an app marked for this reason to the home screen places it as usual (and marks it with a green checkmark). Note, however, that this will not display the app on devices that do not support it or allow it to run on such devices.

Actions possible in the app list:

- Dragging an icon to the home screen pages or the Dock section adds it in the location where it is put.
- Entering text in the search field at the top displays only those apps with matching names.
- Choosing a command from the pop-up menu restricts the display to a certain kind of app:
  - **All Apps**: No restriction.
  - **System Apps**: Apps included with iOS.
  - **App Store Apps**: App Store apps listed in LANrev.
  - **Enterprise Apps**: Enterprise apps listed in LANrev.
  - **Device Apps**: Apps found on the selected devices. (Applies only when the layout editor was opened with the **Create Home Screen Layout Configuration Profile** command.)
  - **Used**: Apps that have been added to the layout.
  - **Unused**: Apps that have not yet been added.
  - **Hidden**: Apps that have been hidden.
  - **Category "xxx"**: Apps belonging to the specified category.
- Right-clicking an app and choosing **Hide** hides it. For details, see "Home screen pages" on page 680.
- Right-clicking an app and choosing **Remove** removes it from the layout. This command is available only for apps that have been placed in the layout.

Lock Screen section

The Lock Screen section of the home screen layout editor lets you set the wallpaper for the lock screen.

Actions possible in this section:

- Dragging an image to the "Drop image" area sets that image as the lock screen wallpaper.

- When the wallpaper has been set, right-clicking the section and choosing **Remove Wallpaper** removes the wallpaper .

Dock section

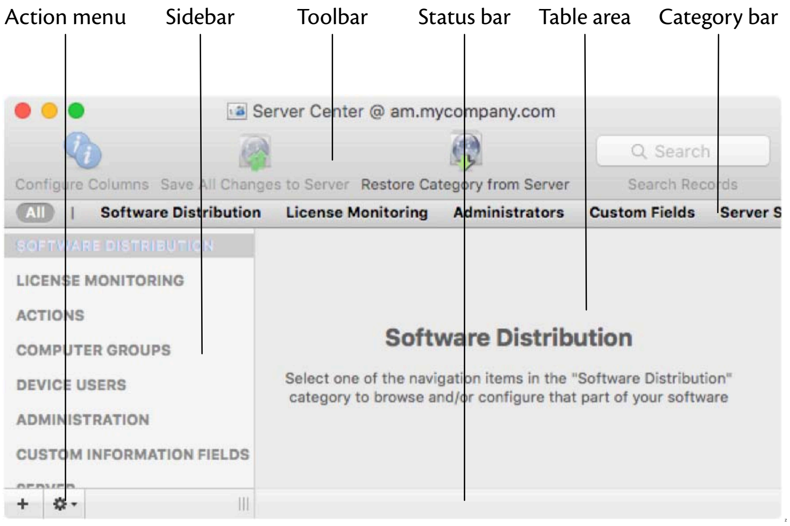
The Dock section of the home screen layout editor lets you specify the apps that appear in the device’s dock.

Actions possible in this section:

- Dragging app icons from the app list to the section adds that app to the dock.
- Dragging app icons to another location in the Dock section moves them to the new location.
- Moving the mouse over an app icon displays an “X” badge on the icon. Clicking that “X” removes the icon.
  Clicking the “X” for a built-in app such as Settings does not remove it, but hides it (see below).
  If the icon is a folder, the folder contents is removed as well.
- Right-clicking an icon and choosing **Hide** from the context menu removes the app from the home screen and prevents its installation by any means until it is made visible again, as described in “App list” on page 681 or it has been added back to a home screen page by dragging it from the app list.
- Pressing Command-A selects all icons if the Dock section is where you clicked most recently.
- Dragging an app icon on top of another app icon creates a folder with both apps. See “Home screen pages” on page 680 for a list of folder-related actions.

Chapter 24 Server Center

The Server Center is a module of the LANrev system that lets you easily manage the software distribution and license monitoring capabilities of the software. You can also manage administrator accounts, configure custom information fields, and set server options. All these functions are controlled via the **Server Center** window in LANrev Admin.



The elements of the **Server Center** window are described below:

- **Toolbar** (page 686)
- **Category bar** (page 691)
- **Status bar** (page 691)
- **Table columns** (page 691)
- **Sidebar** (page 692)
- **Action and context menus** (page 698)
  - **Software Distribution** (page 699)
    - **New Software Package** (page 700)
    - **New Metapackage** (page 710)
    - **Duplicate Software Package** (page 718)
    - **New Smart Software Package Group** (page 718)
    - **New Payload** (page 719)
    - **Duplicate Payload** (page 720)
    - **New Smart Payload Group** (page 720)
    - **New Mac App Store Application Package** (page 721)
    - **New Smart Mac App Store Application Group** (page 722)
    - **New Configuration Profile** (page 722)
    - **New Smart Configuration Profile Group** (page 725)
    - **New Device Enrollment Profile** (page 725)
    - **New Smart Enrollment Profile Group** (page 725)
    - **New Distribution Point** (page 725)
    - **New Smart Distribution Point Group** (page 727)
    - **New Disk Image** (page 728)

  - **Edit <item>** (page 773)
  - **Remove <item>** (page 774)
  - **Retrieve Payloads** (page 774)
  - **Retry Package** (page 774)
  - **Reset Package** (page 775)
  - **Export Package** (page 775)
  - **Install Selected Software Packages** (page 775)
  - **Export License Specification** (page 775)
  - **Repeat Selected Installations** (page 776)
  - **Show Action Details** (page 776)
  - **Duplicate Action** (page 776)
  - **Edit Action** (page 776)
  - **Remove Action** (page 776)
  - **Remove Action from Group** (page 777)
  - **Re-execute This Action for All Devices** (page 777)
  - **Re-execute This Action for This Group** (page 777)
  - **Change Action Schedule** (page 777)
  - **Reset Current Server Load** (page 778)
  - **Assign Device Enrollment Profile** (page 778)
  - **Unassign Device Enrollment Profile** (page 778)
  - **Enroll Devices in MDM** (page 779)
  - **Install LANrev Agent via MDM** (page 779)
  - **Reload Device Enrollment Data** (page 780)
- **Server** (page 780)
  - **Server Settings** (page 780)
  - **Certificate Settings** (page 799)
  - **Server Monitor** (page 800)

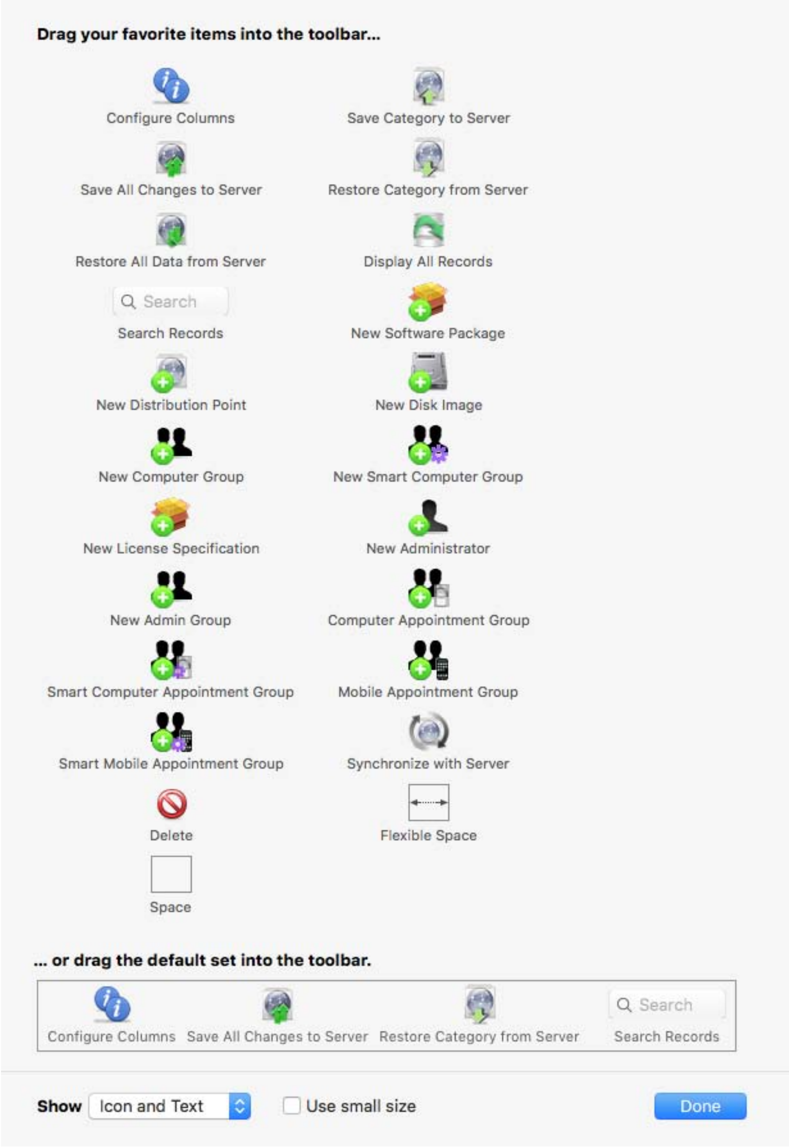
The + button in the lower left-hand corner is not separately described; clicking it creates an item in the selected folder, just as if you had chosen the appropriate menu command.

Toolbar

The **Server Center** window has a toolbar that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar can contain these elements:



The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** through **Print**).

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Save Category to Server

The **Save Category to Server** command updates the LANrev server with the changes that you have made in currently active category in the **Server Center** window.

Categories include:

- Software distribution and licensing (comprises the **Software Distribution**, **License Monitoring**, and **Computer Groups** headings in the sidebar)
- Administration
- Custom information fields
- Server settings

Clicking **Save Category to Server** has the same effect as choosing the corresponding **Save …** command from the **Server** menu.

Save All Changes to Server

The **Save All Changes to Server** icon updates the LANrev Server with all changes that you have made locally in the **Server Center** window.

It has the same effect as the **Save All Settings** command described on page 484.

Restore Category from Server

The **Restore Category from Server** icon loads the data for the currently active category from the server and replaces the local data in that category with it.

The categories are the same as for the **Save Category to Server** button described above.

Clicking **Restore Category from Server** has the same effect as choosing the corresponding **Restore …** command from the **Server** menu.

Restore All Data from Server

The **Restore All Data from Server** command loads all data for all categories in the Server Center window from the LANrev server, overwriting any changes you may have made locally.

It has the same effect as the **Restore All Settings** command described on page 484.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

It has the same effect as the **Display All Records** command described on page 397.

Search Records

The **Search Records** field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Pressing Return executes the search.

New Software Package

The **New Software Package** command opens the dialog for specifying a new software package.

It has the same effect as the **New Software Package** command described on page 700.

New Distribution Point

The **New Distribution Point** command opens the dialog for specifying a new distribution point.

It has the same effect as the **New Distribution Point** command described on page 725.

New Disk Image

The **New Disk Image** command opens the dialog for specifying a new disk image.

It has the same effect as the **New Disk Image** command described on page 728.

New Computer Group

The **New Computer Group** command opens the dialog for specifying a new computer group.

It has the same effect as the **New Computer Group** command described on page 740.

New Smart Computer Group

The **New Smart Computer Group** command opens the dialog for specifying a new smart computer group.

It has the same effect as the **New Smart Computer Group** command described on page 741.

New License Specification

The **New License Specification** command opens the dialog for specifying a new license specification.

It has the same effect as the **New License Specification** command described on page 732.

New Administrator

The **New Administrator** button creates a new administrator account.

It has the same effect as the **New Administrator** command described on page 758.

New Admin Group

The **New Admin Group** button creates a new group for administrator accounts in the sidebar.

It has the same effect as the **New Administrator Group** command described on page 763.

Computer Appointment Group

The **Computer Appointment Group** button creates a new appointment group in the sidebar for assigning administrators to computers.

It has the same effect as the **New Computer Appointment Group** command described on page 763.

Smart Computer Appointment Group

The **Smart Computer Appointment Group** button creates a new appointment group in the sidebar for assigning administrators to computers.

It has the same effect as the **New Smart Computer Appointment Group** command described on page 764.

Mobile Appointment Group

The **Mobile Appointment Group** button creates a new appointment group in the sidebar for assigning administrators to mobile devices.

It has the same effect as the **New Mobile Devices Appointment Group** command described on page 763.

Smart Mobile Appointment Group

The **Smart Mobile Appointment Group** button creates a new appointment group in the sidebar for assigning administrators to computers.

It has the same effect as the **New Smart Mobile Devices Appointment Group** command described on page 764.

Synchronize with Server

The **Synchronize with Server** button synchronizes the currently displayed section of the Server Center (for example, software distribution or server settings) with the server.

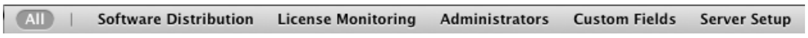
Delete

The **Delete** command deletes the selected objects from the window.

It has the same effect as the **Delete** command described on page 392.

Category bar

The **Server Center** window contains a category bar that lets you restrict the display in the window to one or a few of the categories listed in the sidebar.



Clicking each category toggles its display on or off. If all categories are off in the category bar, all categories are displayed. You can activate display of each category independently of the others, for example, displaying custom information fields together with the server setup.

NOTE Clicking a category with the Option key held down restricts the display in the window to that category.

Computer groups are displayed if either **Software Distribution** or **License Monitoring** is activated; they cannot be displayed or hidden on its own.

Status bar

The **Server Center** window has a status bar displaying information on the state of the Server Center.

The status bar displays the number of records currently shown in the window.

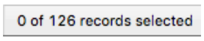

0 of 126 records selected

Table columns

The columns displayed in the **Server Center** change depending on the object selected in the sidebar.

The columns display information items applicable to the category selected in the sidebar or a custom information view similar to a dialog. Columns can be configured as for other browser windows. (Configuring columns is described in “Opening and configuring browser windows” on page 132.)

Sidebar

The **Server Center** window contains a sidebar with a number of categories and smart groups custom-made for using the Server Center's functions. The smart groups are divided into several categories; there are also settings categories.

Categories in the sidebar that contain modifications which require uploading to the server before becoming active are marked with a small pen icon (✎). Choose the appropriate command from the **Server** menu to save these changes to the server.

Software Distribution

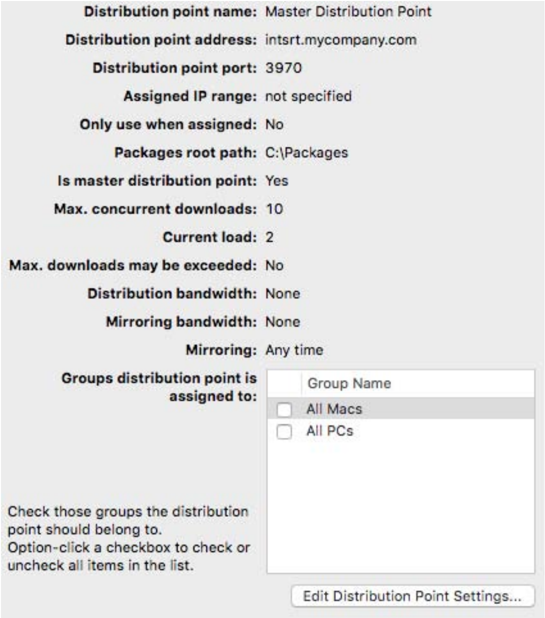
This category contains several subcategories:

- **Payloads**: All installers and installer help support files that have been defined for software distribution.
  Clicking a payload displays the payload's details in the main window area. Double-clicking a payload displays the **Payload** dialog.
- **Software Packages**: All software packages and metapackages that have been defined for software distribution.
  Clicking a package or metapackage displays its settings in the main window area. You can check groups to assign the package to these groups. Holding down the Option key checks or unchecks all groups in the list.
  Double-clicking a metapackage opens the **Software Distribution Metapackage** dialog. Double-clicking a software package opens the **Software Distribution Package** dialog.
  Clicking a payload displays the file contained in the payload. Double-clicking a payload file displays the **Payload** dialog.
- **macOS Patches**: All software packages that have automatically been created by the operating system patch management for macOS clients. (Details are available in "Automated patch management" on page 333.)
  - **Accepted Patches**: Automatically created patch software packages that have been accepted by an administrator.
  - **Rejected Patches**: Automatically created patch software packages that an administrator has decided should not be installed on client macOS computers.
  - **Unconfirmed Patches**: Automatically created patch software packages that no administrator has yet decided on.

  Within these categories, patches are further grouped according to the version of macOS to which they apply. Some patches may apply to more than one version. In this case, they are listed in all applicable subgroups. Deleting the patch from any of those groups deletes it from all others as well.
  Clicking a patch displays its details in the **Server Center** window's table area. Double-clicking a patch opens it in an editing dialog similar to the one described in **New Software Package** (page 700).

- **macOS Third-Party Patches**: All software packages that have automatically been created by the third-party patch management for macOS clients. (Details are available in “Automated patch management” on page 333.)
  The subcategories are the same as for **macOS Patches**, described above, except that third-party patches are not further grouped by OS version.
- **Windows Patches**: All software packages that have automatically been created by the operating system patch management for Windows clients. (Details are available in “Automated patch management” on page 333.)
  The subcategories are the same as for **macOS Patches**, described above. Patches for Windows are also subgrouped according to the Windows version for which they are intended.
- **Windows Third-Party Patches**: All software packages that have automatically been created by the third-party patch management for Windows clients. (Details are available in “Automated patch management” on page 333.)
  The subcategories are the same as for **macOS Patches**, described above, except that third-party patches are not further grouped by OS version.
- **Mac App Store Applications**: All packages for Mac app store apps that have been created in LANrev.
- **Configuration Profiles**: All computer configuration profiles that have been created in or imported into LANrev.
  Clicking a profile displays its details in the main window area. Double-clicking it opens the profile in the configuration profile editor.
- **Device Enrollment Profiles**: All device enrollment profiles that have been created in LANrev.
- **macOS Disk Images**: All disk images for macOS clients that have been defined for software distribution.
  Clicking a disk image displays its details in the main window area. Double-clicking it lets you edit its name.
- **Windows Disk Images**: All disk images for Windows clients that have been defined for software distribution.
- **Distribution Points**: All distribution points that have been defined for software distribution.

Clicking a distribution point displays its settings and an editable list of groups to which it is assigned:



Distribution point name: Master Distribution Point
Distribution point address: intsrt.mycompany.com
Distribution point port: 3970
Assigned IP range: not specified
Only use when assigned: No
Packages root path: C:\Packages
Is master distribution point: Yes
Max. concurrent downloads: 10
Current load: 2
Max. downloads may be exceeded: No
Distribution bandwidth: None
Mirroring bandwidth: None
Mirroring: Any time
Groups distribution point is assigned to:

Group Name
☐ All Macs
☐ All PCs

Check those groups the distribution point should belong to.
Option-click a checkbox to check or uncheck all items in the list.

Checking a group assigns the distribution point to it, unchecking the group unassigns the distribution point. When a distribution point is assigned to a group, computers from that group download installers preferably from that distribution point.

Note: Holding down the Option key while clicking a checkbox in the list of assigned groups checks or unchecks all groups in the list.

Double-clicking a distribution point displays its settings in the **Distribution Point** dialog.

- **Software Installation Status**: This is a collection of smart groups that contain software installation processes by their states:
  - **General log**: All installation processes, whether scheduled, under way, or completed.
  - **Installations in Progress**: Installation processes that have begun but are not yet completed.
  - **Successful Installations**: Installation processes that have been completed with the successful installation of the software.
  - **Failed Installations**: Installation processes that have been terminated without successfully installing the software.
  - **Deferred Installations**: Installation processes that were scheduled for a time in the past but had to be deferred because the target computer could not be contacted.
  - **Refused Installations**: Installation processes that failed because the user of the target computer declined the installation.

- **Profile Installation Status**: This is a collection of smart groups that contain installation processes for computer configuration profiles by their states:

  - **General log**: All installation processes, whether scheduled, successful or unsuccessful.
  - **Successful Installations**: Installation processes that have been completed with the successful installation of the profile.
  - **Failed Installations**: Installation processes that have been terminated without successfully installing the profile.

Clicking any subcategory displays all installation processes that are part of the category.

License Monitoring

- **License Specifications**: All license specifications that have been defined for license monitoring.
  Clicking a license specification displays its details in the main window area. Double-clicking it opens the **License Specification** dialog.
- **License Purchases**: All license specifications for which license purchases that have been entered.
  Clicking a license specification here displays the specification's purchasing details in the main window area. Double-clicking it opens the **License Specification** dialog.
- **Reports**: This is a collection of smart groups that contain license specifications by their states and other reports:
  - Selecting the **Reports** group itself displays all license specifications, regardless of status.
  - **Fully compliant**: All software licenses that are not exceeded.
  - **Licenses exceeded**: All software licenses that are used more often than the number of licenses in the license specification allows.
  - **Prohibited software**: All found software instances that are prohibited according to its license specifications. Each agent has one entry per type of prohibited software that was detected on it.
  - **Undetermined licenses**: All license specifications that have been defined and saved to the LANrev server, but which no agent has yet checked for.
  - **Software usage**: All found software instances on all agents. Each agent has one entry per licensed software that was detected on it.
  - **Missing software**: License specifications that are assigned to a computer group but not present on all computers of each group to which they have been assigned. There is one entry per missing software per agent.
  - **History**: List of all license monitoring counts. Each count is timestamped. There is one entry for each license specification per reporting date.
  - **History summary**: A statistical overview of the license usage in the past.

Clicking any of the subcategories displays the items that belong to it.

Computer Groups

This category contains all computer groups that you have defined. It also creates a few predefined smart groups:

- **All Macs**: All administered computers running macOS.
  - **Assigned Packages**: All packages that are assigned to the group.
    Clicking the subcategory displays all assigned packages.
  - **Assigned License Specifications**: All license specifications that are assigned to the group.
    Clicking the subcategory displays all assigned license specifications.
  - **Assigned Distribution Points**: All distribution points that are assigned to the group. Assigning distribution points to a group tells the LANrev agents in the group to prefer these distribution points for installer downloads.
    Clicking the subcategory displays all assigned distribution points.
  - **Forbidden Configuration Profiles**: All configuration profiles that may not be installed on the computers in this group.
  - **Auto-install Configuration Profiles**: All configuration profiles that are automatically installed on any computer that becomes a member of this group.
  - **Auto-install, Auto-remove Configuration Profiles**: All configuration profiles that are automatically installed on any computer that becomes a member of this group and are automatically removed from any computer that leaves this group.
  - **Device Enrollment Profiles**: The device enrollment profile that is automatically installed on all members of the computer group, except for computers on which a device enrollment profile has already been installed through another computer group.
    Note that, if a computer belongs to multiple groups that each specify an enrollment profile, it is undefined which profile is assigned to the computer. We therefore recommend that you set up your groups so that no computer belongs to more than one group with a device enrollment profile.
- **All PCs**: All administered computers running Windows.
  This smart group contains the same subgroups as **All Macs**, described above, except for the **Device Enrollment Profiles** group.
- **Unassigned Computers**: All administered computers that are not part of any computer group.
  Clicking the category displays all unassigned computers.

Device Users

All users that have enrolled with their Active Directory or Open Directory accounts that have been created in LANrev.

Each user entry in the sidebar can be expanded to list the computers assigned to the user.

The users listed are the same as in the sidebar of the Mobile Devices window, although the devices are different.

Administration

- **Active Directory**: All Active Directory accounts from the Active Directory groups that have been specified in the **Server Settings** dialog's **Active Directory** subpane.
- **Administrators**: All administrator accounts that have been defined in LANrev Server and all manually managed administrator groups.
  Clicking an administrator displays all agents to which it has been assigned in the main window area.
  Double-clicking an administrator displays its settings in the **Administrators** dialog.
- **Appointments**: All standard and smart appointment groups. Any devices that have not been added to any appointment group are contained in the **Unmanaged Computers** and **Unmanaged Mobile Devices** groups.
  Clicking an appointment group displays the devices that are part of it. Double-clicking a standard appointment group lets you edit its name; double-clicking a smart appointment group lets you edit its definition.
  Clicking the **Assigned Admins** category within an appointment group displays the administrators that are part of the group.

The **Administration** category also contains all smart administrator groups that have been defined.

Clicking a smart administrator group displays all administrators who belong to it; double-clicking the group opens its definition.

Custom Information Fields

This category contains all custom information fields that have been defined.

Clicking a custom information field displays its settings in the main window area.

Server

This category groups the server-related information.

- **Server Settings**: Clicking this subcategory displays the server settings in a dialog-like format in the main part of the **Server Center** window.
  This is described in “Server Settings” on page 780.
- **Certificate Settings**: Clicking this subcategory displays the settings required for SCEP access.
  This is described in “Certificate Settings” on page 799.

- **Server Monitor**: Clicking this subcategory displays a monitoring pane in which important server statistics are displayed.
  This is described in “Server Monitor” on page 800.

Action and context menus

The action and the context menus of the **Server Center** window contain commands for managing all elements of the center.

The commands are described in detail in the following sections

- **Software Distribution** (page 699)
  - **New Software Package** (page 700)
  - **New Metapackage** (page 710)
  - **Duplicate Software Package** (page 718)
  - **New Smart Software Package Group** (page 718)
  - **New Payload** (page 719)
  - **Duplicate Payload** (page 720)
  - **New Smart Payload Group** (page 720)
  - **New Mac App Store Application Package** (page 721)
  - **New Smart Mac App Store Application Group** (page 722)
  - **New Configuration Profile** (page 722)
  - **New Smart Configuration Profile Group** (page 725)
  - **New Device Enrollment Profile** (page 725)
  - **New Smart Enrollment Profile Group** (page 725)
  - **New Distribution Point** (page 725)
  - **New Smart Distribution Point Group** (page 727)
  - **New Disk Image** (page 728)
  - **New Smart Disk Image Group** (page 729)
  - **New Smart Software Installation Status Group** (page 730)
  - **New Smart Profile Installation Status Group** (page 730)
  - **New Missing Software Packages Group** (page 731)
- **License Monitoring** (page 732)
  - **New License Specification** (page 732)
  - **New Smart License Specification Group** (page 738)
  - **New License Status Report** (page 738)
  - **New Software Usage Report** (page 739)
  - **New History Report** (page 739)
  - **New History Summary Report** (page 740)
  - **New Missing Software Report** (page 740)
- **Computer Groups** (page 740)
  - **New Computer Group** (page 740)
  - **New Smart Computer Group** (page 741)
  - **Remove All Group Members** (page 742)
- **Administrator Setup** (page 758)
  - **New Administrator** (page 758)
  - **Remove Administrator from Group** (page 763)
  - **New Administrator Group** (page 763)
  - **New Computer Appointment Group** (page 763)
  - **New Smart Computer Appointment Group** (page 764)
  - **New Mobile Devices Appointment Group** (page 765)

  - **New Smart Mobile Devices Appointment Group** (page 765)
  - **New Smart Administrator Group** (page 766)
  - **Refresh** (page 767)
- **Custom Information Fields** (page 767)
  - **New Custom Information Field** (page 767)
  - **Duplicate Custom Information Field** (page 771)
  - **Export Selected Fields** (page 772)
  - **Import Fields** (page 772)
- **New Category** (page 772)
- **Edit <item>** (page 773)
- **Remove <item>** (page 774)
- **Retrieve Payloads** (page 774)
- **Retry Package** (page 774)
- **Reset Package** (page 775)
- **Export Package** (page 775)
- **Install Selected Software Packages** (page 775)
- **Export License Specification** (page 775)
- **Repeat Selected Installations** (page 776)
- **Show Action Details** (page 776)
- **Duplicate Action** (page 776)
- **Edit Action** (page 776)
- **Remove Action** (page 776)
- **Remove Action from Group** (page 777)
- **Re-execute This Action for All Devices** (page 777)
- **Re-execute This Action for This Group** (page 777)
- **Change Action Schedule** (page 777)
- **Reset Current Server Load** (page 778)
- **Enroll Devices in MDM** (page 779)
- **Install LANrev Agent via MDM** (page 779)
- **Reload Device Enrollment Data** (page 780)
- **Update AD User Information** (page 780)

When one or more administered computers are selected in the window, other commands are displayed in the context menu that are described in “Commands menu” on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Software Distribution

The **Software Distribution** submenu contains commands for managing software distribution functions:

- **New Software Package** (page 700)
- **New Metapackage** (page 710)
- **Duplicate Software Package** (page 718)
- **New Smart Software Package Group** (page 718)
- **New Payload** (page 719)
- **Duplicate Payload** (page 720)
- **New Smart Payload Group** (page 720)
- **New Mac App Store Application Package** (page 721)
- **New Smart Mac App Store Application Group** (page 722)
- **New Configuration Profile** (page 722)

- **New Smart Configuration Profile Group** (page 725)
- **New Device Enrollment Profile** (page 725)
- **New Smart Enrollment Profile Group** (page 725)
- **New Distribution Point** (page 725)
- **New Smart Distribution Point Group** (page 727)
- **New Disk Image** (page 728)
- **New Smart Disk Image Group** (page 729)
- **New Smart Software Installation Status Group** (page 730)
- **New Smart Profile Installation Status Group** (page 730)
- **New Missing Software Packages Group** (page 731)

New Software Package

The **New Software Package** command creates a new software package.

Choosing the command opens the **Software Distribution Package** dialog. The dialog has four panes:

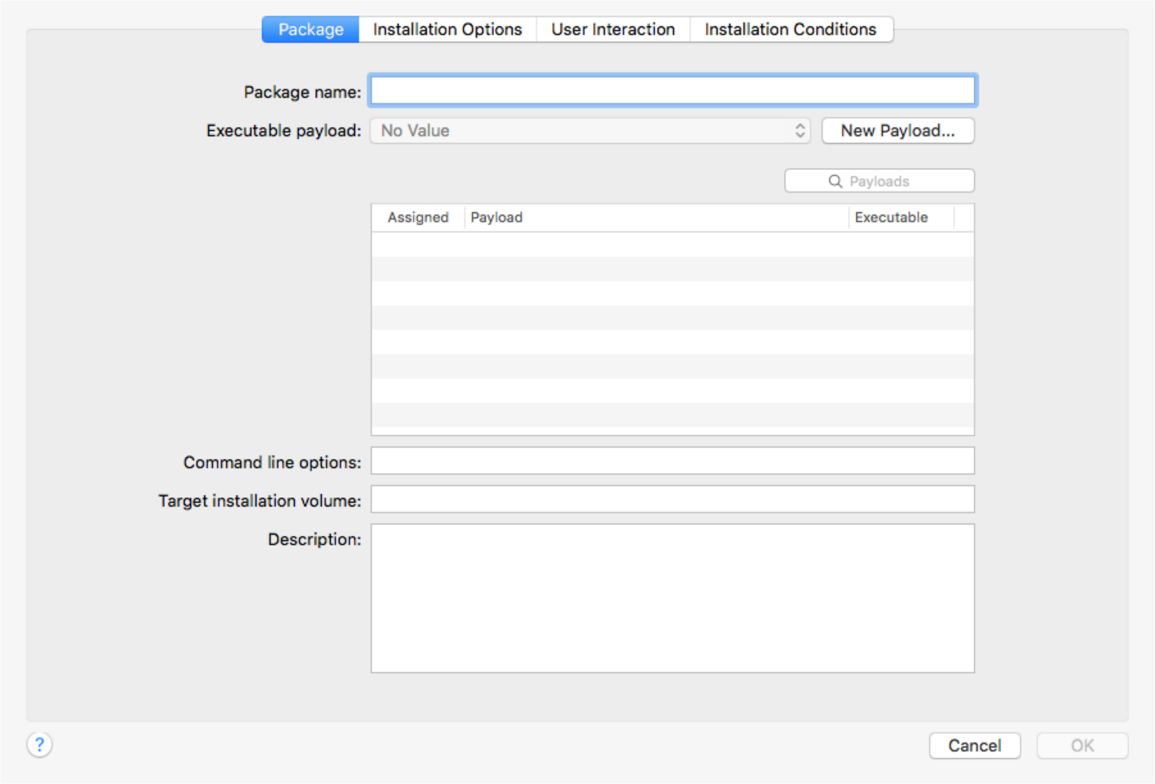
- **Package**
- **Installation Options**
- **User Interaction**
- **Installation Conditions**
- **Adobe CS Options**

All four are described below.

NOTE The **New Software Package** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 758 for details.

Package

The **Package** pane of the **Software Distribution Package** dialog lets you specify basic settings for the software package:



The pane contains these elements:

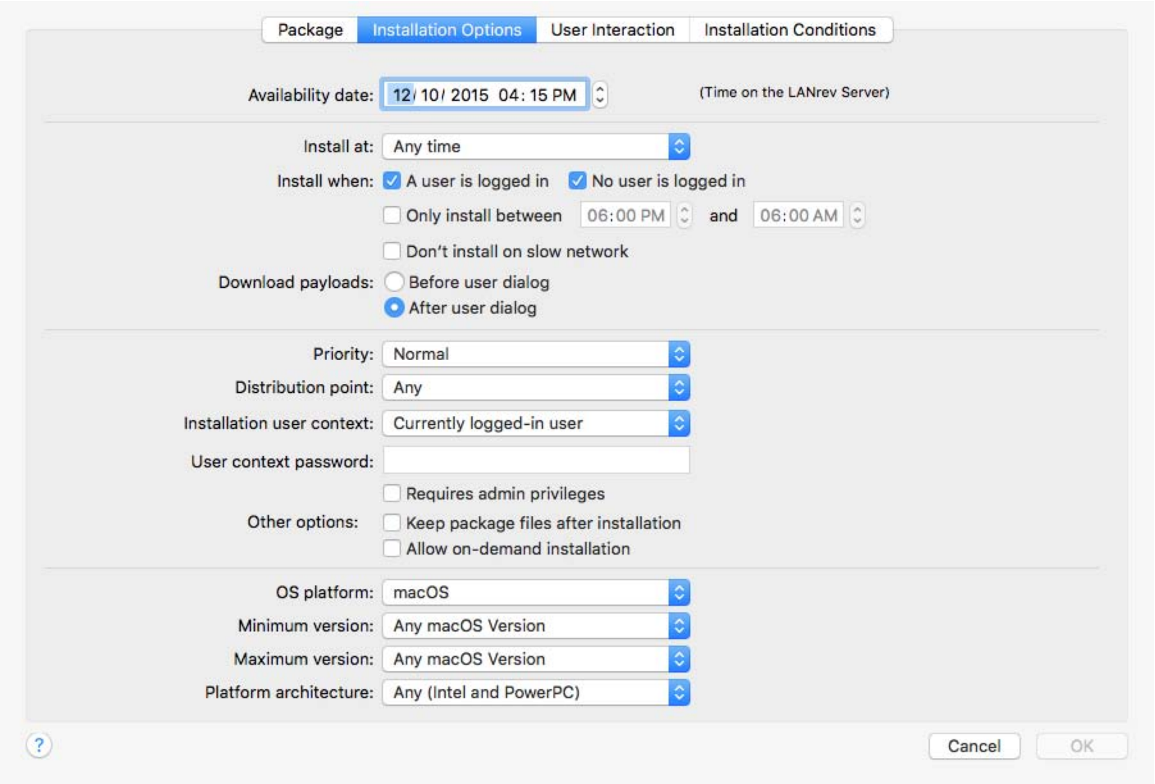
- **Package Name**: The name of the software package.
- **Executable Payload**: The payload that will be launched on the client computers to install this package.
  A package can have any number of payloads; however, there must be exactly one executable payload. Executable payloads can be applications (in particular, installers) or, for macOS target computers, shell scripts.
  Note: Non-executable payloads can, for example, be configuration files for the installer (the executable payload). Including a configuration file as the non-executable payload allows you to perform different installations without needing multiple copies of the executable.
  You can choose the executable from the pop-up menu. The menu contains all payloads checked in the list of payloads.
  Clicking the **New Payload** button opens the **Payload** dialog, letting you define a new payload on the fly.
  The search field lets you filter the list of available payloads.
- **Command line options**: Options for the execution of the payload. (Optional.)
  You can include shell variables in the options, as described in “Environment variables” on page 176.
  Note: When the executable is an MSI, MSP patch file, or MSU updater file and you do not specify command line options,

LANrev adds the `/qn` *option (*`/quiet /norestart` *for MSU files) to run the installer silently.*

- **Target installation volume**: The volume of the target computers on which the software is to be installed; relevant for macOS only. When this is empty, the software is installed on the boot volume.
- **Description**: A description of the software contained in the package. This text is displayed if the local user is asked for confirmation.

Installation Options

The **Installation Options** pane of the **Software Distribution Package** dialog lets you specify various options for the installation of the package:



Availability date: 12/ 10/ 2015 04: 15 PM (Time on the LANrev Server)

Install at: Any time

Install when: ☑ A user is logged in ☑ No user is logged in

□ Only install between 06:00 PM and 06:00 AM

□ Don't install on slow network

Download payloads: ○ Before user dialog ● After user dialog

Priority: Normal

Distribution point: Any

Installation user context: Currently logged-in user

User context password:

Other options: □ Requires admin privileges □ Keep package files after installation □ Allow on-demand installation

OS platform: macOS

Minimum version: Any macOS Version

Maximum version: Any macOS Version

Platform architecture: Any (Intel and PowerPC)

The pane contains these elements:

- **Availability date**: The earliest date when this package may be used for software installations on administered computers.
- **Install at**: Whether to install the package anytime or just on particular occasions.
- **Install when**: These options let you further specify conditions that must be met for the installation to proceed:
  - **A user is logged in**: If this option is checked, the package will be installed when a user is logged in on the target computer.

  - **No user is logged in**: If this option is checked, the package will be installed when no user is logged in on the target computer (and the computer is running).

  Note: Both these options can be checked at the same time, in which case the package is installed irrespective of whether a user is logged in. It is not possible to uncheck both options. Note, too, that certain settings in the **User Interaction** *pane force the settings of these options, in which case they are disabled.*

  - **Only install between**: This option lets you restrict the installation of the package to a certain period of the day, for example, after hours.
- **Don’t install on slow network**: If this option is checked, installations take place only when the network connection between the client and the distribution point has a nominal transfer rate of at least 100 Mbit/s.
- **Download payloads**: This setting specifies when the Agent downloads a payload, before displaying a user dialog or after. Downloading the payload before displaying the dialog makes the installation feel more responsive to the user. Downloading the payload after the dialog avoids unnecessary downloads when the user cancels the installation.

  The setting has no effect when there is no user interaction during the installation.
- **Priority**: The priority of this package. When more than one package is available for installation on a client, packages with higher priorities are installed first.
- **Distribution point**: An optional restriction on the distribution point from which the installer is transferred to the client:
  - **Any**: No restriction.
  - **From assigned distribution point if available**: When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, another distribution point is used.
  - **From assigned distribution point only**: When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, the installation fails.

  An assigned distribution point is a distribution point that either includes the agent’s IP address in the range of IP addresses it is set to serve (see “New Distribution Point” on page 725 for details) or that has been assigned to a computer group of which the target computer is a member.

  If no IP range has been specified in a distribution point definition, it is considered to be assigned to all clients in the same subnet. (The server’s subnet mask is used to determine the extent of the subnet.)

  Note that a distribution point with the **Only use when assigned to group or via IP range** setting active will never serve packages to clients to which it has not been assigned, irrespective of the distribution point setting in the package.
- **Installation user context**: The user name of the account that is to be used for running the installer.

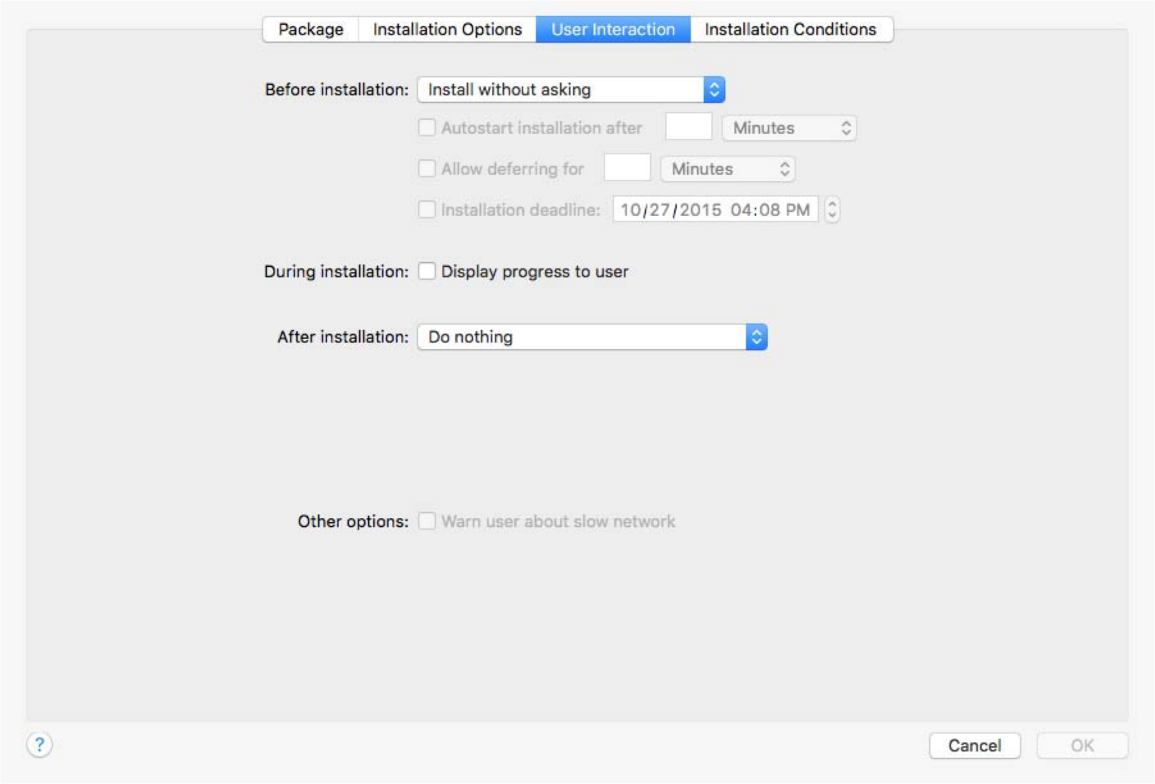
The **Currently logged-in user** option runs the installation in the user context of the user who is logged in on the client computer at installation time.
The **System account user** option runs the installation from the system user account.

- **User context password**: The password for the account to be used. This is not required for installations on macOS.
- **Requires admin privileges**: This option applies only to installations on macOS. If it is checked, the installer is authorized to run with administrator privileges.
  Note: This does not change the user account from which the package is installed; it merely increases the available privileges for the installation, if necessary.
- **Other options**: Miscellaneous settings.
  - **Keep package files after installation**: If this option is checked, LANrev does not delete the installation files after the installation is complete.
  - **Allow on-demand installation**: If this option is checked, this package appears when the user manually queries the software distribution server for new packages.
    Checking this option disables a number of other options in the **Installation Options** and **User Interaction** panes.
- **OS Platform**: The operating systems on which the package may be installed.
  For automatically generated OS patches, this information is disregarded and cannot be edited.
- **Minimum OS**: The lowest version of the operating system on which the package may be installed.
  For automatically generated OS patches, this information is disregarded and cannot be edited.
- **Maximum OS**: The highest version of the operating system on which the package may be installed.
  For automatically generated OS patches, this information is disregarded and cannot be edited.
- **Platform architecture**: This option lets you restrict the installation to only Intel or PowerPC-based computers under macOS. Under Windows, you can restrict installations to 32-bit or 64-bit versions of the OS.
  For automatically generated OS patches, this information is disregarded and cannot be edited.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

User Interaction

The **User Interaction** pane of the **Software Distribution Package** dialog lets you specify the information users are given during the installation process and the actions they can perform:



Before installation: Install without asking

□ Autostart installation after Minutes

□ Allow deferring for Minutes

□ Installation deadline: 10/27/2015 04:08 PM

During installation: □ Display progress to user

After installation: Do nothing

Other options: □ Warn user about slow network

The pane contains these elements:

- **Before installation**: The way in which the user may influence the installation:
  - **Install without asking**: The user is not informed of the installation.
  - **Inform user before installation**: The user is informed of the installation before the fact but cannot affect it.
  - **Allow to reschedule**: The user can postpone the installation but not disallow it altogether.
  - **Allow to refuse**: The user may altogether refuse to have this package installed on his or her computer.
- **Autostart installation after**: This option is only active when a **Before installation** option other than **Install without asking** is chosen. It lets you specify a time after which the installation starts automatically when the user does not respond to the installation notification.
- **Allow deferring for**: This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the maximum time for which users can postpone the installation.
- **Installation deadline**: This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before**

installation option. It lets you specify the latest time when the installation must begin.

NOTE When you specify both a maximum deferring interval and an installation deadline, both are active. This means that the earlier of the two resulting dates becomes effective: If the deadline is reached, the installation is forced (unless the user has canceled it altogether), even if the interval has not yet expired. And if the interval expires, the installation begins even if the deadline has not yet been reached.

- **Display progress bar to the user**: If this option is checked, the users of the target computers are informed of the installation progress by a progress bar. If the option is unchecked, there is no feedback on the progress.
- **After installation**: The action that LANrev Agent performs on the target computer after the installation is complete:
  - **Do nothing**: No action is performed.
  - **Notify user**: A message informing the user of the completed installation is displayed.
    An additional option becomes available:
    - **Automatically close notification after**: This option lets you specify a time after which LANrev Agent automatically closes the notification alert.
  - **Restart**: The computer is automatically restarted without a notification displayed first. Processes are sent termination messages, allowing data in open documents to be saved first.
    Additional options become available:
    - **Show notification**: Checking this option causes LANrev Agent to display a notification of the pending restart. The restart happens after the user has responded to the notification.
    - **Restart after no more than**: This option is available only when **Show notification** has been checked. It lets you set an interval after which the restart is performed even when the user does not respond to the notification.
    - **Allow user to postpone restart**: This option is available only when **Show notification** has been checked. It lets you give the user the option to defer the restart to a later date.
    - **Show dialog again every**: This option is available only when **Allow user to postpone restart** has been checked. It lets you make LANrev display the restart notification dialog at regular intervals, reminding the user that a restart is still required. If an interval has been specified in the **Restart after no more than** option (see above), it applies to these reminders as well.
  - **Force restart**: As **Restart**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost. The same options as for **Restart** become available.
  - **Force restart (FileVault authenticated)**: As **Force restart**, above, but the FileVault is unlocked without

requiring the presence of a local user to enter the FileVault key.
This option applies only to computers meeting all these criteria:

- macOS 10.8.2 and above.
- MacBook Pro mid 2009 or newer, MacBook or iMac late 2009 or newer, Mac mini mid 2010 or newer, MacBook Air late 2010 or newer, Mac Pro late 2013 or newer.
- The currently valid FileVault key has been stored in LANrev. (See “macOS profiles” on page 668 for more information.)

Other computers will be simply force-restarted.
Choosing this option lets you start the administered computer once without requiring the presence of the local user to enter the FileVault password.
Note: This option leaves the target computers running and unlocked. Depending on the circumstances, this may present a security risk.

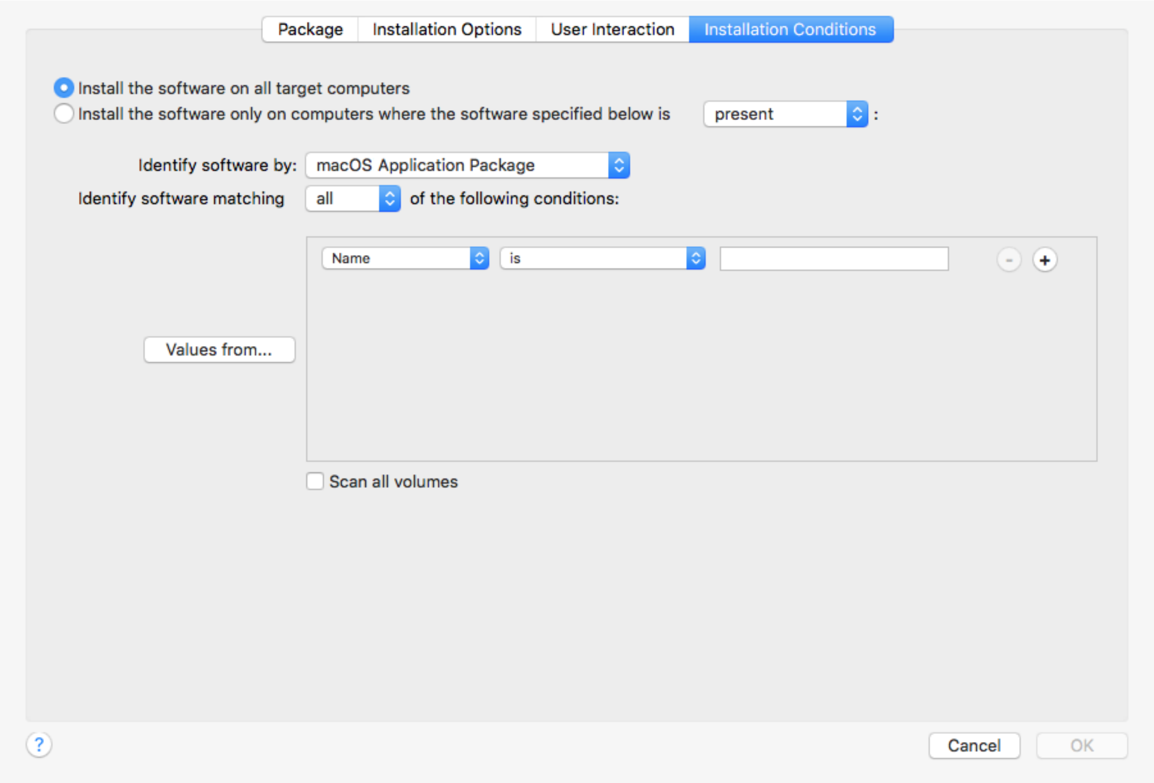
- **Shut down**: As **Restart**, above, but the target computer is shut down instead of restarted.
  The same options as for **Restart** become available.
- **Force shutdown**: As **Shut down**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost.
  The same options as for **Restart** become available.

- **Warn about slow network**: If this option is checked, the user of a target computer is warned before installations when the network connection between the client and the distribution point has a nominal transfer rate of less than 100 Mbit/s. The warning is not displayed if the software package is set to install without asking the user.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

Installation Conditions

The **Installation Conditions** pane of the **Software Distribution Package** dialog lets you specify that a package be installed only on client computers that meet certain criteria:



● Install the software on all target computers
○ Install the software only on computers where the software specified below is present :

Identify software by: macOS Application Package

Identify software matching all of the following conditions:

Name is

□ Scan all volumes

The pane contains these elements:

- **Install the software on all target computers**: The package will be installed on all computers in the computer groups to which it is assigned.
- **Install the software only on computers where the software specified below is**: Choose whether the package is to be installed only on computers that already have certain software (choose **present**) or on computers that lack specified software (choose **not present**).

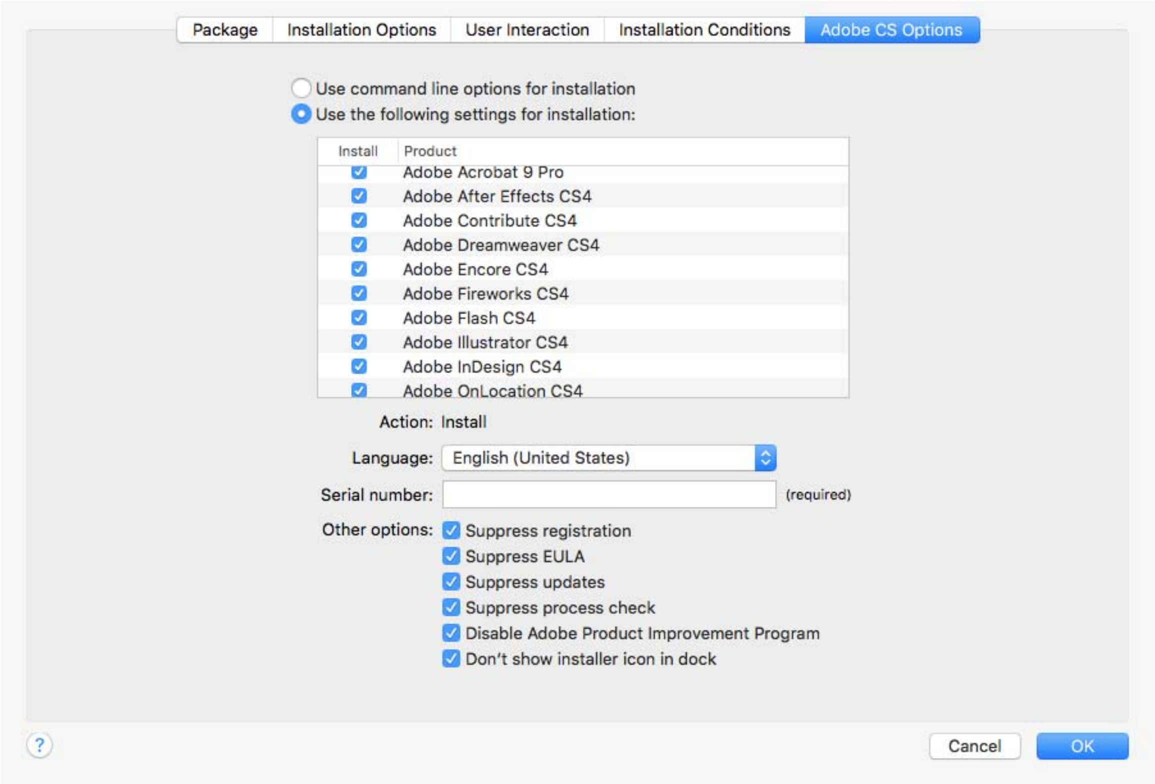
The rest of the elements are similar to the corresponding ones in the **New License Specification** dialog discussed on page 732.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

Adobe CS Options

The **Adobe CS Options** pane of the **Software Distribution Package** dialog lets you set special options for installing, uninstalling or updating the Adobe Creative Suite. The tab is available only when a payload containing an Adobe CS3 or CS4 installer or updater is assigned to the software package.

NOTE The settings in this tab are not compatible with Adobe CS 5 or newer. For remotely distributing these versions of Adobe CS, prepare an installer using Adobe Application Manager Enterprise Edition (AAMEE) and use that installer to create a standard software distribution package in LANrev Admin.



○ Use command line options for installation
● Use the following settings for installation:

Install	Product
☑	Adobe Acrobat 9 Pro
☑	Adobe After Effects CS4
☑	Adobe Contribute CS4
☑	Adobe Dreamweaver CS4
☑	Adobe Encore CS4
☑	Adobe Fireworks CS4
☑	Adobe Flash CS4
☑	Adobe Illustrator CS4
☑	Adobe InDesign CS4
☑	Adobe OnLocation CS4

Action: Install

Language: English (United States)

Serial number: (required)

Other options:
☑ Suppress registration
☑ Suppress EULA
☑ Suppress updates
☑ Suppress process check
☑ Disable Adobe Product Improvement Program
☑ Don't show installer icon in dock

The pane contains these elements:

- **Use command line options for installation**: If you choose this option, you can specify the installer behavior by supplying command line options in the **Package** pane.
  If you choose this option, all other settings in the dialog are ignored.
- **Use the following settings for installation**: If you choose this option, you can check the components that you want to be installed by this package in the scrolling list. You can also set additional options through the other checkboxes and radio buttons.
  The exact content of the list depends on which Adobe CS installer you are using.
- **Action**: Displays whether this package installs or uninstalls software. (You made this choice when creating the payload.)
- **Language**: The desired user interface language for the installed software.
- **Serial number**: Enter the serial number for the package here.

Depending on the specific Adobe software you are installing the serial number is either optional or mandatory; this is indicated beside the field.
If you do not enter an optional serial number, the serial number will have to be entered individually for each installed copy when it is first launched.

- **Other options**: These settings let you disable various optional functions of the installer:
  - **Suppress registration** : If this option is checked, local users are not prompted to register their copy of Adobe CS.
  - **Suppress EULA**: If this option is checked, the license agreement is not displayed when Adobe CS is first started on the a target computer.
  - **Suppress updates**: If this option is checked, the installed copies of Adobe CS will not check Adobe's servers for available updates.
  - **Suppress process check**: If this option is checked, the installer does check for certain running applications.
    If the option is unchecked, the installer refuses to run on a target computer on which any of these applications is running.
  - **Disable Adobe Product Improvement Program**: If this option is checked, the Adobe Product Improvement Program (a tool that collects data and sends it to Adobe) is disabled.
  - **Don't show installer icon in dock**: If this option is checked, the Adobe CS installer does not show up in the dock of target macOS computers.

If the assigned payload contains an Adobe CS updater (instead of an installer), only some of the options in the dialog are available.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Distribution and Licensing Info" command (described on page 481).

New Metapackage

The **New Metapackage** command creates a new metapackage.

Choosing the command opens the **Metapackage** dialog. The dialog has four panes:

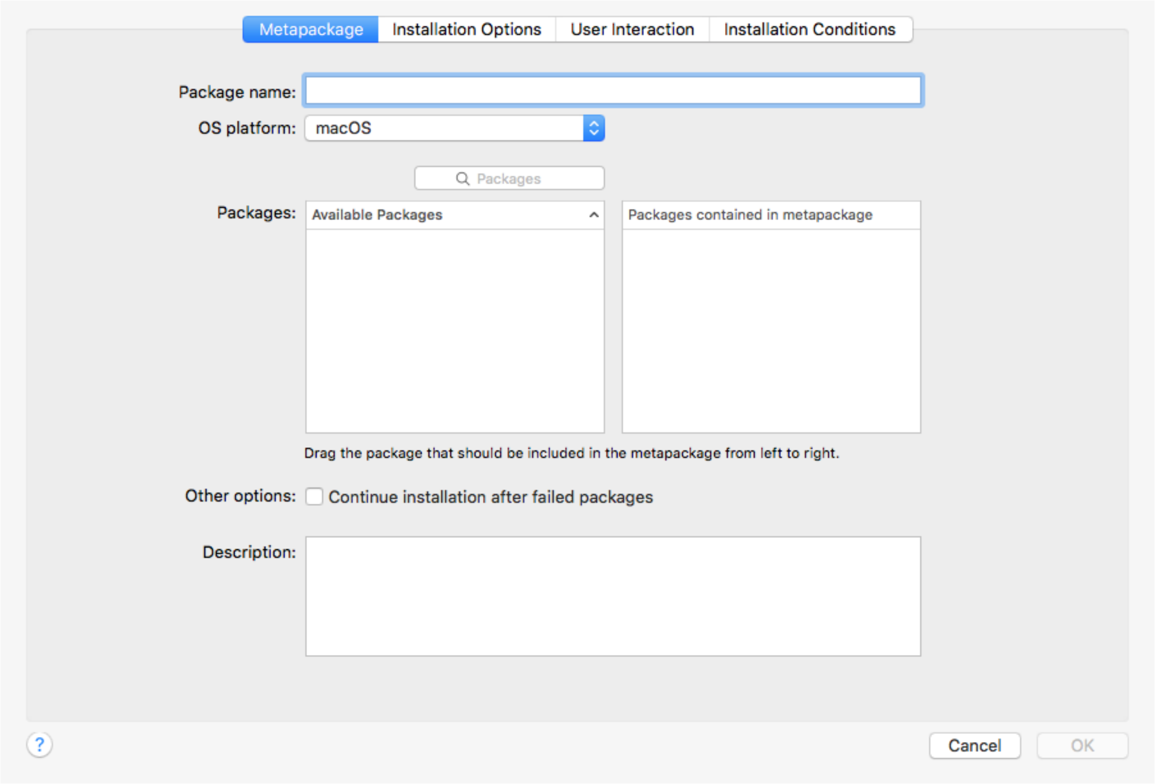
- **Metapackage**
- **Installation Options**
- **User Interaction**
- **Installation Conditions**

All four are described below.

NOTE The **New Metapackage** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 758 for details.

Metapackage

The **Package** pane of the **Metapackage** dialog lets you specify basic settings for the metapackage:


Metapackage
Installation Options
User Interaction
Installation Conditions
Package name:
OS platform: macOS
Packages
Packages:
Available Packages
Packages contained in metapackage
Drag the package that should be included in the metapackage from left to right.
Other options: □ Continue installation after failed packages
Description:
?
Cancel
OK

The pane contains these elements:

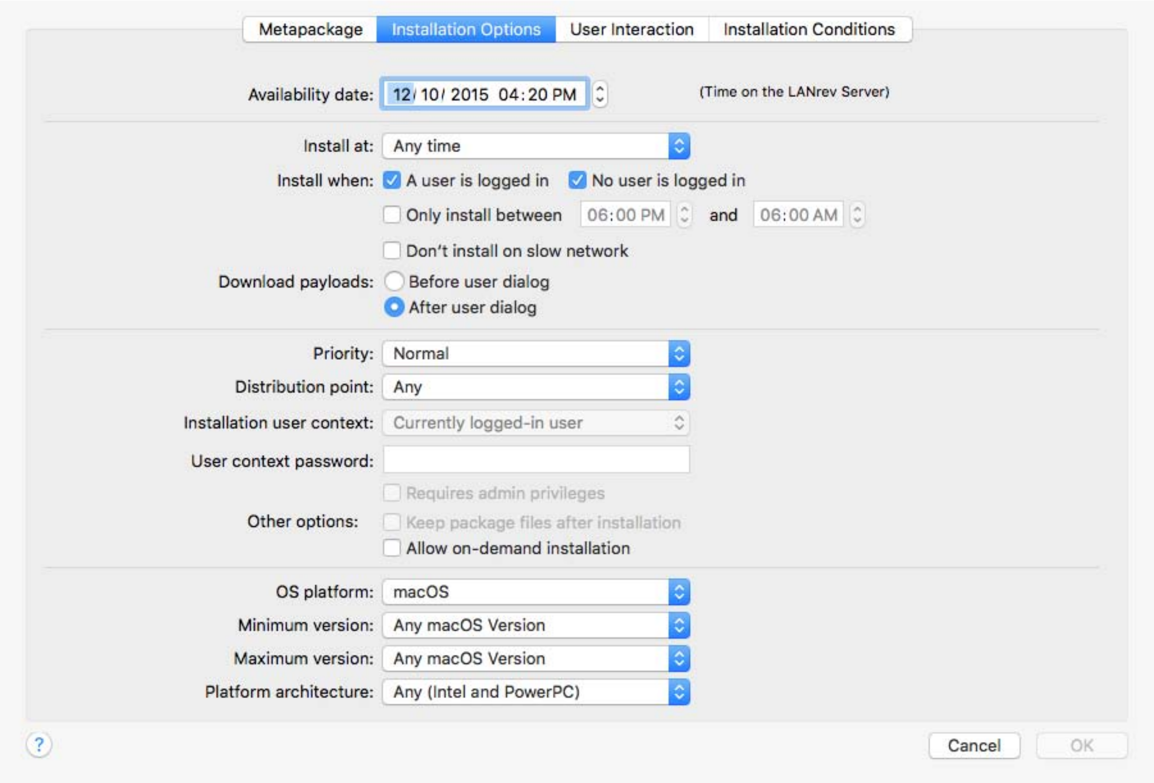
- **Package Name**: The name of the metapackage.
- **OS Platform**: The operating systems on which the metapackage may be installed. The chosen platform determines which packages are displayed in the pane.
- **Packages**: These two lists display the available packages and the packages contained in the metapackage.
  Dragging a package to the right list adds it to the package; dragging it back to the left list removes it. Dragging packages within the right lost changes their installation order: Packages are installed in the order listed, from top to bottom.
  Entering text in the filter field above the lists filters the list of available packages.
- **Continue installation after failed packages**: If this option is checked, LANrev will skip over any failed packages and install the rest of the packages in the metapackage. If the option is

unchecked, the installation of a metapackage is stopped when a package contained in it fails to install.

- **Description**: A description of the software contained in the metapackage. This text is displayed if the local user is asked for confirmation.

Installation Options

The **Installation Options** pane of the **Metapackage** dialog lets you specify various options for the installation of the package:



Availability date: 12/10/2015 04:20 PM (Time on the LANrev Server)

Install at: Any time

Install when: ☑ A user is logged in ☑ No user is logged in

□ Only install between 06:00 PM and 06:00 AM

□ Don't install on slow network

Download payloads: ○ Before user dialog ● After user dialog

Priority: Normal

Distribution point: Any

Installation user context: Currently logged-in user

User context password:

Other options: □ Requires admin privileges □ Keep package files after installation □ Allow on-demand installation

OS platform: macOS

Minimum version: Any macOS Version

Maximum version: Any macOS Version

Platform architecture: Any (Intel and PowerPC)

NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Availability date**: The earliest date when this metapackage may be used for software installations on administered computers.
- **Install at**: Whether to install the metapackage anytime or just on particular occasions.
- **Install when**: These options let you further specify conditions that must be met for the installation to proceed:
  - **A user is logged in**: If this option is checked, the metapackage will be installed when a user is logged in on the target computer.

  - **No user is logged in**: If this option is checked, the metapackage will be installed when no user is logged in on the target computer (and the computer is running).

  Note: Both these options can be checked at the same time, in which case the metapackage is installed irrespective of whether a user is logged in. It is not possible to uncheck both options. Note, too, that certain settings in the **User Interaction** *pane force the settings of these options, in which case they are disabled.*

  - **Only install between**: This option lets you restrict the installation of the metapackage to a certain period of the day, for example, after hours.
  - **Don’t install on slow network**: If this option is checked, installations take place only when the network connection between the client and the distribution point has a nominal transfer rate of at least 100 Mbit/s.

- **Download payloads**: This setting specifies when the Agent downloads a payload, before displaying a user dialog or after. Downloading the payload before displaying the dialog makes the installation feel more responsive to the user. Downloading the payload after the dialog avoids unnecessary downloads when the user cancels the installation.

  The setting has no effect when there is no user interaction during the installation.
- **Priority**: The priority of this metapackage. When more than one metapackage or standard package is available for installation on a client, packages with higher priorities are installed first.
- **Distribution point**: An optional restriction on the distribution point from which the installer is transferred to the client:
  - **Any**: No restriction.
  - **From assigned distribution point if available**: When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, another distribution point is used.
  - **From assigned distribution point only**: When an assigned distribution point (see below) is available, that distribution point is used. When no assigned distribution point is available, the installation fails.

  An assigned distribution point is a distribution point that either includes the agent’s IP address in the range of IP addresses it is set to serve (see “New Distribution Point” on page 725 for details) or that has been assigned to a computer group of which the target computer is a member.

  If no IP range has been specified in a distribution point definition, it is considered to be assigned to all clients in the same subnet. (The server’s subnet mask is used to determine the extent of the subnet.)

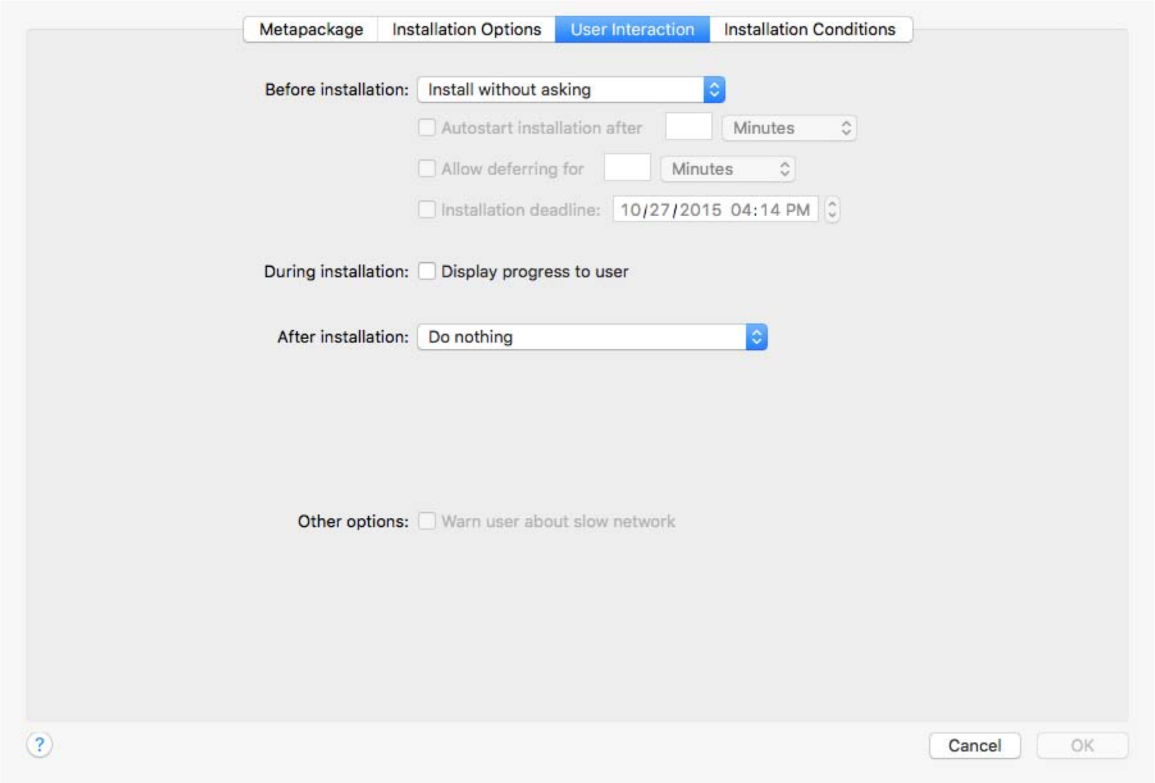
  Note that a distribution point with the **Only use when assigned to group or via IP range** setting active will never serve packages to clients to which it has not been assigned, irrespective of the distribution point setting in the package.
- **Installation user context**: This option is not available for metapackages; all packages are installed with their individual user contexts.

- **User context password**: This option is not available for metapackages; all packages are installed with their individual user passwords (if any).
- **Requires admin privileges**: This option is not available for metapackages; all packages are installed with their individual settings.
- **Other options**: Miscellaneous settings.
  - **Keep package files after installation**: This option is not available for metapackages; all packages are installed with their individual settings.
- **OS Platform**: The operating systems on which the metapackage may be installed.
- **Minimum OS**: The lowest version of the operating system on which the metapackage may be installed.
- **Maximum OS**: The highest version of the operating system on which the metapackage may be installed.
- **Platform architecture**: This option lets you restrict the installation to only Intel or PowerPC-based computers under macOS. Under Windows, you can restrict installations to 32-bit or 64-bit versions of the OS.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

User Interaction

The **User Interaction** pane of the **Metapackage** dialog lets you specify the information users are given during the installation process and the actions they can perform:



Before installation: Install without asking

□ Autostart installation after Minutes

□ Allow deferring for Minutes

□ Installation deadline: 10/27/2015 04:14 PM

During installation: □ Display progress to user

After installation: Do nothing

Other options: □ Warn user about slow network

NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Before installation**: The way in which the user may influence the installation:
    - **Install without asking**: The user is not informed of the installation.
    - **Inform user before installation**: The user is informed of the installation before the fact but cannot affect it.
    - **Allow to reschedule**: The user can postpone the installation but not disallow it altogether.
    - **Allow to refuse**: The user may altogether refuse to have this metapackage installed on his or her computer.
- **Autostart installation after**: This option is only active when a **Before installation** option other than **Install without asking** is chosen. It lets you specify a time after which the installation starts automatically when the user does not respond to the installation notification.
- **Allow deferring for**: This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the maximum time for which users can postpone the installation.

- **Installation deadline**: This option is only active when **Allow to reschedule** or **Allow to refuse** has been chosen as the **Before installation** option. It lets you specify the latest time when the installation must begin.

NOTE When you specify both a maximum deferring interval and an installation deadline, both are active. This means that the earlier of the two resulting dates becomes effective: If the deadline is reached, the installation is forced (unless the user has canceled it altogether), even if the interval has not yet expired. And if the interval expires, the installation begins even if the deadline has not yet been reached.

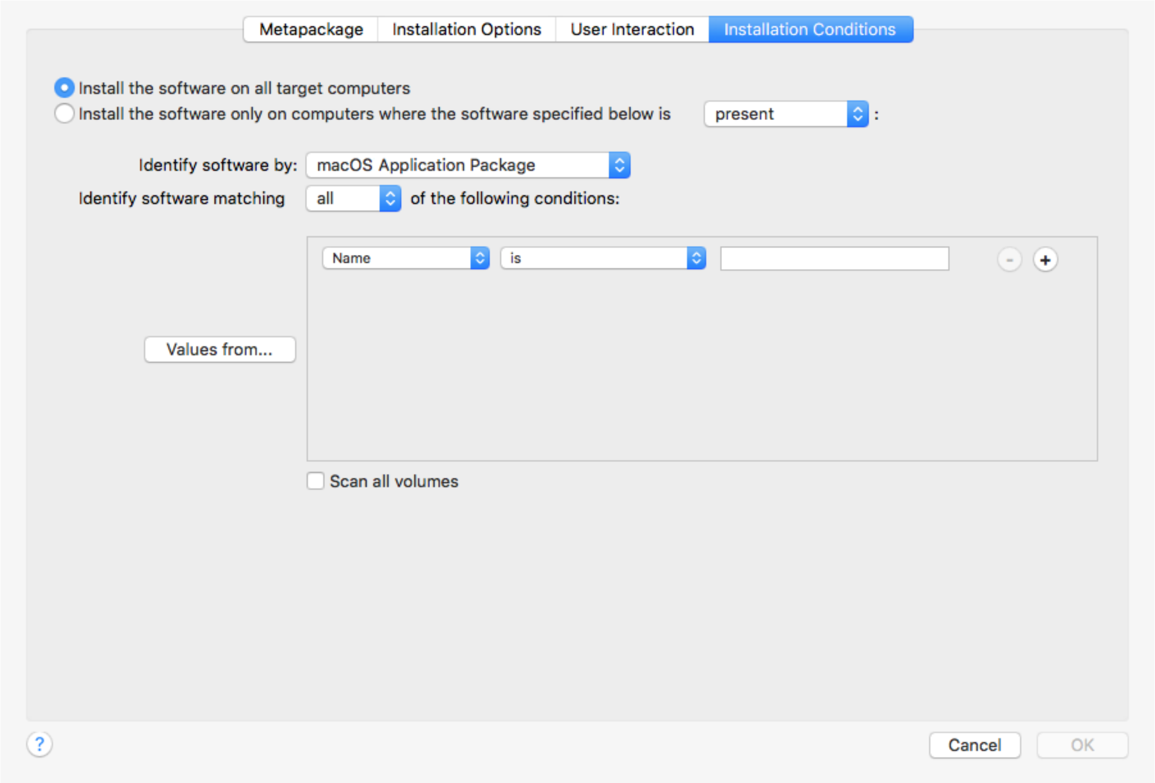
- **Display progress bar to the user**: If this option is checked, the users of the target computers are informed of the installation progress by a progress bar. If the option is unchecked, there is no feedback on the progress.
- **After installation**: The action that LANrev Agent performs on the target computer after the installation is complete:
  - **Do nothing**: No action is performed.
  - **Notify user**: A message informing the user of the completed installation is displayed.
    An additional option becomes available:
    - **Automatically close notification after**: This option lets you specify a time after which LANrev Agent automatically closes the notification alert.
  - **Restart**: The computer is automatically restarted without a notification displayed first. Processes are sent termination messages, allowing data in open documents to be saved first.
    Additional options become available:
    - **Show notification**: Checking this option causes LANrev Agent to display a notification of the pending restart. The restart happens after the user has responded to the notification.
    - **Restart after no more than**: This option is available only when **Show notification** has been checked. It lets you set an interval after which the restart is performed even when the user does not respond to the notification.
    - **Allow user to postpone restart**: This option is available only when **Show notification** has been checked. It lets you give the user the option to defer the restart to a later date.
    - **Show dialog again every**: This option is available only when **Allow user to postpone restart** has been checked. It lets you make LANrev display the restart notification dialog at regular intervals, reminding the user that a restart is still required. If an interval has been specified in the **Restart after no more than** option (see above), it applies to these reminders as well.
  - **Force restart**: As **Restart**, above, but processes are forcibly terminated. All unsaved data is irrecoverably lost. The same options as for **Restart** become available.

- **Warn about slow network**: If this option is checked, the user of a target computer is warned before installations when the network connection between the client and the distribution point has a nominal transfer rate of less than 100 Mbit/s. The warning is not displayed if the metapackage is set to install without asking the user.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Distribution and Licensing Info" command (described on page 481).

Installation Conditions

The **Installation Conditions** pane of the **Metapackage** dialog lets you specify that a metapackage be installed only on client computers that meet certain criteria:



● Install the software on all target computers
○ Install the software only on computers where the software specified below is: present

Identify software by: macOS Application Package

Identify software matching: all of the following conditions:

Name | is |

□ Scan all volumes

NOTE The installation options specified in this pane override any conflicting options of the packages contained in the metapackages.

The pane contains these elements:

- **Install the software on all target computers**: The metapackage will be installed on all computers in the computer groups to which it is assigned.
- **Install the software only on computers where the software specified below is**: Choose whether the metapackage is to be installed only on computers that already have certain software

(choose **present**) or on computers that lack specified software (choose **not present**).

The rest of the elements are similar to the corresponding ones in the **Software License Specification** dialog discussed on page 732.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Distribution and Licensing Info" command (described on page 481).

Duplicate Software Package

The **Duplicate Software Package** command lets you create a new software distribution package or metapackage based on an existing one.

Depending on which type of package is selected, choosing the command opens the **Software Distribution Package** dialog that is described in "New Software Package" on page 700 or the Metapackage dialog described in "New Metapackage" on page 710, with the selected package's settings displayed. If you click **OK** in that dialog, a new package is created.

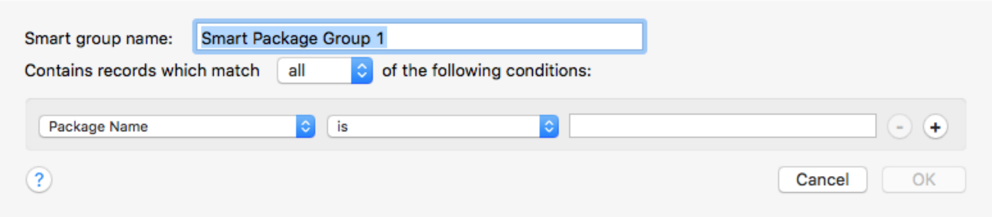
NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Distribution and Licensing Info" command (described on page 481).

NOTE The **Duplicate Software Package** command can be used only by administrators with the **Modify Software Packages** right. See "New Administrator" on page 758 for details.

New Smart Software Package Group

The **New Smart Software Package Group** command creates a new smart group for software packages and metapackages.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Package Group 1

Contains records which match all of the following conditions:

Package Name is

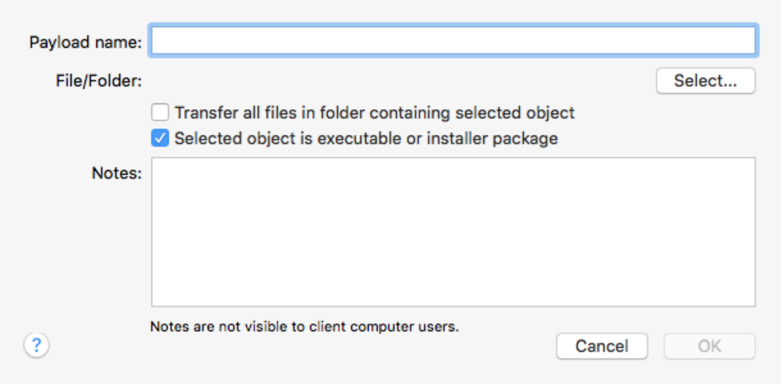
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand text pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Packages** subcategory of the **Software Distribution** category (see page 878).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Payload

The **New Payload** command lets you create a new payload specification for use in software distribution packages.

Choosing the command opens the **Payload** dialog:


Payload name:

File/Folder:

□ Transfer all files in folder containing selected object

☑ Selected object is executable or installer package

Notes:

Notes are not visible to client computer users.

The dialog contains these elements:

- **Payload name**: The name by which the payload is displayed in LANrev. You can enter any name desired.
- **File/Folder**: The file or folder that forms this payload. Clicking the **Select** button lets you select a file or folder.
- **Transfer all files in folder containing selected object**: If this option is checked, all files that are located in the same folder as the payload file are transferred as part of this payload. If the option is unchecked, only the file itself is transferred.
- **Selected object is executable or installer package**: If this option is checked, this payload is considered executable by LANrev. Each software distribution package must contain exactly one executable payload.

- **Notes**: Here you can enter explanations and remarks for yourself or other administrators. The text in this field is not visible to users of client computers.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 392.

NOTE The **New Payload** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 758 for details.

Duplicate Payload

The **Duplicate Payload** command lets you create a new payload based on an existing one.

Choosing the command opens the **Payload** dialog that is described in “New Payload” on page 719. If you click **OK** in that dialog, a new package is created.

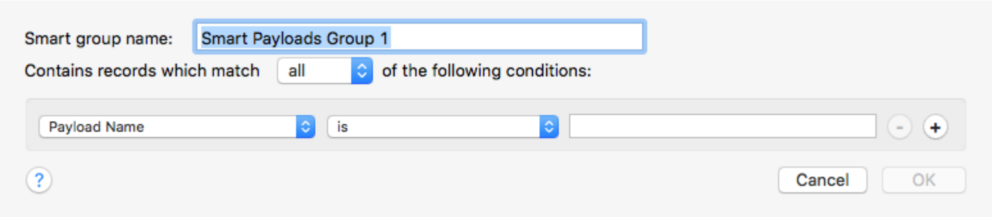
NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **Duplicate Payload** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 758 for details.

New Smart Payload Group

The **New Smart Payload Group** command creates a new smart group for payloads.

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart Payloads Group 1

Contains records which match all of the following conditions:

Payload Name is

The dialog contains these elements:

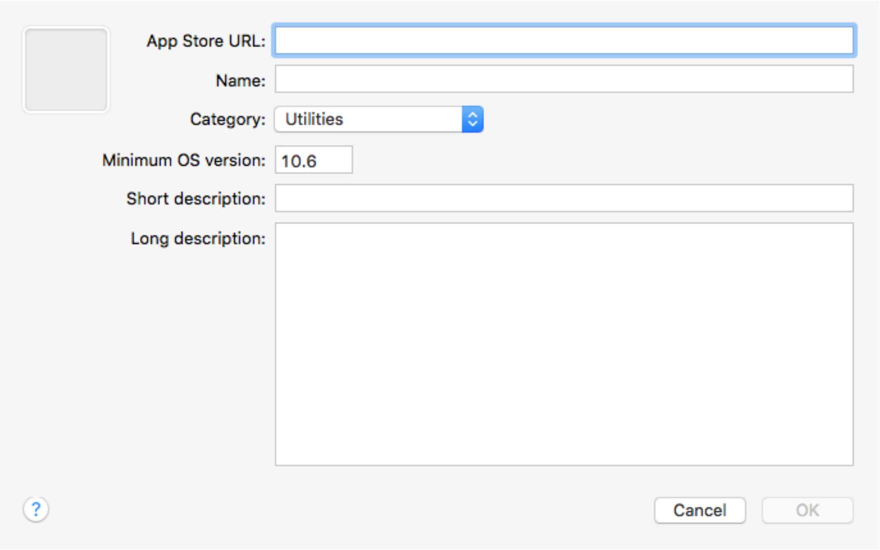
- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified

conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).

- Conditions area:
  - The left-hand text pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Packages** subcategory of the **Software Distribution** category (see page 878).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Mac App Store Application Package

This command opens the **Mac App Store Application** dialog in which you can specify a new application package for an application from the Mac App Store.


App Store URL:
Name:
Category: Utilities
Minimum OS version: 10.6
Short description:
Long description:

The dialog contains these elements:

- The field for the icon at the top left. This field is filled automatically when the app store URL is specified but you can paste in a custom graphic.
- **App Store URL**: The URL of the Mac App Store page for this application.
  You can obtain the URL by choosing **Copy Link** from the small menu to the right of the price tag in the applications listing. Entering the URL and leaving this field fills in some of the other fields with information downloaded from the App Store.
- **Name**: The name for the package.
- **Category**: The App Store category to which the app belongs.

- **Minimum OS version**: The minimum version of macOS required to run this application.
- **Short description**: A brief description of the application.
- **Long description**: A more extensive description of the application.

New Smart Mac App Store Application Group

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for Mac App Store application packages defined in LANrev.

For details, see "New Smart Group" on page 522.

Duplicate Application Package

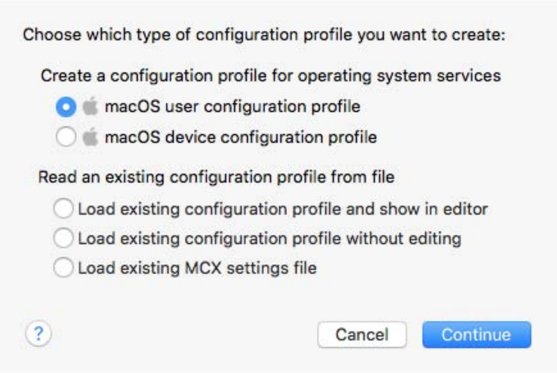
The **Duplicate Application Package** command lets you create a new app store application package based on an existing one.

Choosing the command opens the **Mac App Store Application** dialog that is described in "New Mac App Store Application Package" on page 721. If you click **OK** in that dialog, a new package is created.

NOTE The **Duplicate Application Package** command can be used only by administrators with the **Modify Software Packages** right. See "New Administrator" on page 758 for details.

New Configuration Profile

This command opens the **Configuration Profile Type** dialog, in which you can choose the type of configuration you want to create.



Choose which type of configuration profile you want to create:

Create a configuration profile for operating system services

● macOS user configuration profile

○ macOS device configuration profile

Read an existing configuration profile from file

○ Load existing configuration profile and show in editor

○ Load existing configuration profile without editing

○ Load existing MCX settings file

Depending on which option you choose, clicking **OK** has different effects:

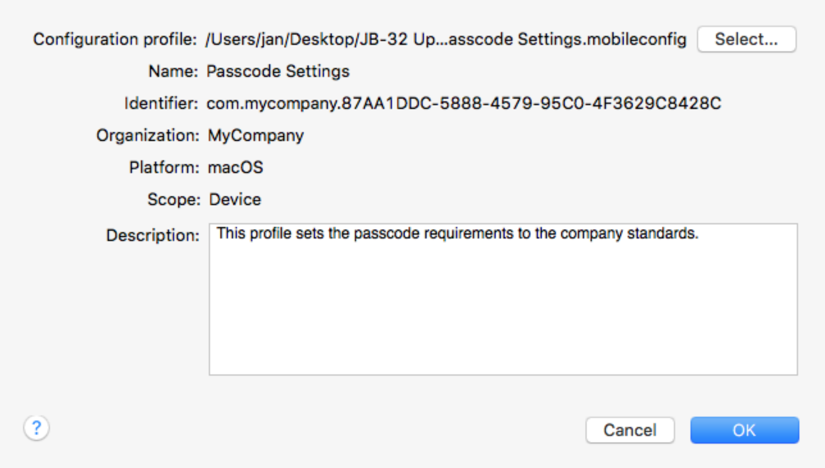
- **macOS user configuration profile**: The profile editor is opened with the settings for a macOS user configuration

profile displayed. Choosing **macOS device configuration profile** has a similar effect, but in this case the settings for a device profile are displayed.
For more information on the profile editor, see “Configuration profile editor” on page 666.

- **Load existing configuration profile and show in editor**: You can choose a configuration profile file from disk and open it in the profile editor.
- **Load existing configuration profile without editing**: You can choose a configuration profile file from disk and import it into LANrev without editing it.
The profile is displayed in the **Configuration Profile** dialog (see below).
- **Load existing MCX settings file**: You can choose an MCX settings file from disk and import it into LANrev without editing it.
The file is displayed in the **Configuration Profile** dialog (see below).

Configuration Profile dialog for profiles

The **Configuration Profile** dialog lets you import an existing configuration profile from disk into LANrev that can then be distributed to administered computers.



Configuration profile: /Users/jan/Desktop/JB-32 Up...asscode Settings.mobileconfig
Name: Passcode Settings
Identifier: com.mycompany.87AA1DDC-5888-4579-95C0-4F3629C8428C
Organization: MyCompany
Platform: macOS
Scope: Device
Description: This profile sets the passcode requirements to the company standards.

The dialog contains these elements:

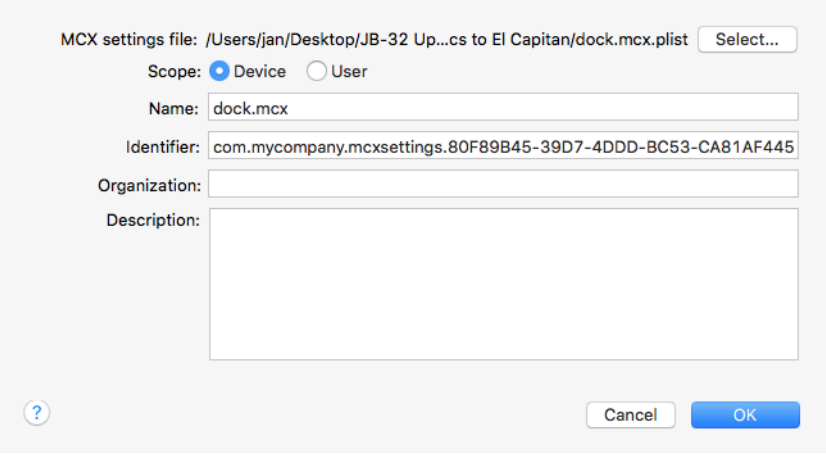
- **Configuration profile**: The file containing the configuration profile. Clicking the **Select** button lets you select the file on your computer.
- **Name**: The name of the profile. The name is automatically read from the profile and cannot be changed in this dialog.
- **Identifier**: The identifier of the profile. The identifier is automatically read from the profile and cannot be changed in this dialog.
- **Organization**: The organization which issued the profile. The identifier is automatically read from the profile and cannot be changed in this dialog.

- **Platform**: The operating system to which the profile applies. The type is automatically detected and cannot be changed in this dialog.
- **Scope**: The kind of profile – user or device profile.
- **Description**: A description of the profile. This description is displayed to the user of the managed computer.

Clicking **OK** imports the profile into the **Configuration Profiles** section of the **Server Center** window.

Configuration Profile dialog for MCX settings files

The **Configuration Profile** dialog lets you import an existing MCX settings file from disk into LANrev that can then be distributed to administered macOS computers.



MCX settings file: /Users/jan/Desktop/JB-32 Up...cs to El Capitan/dock.mcx.plist

Scope: ● Device ○ User

Name: dock.mcx

Identifier: com.mycompany.mcxsettings.80F89B45-39D7-4DDD-BC53-CA81AF445

Organization:

Description:

The dialog contains these elements:

- **MCX settings file**: The file containing the MCX settings. Clicking the **Select** button lets you select the file on your computer.
- **Scope**: Whether the settings are applied to a device or a user account.
- **Name**: The name of the settings. The name is automatically read from the file and can be changed in this dialog.
- **Identifier**: The identifier of the settings. The identifier is automatically read from the file and can be changed in this dialog.
- **Organization**: The organization which issued the settings.
- **Description**: A description of the settings. This description is displayed to the user of the managed computer.

Clicking **OK** imports the profile into the **Configuration Profiles** section of the **Server Center** window.

New Smart Configuration Profile Group

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group for computer configuration profiles defined in LANrev.

For details, see “New Smart Group” on page 522.

New Device Enrollment Profile

This command lets you create a new device enrollment profile. Choosing the command opens the **Device Enrollment Profile Editor** dialog, described in “New Smart Group: Enrollment Profiles” on page 603.

New Smart Enrollment Profile Group

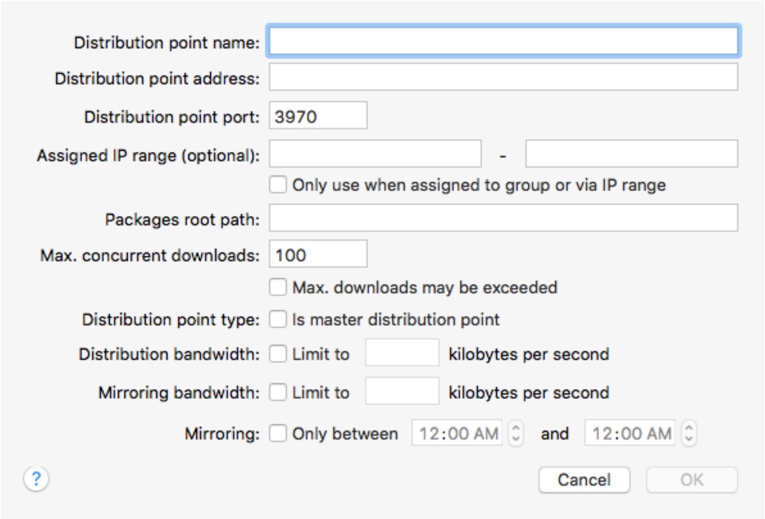
This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that includes all device enrollment profiles meeting the specified criteria.

For details on the **Smart Group** dialog, see “New Smart Group” on page 522.

New Distribution Point

The **New Distribution Point** command creates a new distribution point on which software installers are stored.

Choosing the command opens the **Distribution Point** dialog:



Distribution point name:
Distribution point address:
Distribution point port: 3970
Assigned IP range (optional): -
□ Only use when assigned to group or via IP range
Packages root path:
Max. concurrent downloads: 100
□ Max. downloads may be exceeded
Distribution point type: □ Is master distribution point
Distribution bandwidth: □ Limit to kilobytes per second
Mirroring bandwidth: □ Limit to kilobytes per second
Mirroring: □ Only between 12:00 AM and 12:00 AM

The dialog contains these elements:

- **Distribution point name**: The name by which the distribution point is to be known inside LANrev.
- **Distribution point address**: The distribution point's IP address or DNS name.
  Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain), if you enter a DNS name.
- **Distribution point port**: The port on which the LANrev agent installed on the distribution point communicates.
- **Assigned IP range (optional)**: These fields can be used to assign the distribution point to computers within a particular IP range. The lower limit of the range must be specified in the left-hand field, the upper limit in the right-hand field.
  This setting is used when a package is set to be provided from assigned distribution points, as described in **Distribution Point** in "Installation Options" on page 702.
- **Only use when assigned to group or via IP range**: Checking this option causes the distribution point to serve only client computers to which it has been expressly assigned in one of two ways:
  - Because the computers' IP addresses lie in the specified range
  - Because the distribution point has been assigned to a computer group to which the computers belong

  If this option is off, the distribution point may also serve packages to clients to which it has not been assigned, if the distribution point setting in the packages' specifications is "Any" or "From assigned distribution point if available" and no assigned distribution point is available for the client.
- **Packages root path**: The path on the distribution point of the folder in which LANrev is to store the software installers.
- **Max. concurrent downloads**: The number of download processes that may be under way at the same time.
- **Max. downloads may be exceeded**: This option governs the distribution point's behavior when all available distribution points are operating at capacity and an additional agent request for an installer download comes in:
  - If the option is checked, the installer is provided to the agent even though the specified maximum number of downloads is already in progress, because no other distribution point has available capacity.
  - If the option is unchecked, the agent's request is turned down and the agent must repeat it later.
- **Is master distribution point**: If this option is checked, the distribution point is the master distribution point from which all other distribution points receive their software installers. If it is unchecked, the distribution point is a mirror that receives its installers from the master.
  There must always be exactly one master distribution point.

- **Distribution bandwidth**: This option lets you limit the network bandwidth employed for providing installers to agents.
- **Mirroring bandwidth**: This option lets you limit the network bandwidth employed for mirroring installers between distribution points.
  You cannot limit the mirroring bandwidth for the master distribution point.
- **Only between**: This option lets you restrict mirroring of installers to or from this distribution point to a certain time of the day. Outside of the specified interval, no mirroring involving this distribution point happens.
  You cannot limit the mirroring period for the master distribution point.

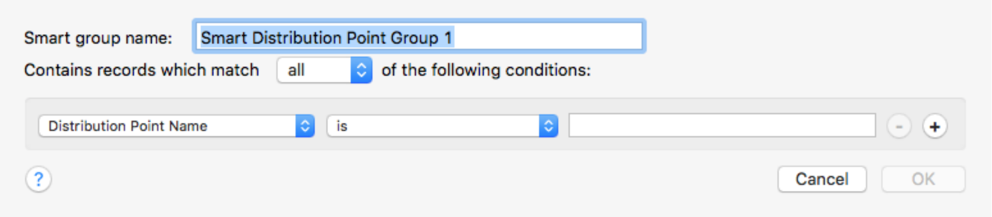
NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **New Distribution Point** command can be used only by administrators with the **Modify Distribution Points** right. See “New Administrator” on page 758 for details.

New Smart Distribution Point Group

The **New Smart Distribution Point Group** command creates a new smart group for distribution points.

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart Distribution Point Group 1
Contains records which match all of the following conditions:
Distribution Point Name · is

The dialog contains these elements:

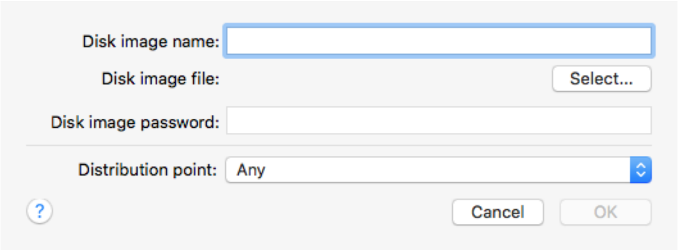
- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand text field lets you enter an information item on which records are to be matched. You can use any information item from the **Distribution Points** subcategory of the **Software Distribution** category (see page 883).

- The pop-up menu contains the possible comparison operators.
- The right-hand text field lets you specify the value to compare record values against.
- The **+** and **–** buttons let you add new conditions or remove existing ones.

New Disk Image

The **New Disk Image** command creates a new disk image specification for reinstalling client computers.

Choosing the command opens the **Disk Image** dialog:



The dialog contains these elements:

- **Disk image name**: The name that you want to give the disk image specification for purposes of identifying it within LANrev.
- **Disk image file**: The file that contains the disk image. LANrev supports Apple’s .dmg format as well as any other disk image that can be mounted without additional software on the target computer, such ISO images (.iso) and Active Disk Image images (.adi).
- **Disk image password**: If the specified disk image is password-protected, enter the password here.
- **Distribution point**: This option specifies from which distribution points the target computer may download the image:
  - **Any**: The image can be downloaded from any distribution point on which it is found.
  - **From assigned distribution point if available**: The image is downloaded from a distribution point that is assigned to the target computer’s subnet or to its computer group. If the image is not available on any such distribution point, it is downloaded from another distribution point.

- **From assigned distribution point only**: As above, but if the image is not available, the installation fails.

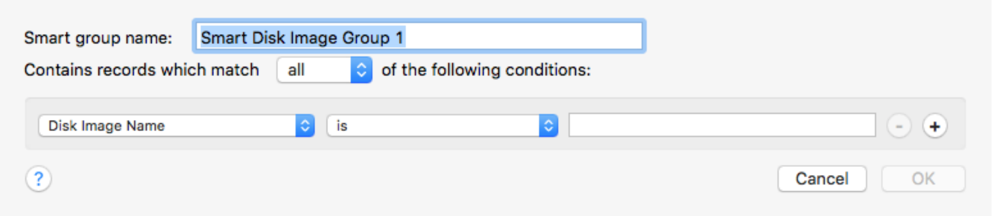
NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **New Disk Image** command can be used only by administrators with the **Modify Disk Images** right. See “New Administrator” on page 758 for details.

New Smart Disk Image Group

The **New Smart Disk Image Group** command creates a new smart group for disk image specifications.

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart Disk Image Group 1

Contains records which match all of the following conditions:

Disk Image Name is

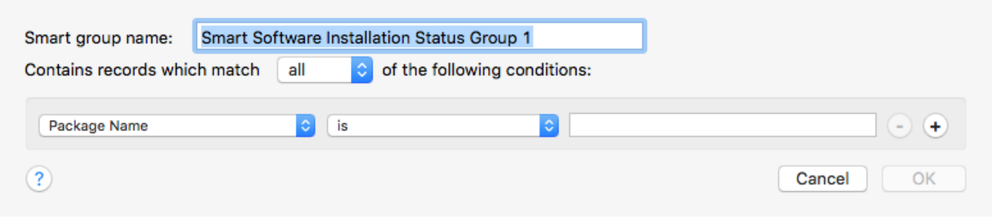
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Disk Images** subcategory of the **Software Distribution** category (see page 884).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Smart Software Installation Status Group

The **New Smart Software Installation Status Group** command creates a new smart group for software installations according to their status.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Software Installation Status Group 1

Contains records which match all of the following conditions:

Package Name is

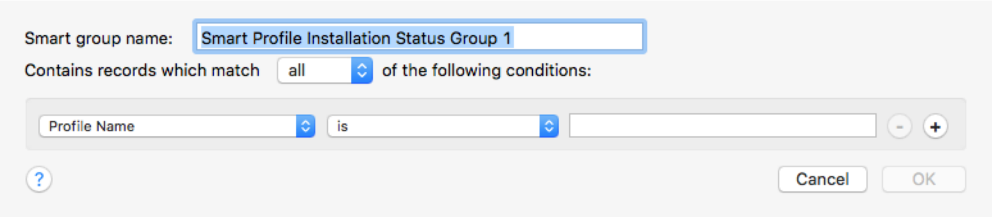
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Installation Status** subcategory of the **Software Distribution** category (see page 884).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Smart Profile Installation Status Group

The **New Smart Profile Installation Status Group** command creates a new smart group for profile installations according to their status.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Profile Installation Status Group 1

Contains records which match all of the following conditions:

Profile Name is

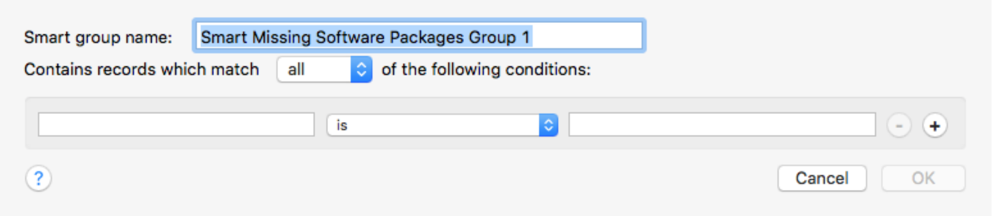
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Configuration Profile Installation Status** subcategory of the **Software Distribution** category (see page 884) as well as the **Agent Name** and **Profile Name** information items (see page 831 and page 882, respectively).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Missing Software Packages Group

The **New Missing Software Packages Group** command creates a new smart group that lists all software packages which are assigned to computers but not installed on them.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Missing Software Packages Group 1

Contains records which match all of the following conditions:

is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. You can use any information item from the **Installation Status** subcategory of the **Software Distribution** category (see page 884).
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.

- The **+** and **–** buttons let you add new conditions or remove existing ones.

License Monitoring

The **License Monitoring** submenu contains commands for managing software distribution functions:

- **New License Specification** (page 732)
- **New Smart License Specification Group** (page 738)
- **New License Status Report** (page 738)
- **New Software Usage Report** (page 739)
- **New History Report** (page 739)
- **New History Summary Report** (page 740)
- **New Missing Software Report** (page 740)

New License Specification

The **New License Specification** command creates a new license specification.

Choosing the command opens the **Software License Specification** dialog, which has two panes:

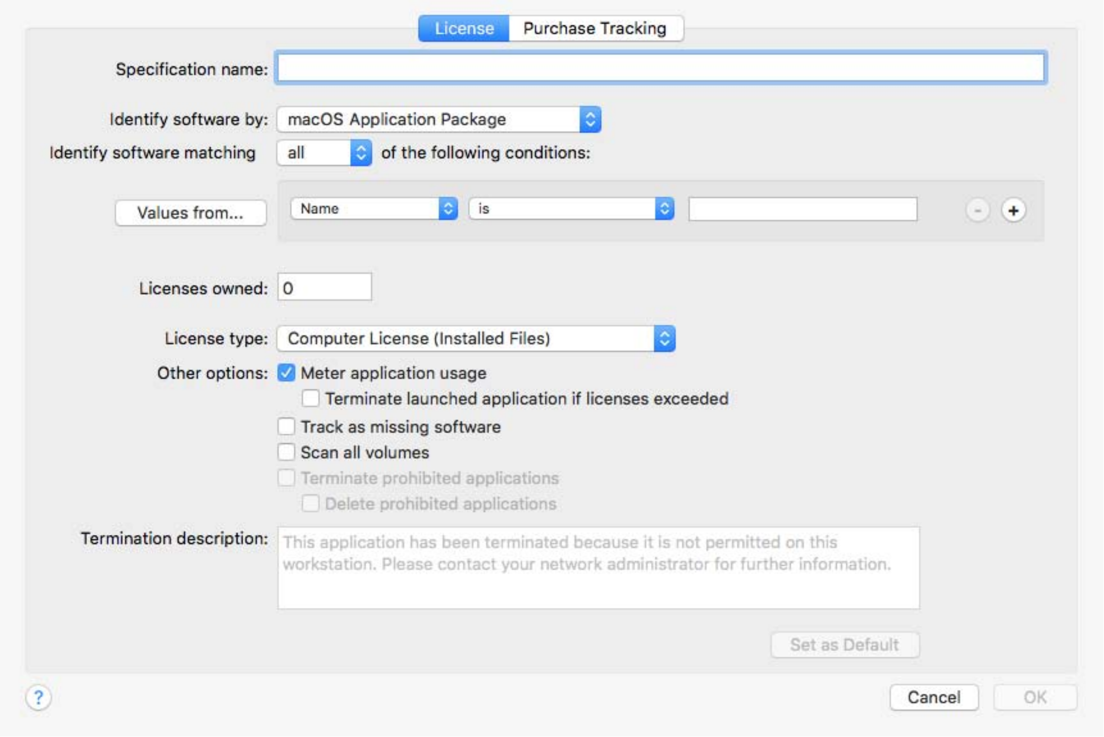
- **License**
- **Purchase Tracking**

Both are described below.

NOTE The **New License Specification** command can be used only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 758 for details.

License

The **License** pane of the **Software License Specification** dialog lets you enter the details of the software license:



Specification name:

Identify software by: macOS Application Package

Identify software matching all of the following conditions:

Name | is

Licenses owned: 0

License type: Computer License (Installed Files)

Other options:
☑ Meter application usage
□ Terminate launched application if licenses exceeded
□ Track as missing software
□ Scan all volumes
□ Terminate prohibited applications
□ Delete prohibited applications

Termination description: This application has been terminated because it is not permitted on this workstation. Please contact your network administrator for further information.

The pane contains these elements:

- **Specification Name**: The name of the license specification.
- **Identify software by**: How the software is to be identified that is described by this license:
  - **macOS Application Package**: a macOS package (a folder appearing as a file).
  - **macOS Application File**: a macOS file. Files are only considered to match if they are executable applications.
  - **macOS File**: a macOS file.
  - **macOS Installer Receipt**: a description of the installed software in the form of an installer package that some macOS installers create.
  - **Windows Application File**: a Window file. Files are only considered to match if they are executable applications.
  - **Windows File**: a Windows file.
  - **Windows Installer Receipt**: a report on the installed software created by MSI installers.
  - **Windows Installed Software**: software installed on the administered computer.
  - **Windows Registry**: specified contents of the Windows registry.
- **Identify software matching**: When **all** is chosen from this pop-up menu, software is found that matches all specified conditions (Boolean AND). If **any** is chosen, software is found that matches at least one of the specified conditions (Boolean OR).

- **Values from**: Clicking this button lets you select a file. All specified conditions are filled with the corresponding parameters from this file. If you later add new conditions, they initially also contain comparison values from this file.
- Condition area: The first pop-up menu lets you choose a condition to match software. The second one contains the possible comparison operators. For most conditions, a text field lets you specify the value to compare files against. The **+** and **–** buttons let you add new conditions or remove existing ones.
  The parameters available for specifying conditions are described in “Files” on page 867, except for **Path** and the conditions available when **Windows Registry** is selected as the software type. These additional conditions are described in “Conditions” on page 735.
  - **Path**: Lets you select files and folders by their paths on the hard disk. It references the **File Path** information item. When this option is chosen, you can specify the user folder on macOS targets and its subfolders using the ~/ notation. (For example, ~/Documents for the user’s documents folder.)
    For Windows targets, you can use the environment variables when this option is chosen, as described in “Environment variables” on page 176.
  - **Original File Name**: The original file name of a Windows file, as displayed in its properties in the Windows Explorer.
  - **Internal Name**: The internal name of a Windows file, as displayed in its properties in the Windows Explorer.

  Note: When you specify a license by Windows registry data, you should use the **Key Name** *and* **Value Name** *conditions only when there is no other way to specify the desired software. Checking either condition requires the entire registry to be parsed, which generates significant local processor load on the client computer. If you do require either condition, specify it after any other conditions that may apply because that causes LANrev to apply it only to the part of the registry that meets those other conditions.*
  Note: When specifying a file version, make sure to use the right format (three numbers for macOS files, four for Windows files), as described in “Gathering information on files” on page 102.
- **Licenses owned**: The number of licenses that are available for use.
  You can either enter these licenses manually or have LANrev calculate them automatically as the sum of your license purchases. In the latter case, you must create purchase records in the dialog’s **Purchase Tracking** pane for all licenses you have purchased of this software.
- **License type**:
  - **Computer License (Installed Files):** The license governs how many copies of the software may be installed in your network.
  - **Floating License (Running Processes):** The license governs how many copies of the software may be in use at the same time.

  - **Site License:** This type indicates software that may be used without restriction throughout your network. Choose it when you want to use the license specification for monitoring purposes.
  - **Prohibited Application**: Using this software is not allowed in your network. (This is not really a license type but allows you to check for the presence of undesirable software.)
- **Meter application usage**: If this option is checked, the running processes on the client computers are checked for the licensed software.
  Note: Only applications on administered computers that have a working network connection to the server are included in the count.
  Note: The computers' hard disks are always checked for installed packages, whether this option is activated or not.
  - **Terminate launched application if licenses exceeded**: If a user launches the specified application and all licenses are already in use, LANrev immediately terminates the application again, displaying the message from the **Termination description** field (see below) on the administered computer.
- **Track as missing software**: LANrev lists this software as missing when it is not installed on a client computer.
- **Scan all volumes**: If this option is checked, all local volumes of administered computers are scanned for this software. If it is unchecked, only boot volumes are scanned.
- **Terminate prohibited applications**: If this option is checked, LANrev automatically terminates any found applications that you have assigned the **Prohibited Application** license type. LANrev displays the message from the **Termination description** field (see below) on the administered computer This option is available only for macOS application packages and files and Windows application files. It requires that the **Meter application usage** option is also checked.
  - **Delete prohibited applications**: If this option is checked, the prohibited application is deleted from the client computer in addition to being terminated.
- **Termination description**: This is the message displayed on client computers when LANrev terminates an application because licenses are exceeded or the application is prohibited. To insert a line break, type Option-Enter.
  Clicking the **Set as Default** button makes the current text in the field the default for any licenses you create from now on.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

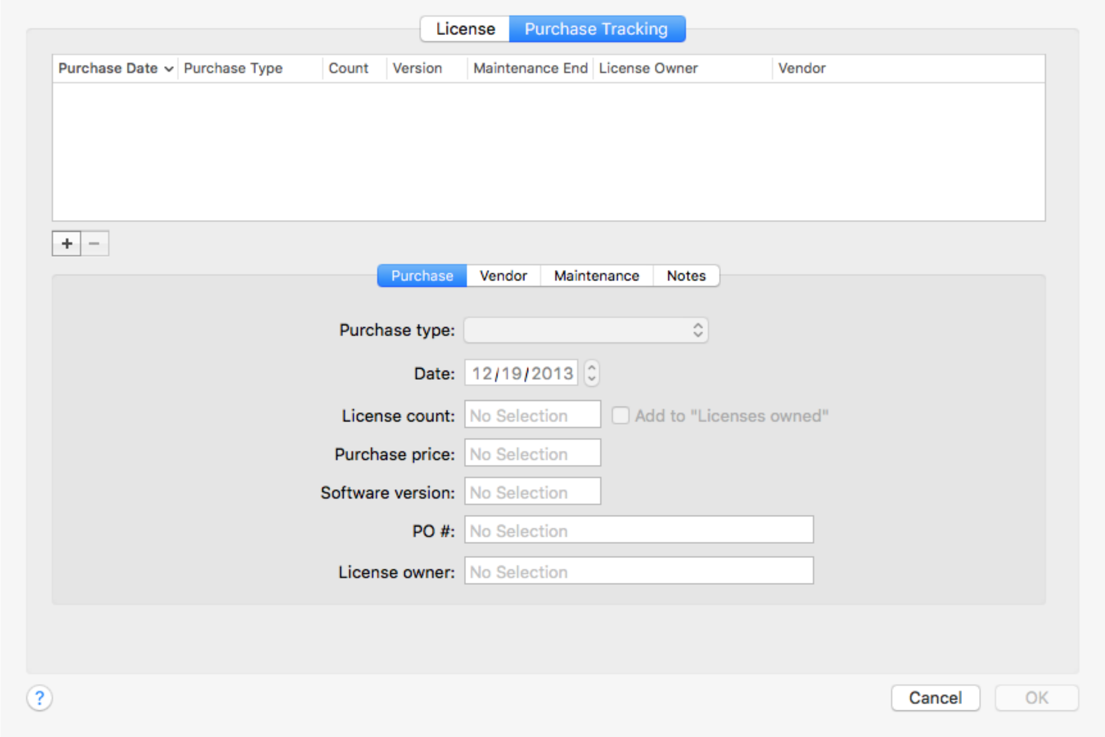
Conditions

Most of the conditions available for specifying how to determine the presence of licensed software are information items that are described in “Files” on page 867. There are, however, some additional conditions:

- **Path** lets you select files and folders by their paths on the hard disk. It references the **File Path** information item.
- **Path of Key** is the path of a key in the Windows registry.
- **Path of Value** is the path of a value in the Windows registry.
- **String at Path** is the value at the supplied path, interpreted as a string.
- **Number at Path** is the value at the supplied path, interpreted as a number.
- **Key Name** is a key with the specified name anywhere in the registry.
- **Value Name** is a value with the specified name anywhere in the registry.
  Note: Searching for either **Key Name** *or* **Value Name** *creates significant processor loads on the clients. Use these options only when there is no other way to identify the presence of the software.*

Purchase Tracking

The **Purchase Tracking** pane of the **Software License Specification** dialog lets you view, create, and maintain records of any purchases and maintenance contracts associated with the specified license:



Purchase Date	Purchase Type	Count	Version	Maintenance End	License Owner	Vendor

Purchase type:

Date: 12/19/2013

License count: No Selection □ Add to "Licenses owned"

Purchase price: No Selection

Software version: No Selection

PO #: No Selection

License owner: No Selection

The pane contains a list of recorded purchases in the upper half and four subpanes – described below – that display full information on the selected purchase.

The **+** button lets you add a new purchase. When a single existing purchase is selected, holding down the Option key while clicking the button duplicates the purchase. The **–** button lets you delete the selected purchase from the list.

Purchase

The **Purchase** subpane lets you record the basic information about a license purchase:

- The **Purchase type** pop-up menu lets you specify the type of purchase you are recording.
- In the **Date** field, the date of the purchase can be entered.
- The **License count** field includes the number of licenses that were bought in the recorded purchase.
- If the **Add to "Licenses owned"** option is checked, the total number of licenses in the **License** pane's **Licenses owned** field is automatically calculated from all purchases with this option checked.
  The option is only available when the purchase type is "New Software".
- The **Purchase price** field lets you record the price of the licenses.
- The **Software version** field contains the version of the software that was bought.
- The **PO #** field lets you specify a purchase order or other internal reference number for the recorded purchase.
- The **License owner** field lets you specify an employee or department that is internally in your organization considered to be the owner of the licenses acquired in the recorded purchase.

Vendor

The **Vendor** subpane lets you record information about the vendor from whom the license was purchased:

- The **Name** field contains the company's name.
- The **Reference #** allows you to specify an internal supplier reference number or a similar key for the vendor's company.
- The **Contact** field contains your contact person at the vendor's company.
- The **Support** field contains a phone number, e-mail address or other contact information for technical support regarding the purchased licenses.

Maintenance

The **Maintenance** subpane lets you specify the maintenance purchased:

- Check the **Maintenance purchased from** option if maintenance has been purchased, either together with software licenses or in a separate agreement. Specify the duration in the two date fields.
- The **Maintenance price** field lets you enter the price of the maintenance contract.
- The **Reference #** field contains a contract number or similar identifying information for the maintenance agreement.

Notes

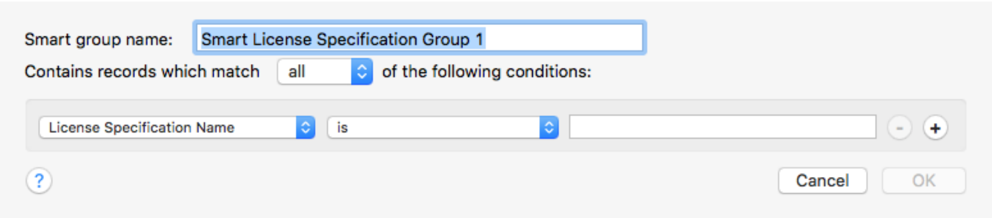
The **Notes** subpane lets you enter any additional information regarding the purchased licenses.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Distribution and Licensing Info" command (described on page 481).

New Smart License Specification Group

The **New Smart License Specification Group** command creates a new smart group for license specifications.

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart License Specification Group 1

Contains records which match all of the following conditions:

License Specification Name is

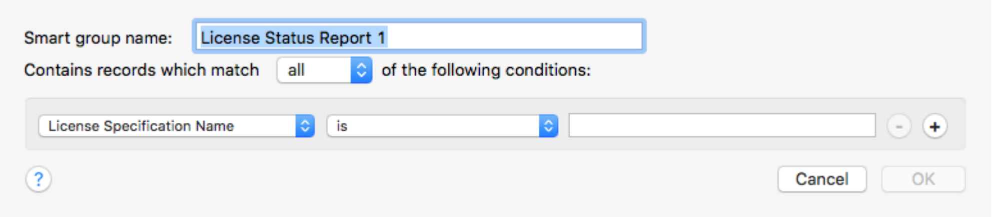
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
  - The pop-up menu in the middle contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New License Status Report

The **New License Status Report** command creates a new licensing report smart group listing license specifications. The report created in this way is similar to the **Fully compliant**, **Licenses exceeded**, or **Prohibited software** reports.

Choosing the command opens the **Smart Group** dialog:



Smart group name: License Status Report 1

Contains records which match all of the following conditions:

License Specification Name · is

The dialog contains these elements:

- **Smart group name**: The name for the licensing report.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
  - The pop-up menu in the middle contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Software Usage Report

The **New Software Usage Report** command creates a new licensing report smart group listing the state of individual computers regarding individual licensed applications. The report created in this way is similar to the **Software usage** or **Missing software** reports.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 725.

New History Report

The **New History Report** command creates a new licensing report smart group listing license history snapshots.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 725.

New History Summary Report

The **New History Summary Report** command creates a new statistical report on the maximum, minimum, and average usage of the specified licenses.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 725.

New Missing Software Report

The **New Missing Software Report** command creates a new report smart group listing missing software that meets the specified criteria.

Except for the available items in the left-hand pop-up menu, this dialog is similar to the one described in “New Distribution Point” on page 725.

Computer Groups

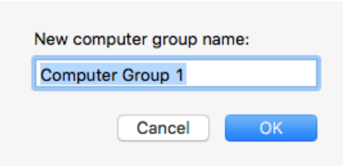
The **Computer Groups** submenu contains commands for managing computer groups for both software distribution and license monitoring:

- **New Computer Group** (page 740)
- **New Smart Computer Group** (page 741)
- **Remove All Group Members** (page 742)

New Computer Group

The **New Computer Group** command creates a new computer group.

Choosing the command opens the **New Computer Group** dialog:


New computer group name: Computer Group 1

The **New computer group name** field lets you specify the name for the new group.

Clicking **OK** creates the group.

Computers, software packages, and license specifications can be assigned to the computer group by dragging them on top of the category.

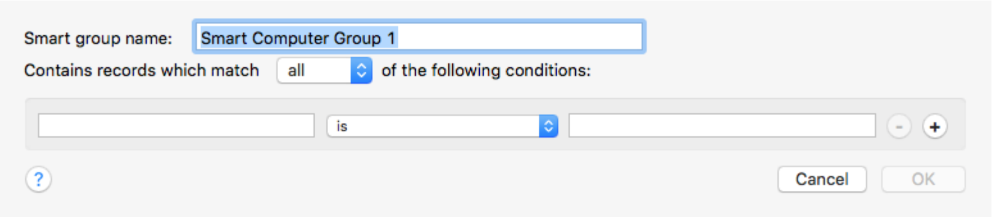
NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **New Computer Group** command can be used only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 758 for details.

New Smart Computer Group

The **New Smart Computer Group** command creates a new smart computer group.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Computer Group 1

Contains records which match all of the following conditions:

is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
    - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
    - The pop-up menu contains the possible comparison operators.
    - The right-hand text field lets you specify the value to compare record values against.
    - The **+** and **–** buttons let you add new conditions or remove existing ones.

Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **New Smart Computer Group** command can be used only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 758 for details.

Remove All Group Members

The **Remove All Group Members** command removes selected computers from a computer group.

Choosing the command removes the selected computers from the computer group in which they were selected. A confirmation alert is displayed first. The computers remain in the database and they also remain in any other computer groups of which they may be members.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Distribution and Licensing Info” command (described on page 481).

NOTE The **Remove All Group Members** command can be used only by administrators with the **Modify Computer Groups** right. See “New Administrator” on page 758 for details.

Actions

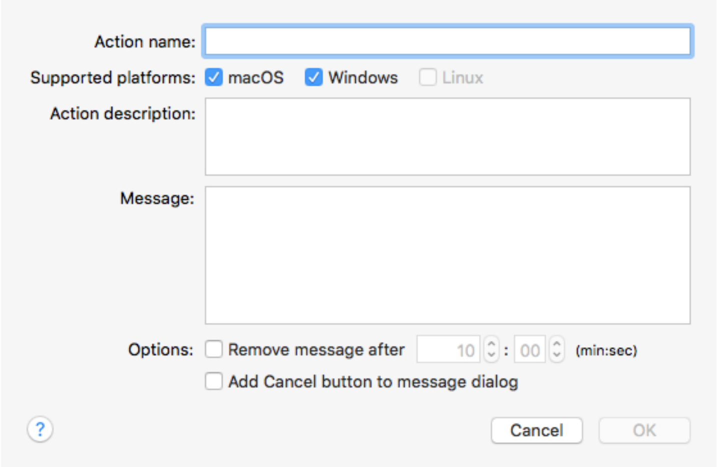
The **Actions** submenu contains commands for working with actions that can be assigned to smart computer groups:

- “New Send Message Action” on page 743
- “New Send E-Mail Action” on page 744
- “New Send SMS (Text Message) Action” on page 745
- “New Set Agent Name Action” on page 746
- “New Set Custom Field Value Action” on page 747
- “New Gather Inventory Action” on page 747
- “New Register User in VPP Action” on page 749
- “New Send VPP Invitation Action” on page 750
- “New Retire User from VPP Action” on page 752
- “New Remove Configuration Profile Action” on page 753
- “New Execute Script Action” on page 754
- “New Terminate Process Action” on page 755
- “New Edit Windows Registry Action” on page 756

- “New Remove from MDM Management Action” on page 757
- “Duplicate Action” on page 758
- “New Smart Actions Group” on page 758

New Send Message Action

This command opens the **Send Message Action** dialog in which you can specify a message that is to be sent to computers that become members of a computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows □ Linux

Action description:

Message:

Options: □ Remove message after 10 : 00 (min:sec)

□ Add Cancel button to message dialog

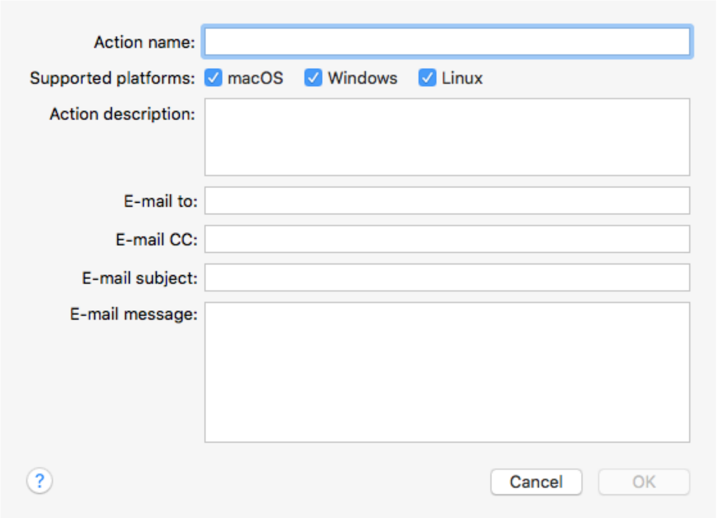
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Message text**: The text that is sent to managed computers that trigger the action. The message appears on-screen on the computer.
  In this text, you can use the variables described in “Variables for computers” on page 401.
- **Remove message after**: If this option is chosen, you can enter a time in minutes and seconds after which the message dialog on the client computer is automatically closed.
  The dialog is closed as if the user had clicked **OK**. (The timeout is, however, noted in the command history.)
- **Add Cancel button to message dialog**: If this option is checked, the message dialog on the client computer has a **Cancel** button in addition to the **OK** button. You can see in the command history whether a user clicked the **Cancel** button.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Send E-Mail Action

This command opens the **Send E-Mail Action** dialog in which you can specify an e-mail that is to be sent when computers become members of a computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows ☑ Linux

Action description:

E-mail to:

E-mail CC:

E-mail subject:

E-mail message:

The dialog contains these elements:

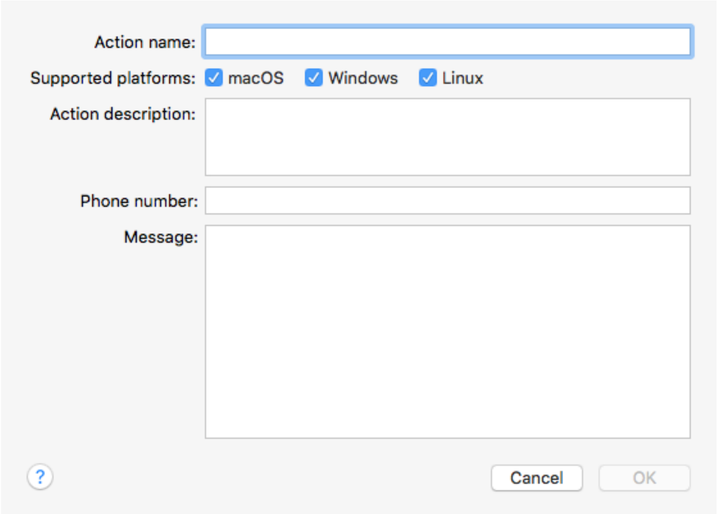
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **E-mail to**: The e-mail address to which the e-mail is to be sent.
- **E-mail cc**: The e-mail addresses to which the e-mail is to be copied, if any.
- **E-mail subject**: The subject of the e-mail.
  In this text, you can use the variables described in “Variables for computers” on page 401.
- **E-mail message**: The body of the e-mail.
  In this text, you can use the variables described in “Variables for computers” on page 401.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

Note that LANrev can send e-mails only when the SMTP information in the **Notification** tab of the **Server Settings** is filled in.

New Send SMS (Text Message) Action

This command opens the **Send SMS Action** dialog in which you can specify an SMS text message that is to be sent when computers become members of a computer group:


Action name:
Supported platforms: ☑ macOS ☑ Windows ☑ Linux
Action description:
Phone number:
Message:

The dialog contains these elements:

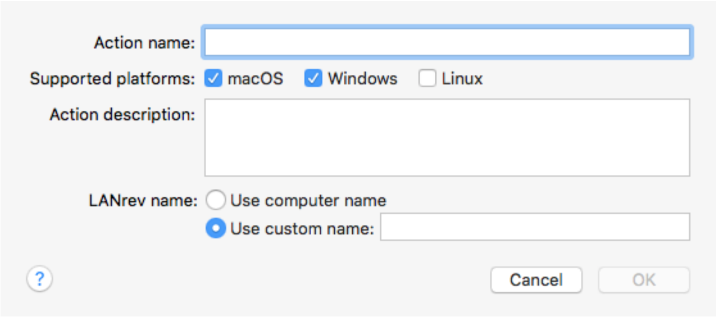
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Phone number**: The telephone number to which the SMS text message is to be sent. When you enter multiple phone numbers separated by commas, the text message is sent to all of them.
- **Message**: The message that is going to be sent. The message may be up to 140 characters long.
  In this text, you can use the variables described in "Variables for computers" on page 401. Note that the limit of 140 characters applies after the variables have been substituted with the actual values.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

Note that LANrev can send texts only when the SMS information in the **Notification** tab of the **Server Settings** is filled in.

New Set Agent Name Action

This command opens the **Set Agent Name Action** dialog in which you can specify that the name that the Agent reports for the computer is changed when the computer becomes the member of a smart computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows □ Linux

Action description:

LANrev name: ○ Use computer name
● Use custom name:

Note that this does not change the actual computer name (as specified in the local settings of the computer), just the name under which the computer appears in LANrev.

The dialog contains these elements:

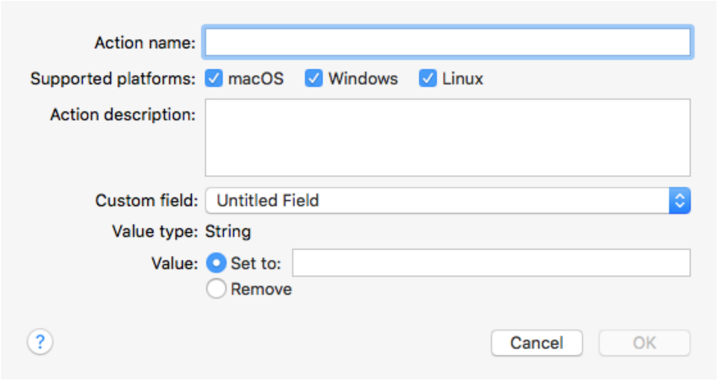
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Use computer name**: If this option is chosen, the computer will appear in LANrev under the name it is has in the local operating system settings.
- **Use custom name**: If this option is chosen, the computer will appear in LANrev under the name specified in the text field beside the option.
  In this text, you can use the variables described in “Variables for computers” on page 401.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

When the action is applied to a device, LANrev renames the device according to the specifications in the action. This action can be applied only to iOS devices running iOS 8 and above and Android devices.

New Set Custom Field Value Action

This command opens the **Set Custom Field Value Action** dialog in which you can specify the value for a custom field that is set for the computer when it becomes the member of a computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows ☑ Linux

Action description:

Custom field: Untitled Field

Value type: String

Value: ● Set to:
○ Remove

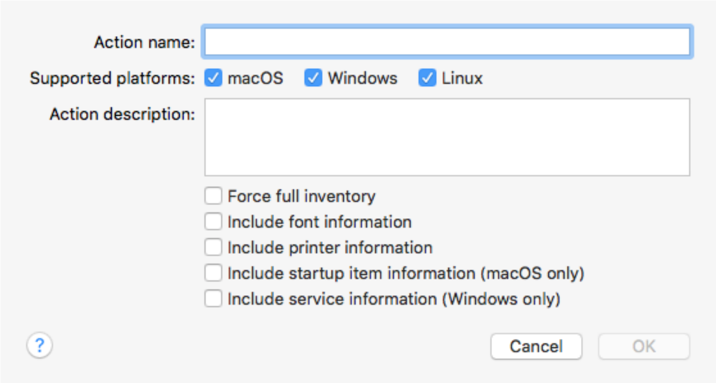
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Custom field**: The field for which the value is set.
  The pop-up menu contains all manual custom information fields that have been defined on the server.
- **Value type**: The data type that the field value must have.
- **Value**: The value to which the field is set on the device on which the action is executed. If you choose the **Remove** option, any existing value is removed from the field.
  In this text, you can use the variables described in “Variables for computers” on page 401.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Gather Inventory Action

This command opens the **Gather Inventory Action** dialog in which you can specify that the information stored on the inventory server for a computer is updated when it becomes the member of a computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows ☑ Linux

Action description:

□ Force full inventory

□ Include font information

□ Include printer information

□ Include startup item information (macOS only)

□ Include service information (Windows only)

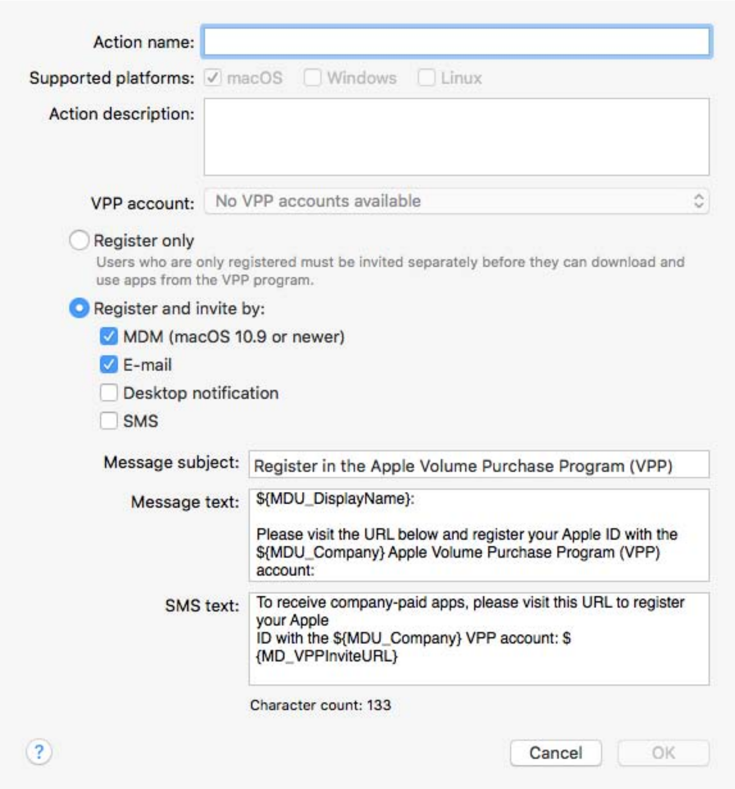
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Force full inventory**: If this option is checked, the server retrieves all inventory information from the agents on the target computers. If the option is unchecked, only information that has changed since the last transmission is transmitted to the server.
- **Include font information**: If this option is checked, font information is gathered from the target computers. If the option is unchecked, no font information is gathered.
- **Include printer information**: If this option is checked, information on printers is gathered from the target computers. If the option is unchecked, no printer information is gathered.
- **Include startup item information**: If this option is checked, information on startup items is gathered from the target macOS computers. If the option is unchecked, no startup item information is gathered.
- **Include service information**: If this option is checked, information on active services is gathered from the target Windows computers. If the option is unchecked, no services information is gathered.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Register User in VPP Action

This command opens the **Register User in VPP Action** dialog in which you can specify a VPP account to which to add users of computers on which the action is executed as well as whether to send an invitation message at the same time and, if so, what message to send:



Action name:

Supported platforms: ☑ macOS □ Windows □ Linux

Action description:

VPP account: No VPP accounts available

○ Register only

Users who are only registered must be invited separately before they can download and use apps from the VPP program.

● Register and invite by:

☑ MDM (macOS 10.9 or newer)

☑ E-mail

□ Desktop notification

□ SMS

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text: ${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

SMS text: To receive company-paid apps, please visit this URL to register your Apple ID with the ${MDU_Company} VPP account: ${MD_VPPInviteURL}

Character count: 133

The dialog contains these elements:

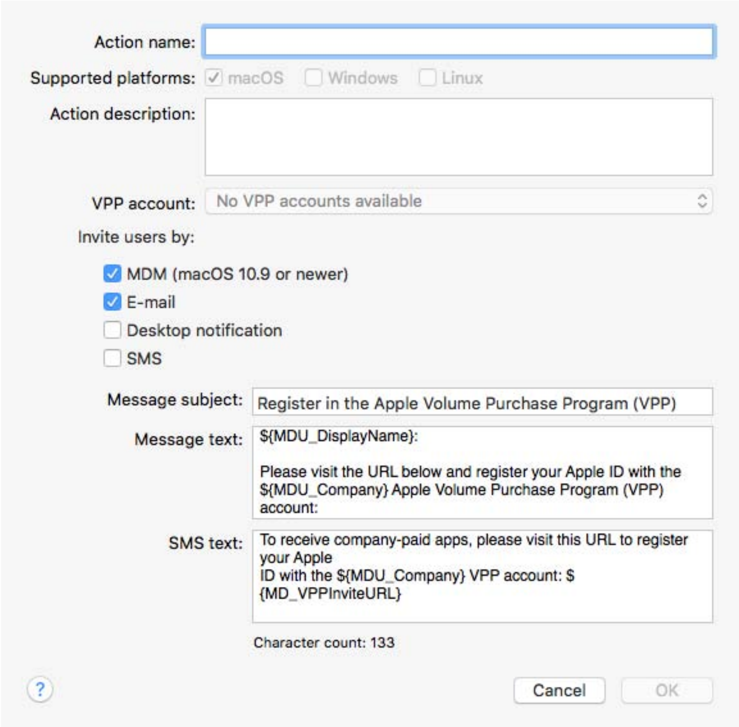
- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: The account in which you want to register the users of the computer. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
- **Register only**: If this option is checked, the users affected by this action are registered for the VPP account, but not invited to link their Apple ID to the account. This invitation has to happen later through the **New Send VPP Invitation Action** action or the **Send VPP Invitation** command.
  This two-step process is faster on Apple's back-end then immediately inviting users and is therefore recommended if you expect to process large numbers of users in one go.

- **Register and invite by**: Check all channels over which you want to send the registration notice to the users. (Users need to complete the registration themselves by entering their personal Apple ID on Apple's VPP website.)
  Invitations via MDM can only be sent to clients running macOS 10.9 and above.
  For registering a large number of users, this option can be slower than choosing **Register only**.
- **Message subject**: The subject text for the invitation.
  In this text, you can use the variables described in "Variables for computers" on page 401.
- **Message text**: The text of the message sent via e-mail.
  In this text, you can use the variables described in "Variables for computers" on page 401.
  In addition, you can use the MD_VPPInviteURL variable, which is displayed as a link to the web page in the App Store where the users have to enter her or his Apple ID to register for the VPP account of your organization.
- **SMS text**: The text of the message sent via SMS.
  You can use the same variables as for **Message text**.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Send VPP Invitation Action

This command opens the **Send VPP Invitation Action** dialog in which you can specify a VPP account to which users of computers on which the action is executed are invited. You can also specify the invitation message to send:



Action name:

Supported platforms: ☑ macOS □ Windows □ Linux

Action description:

VPP account: No VPP accounts available

Invite users by:

☑ MDM (macOS 10.9 or newer)
☑ E-mail
□ Desktop notification
□ SMS

Message subject: Register in the Apple Volume Purchase Program (VPP)

Message text: ${MDU_DisplayName}:

Please visit the URL below and register your Apple ID with the ${MDU_Company} Apple Volume Purchase Program (VPP) account:

SMS text: To receive company-paid apps, please visit this URL to register your Apple
ID with the ${MDU_Company} VPP account: $
{MD_VPPInviteURL}

Character count: 133

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: The account in which you want to register the users of the devices. The pop-up menu lists all accounts that have been defined in the **MDM** tab of the server settings.
- **Invite users by**: Check all channels over which you want to send the registration notice to the users. (Users need to complete the registration themselves by entering their personal Apple ID on Apple’s VPP website.)
  Invitations via MDM can only be sent to clients running macOS 10.9 and above.
- **Message subject**: The subject text for the invitation.
  In this text, you can use the variables described in “Variables for computers” on page 401.
- **Message text**: The text of the message sent via e-mail.
  In this text, you can use the variables described in “Variables for computers” on page 401.
  In addition, you can use the MD_VPPInviteURL variable, which is displayed as a link to the web page in the App Store where

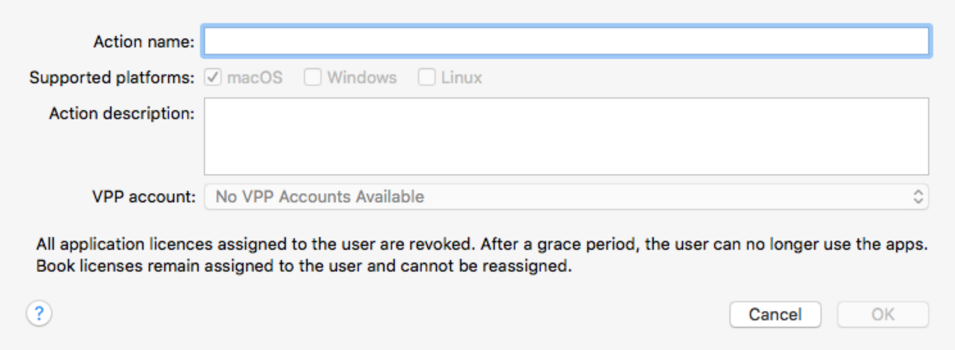
the users have to enter her or his Apple ID to register for the VPP account of your organization.

- **SMS text**: The text of the message sent via SMS.
  You can use the same variables as for **Message text**.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Retire User from VPP Action

This command opens the **Retire User from VPP Action** dialog in which you can specify the VPP account from which to remove the users of computers:



Action name:

Supported platforms: ☑ macOS ☐ Windows ☐ Linux

Action description:

VPP account: No VPP Accounts Available

All application licences assigned to the user are revoked. After a grace period, the user can no longer use the apps. Book licenses remain assigned to the user and cannot be reassigned.

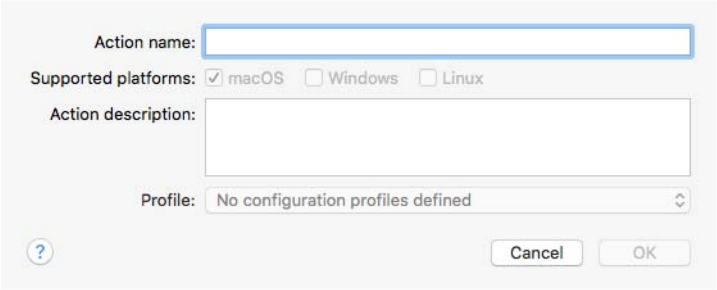
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **VPP account**: A list of all available VPP accounts. The users of the target computers will be removed from the selected account when the action is triggered.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Remove Configuration Profile Action

This command opens the **Remove Configuration Profile Action** dialog in which you can specify a configuration profile that is to be removed from a computer when it becomes a member of a computer group:



Action name:

Supported platforms: ☑ macOS ☐ Windows ☐ Linux

Action description:

Profile: No configuration profiles defined

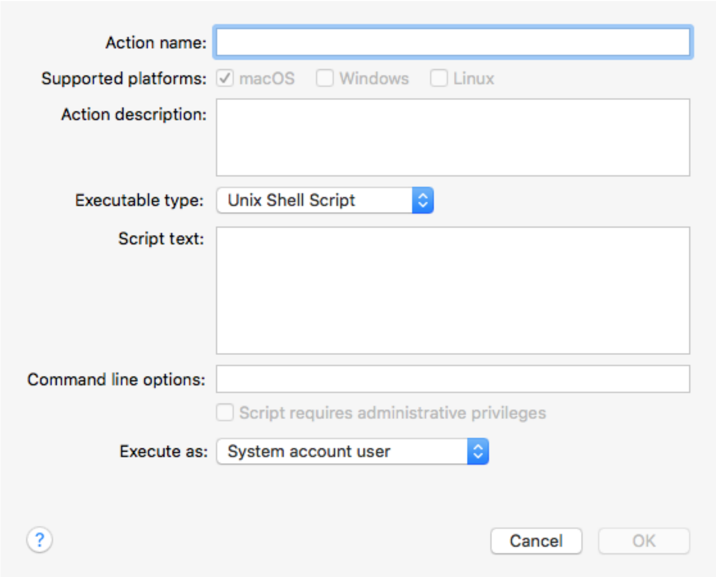
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Configuration profile**: A list of all available configuration profiles. The chosen profile will be removed from the target computers when the action is triggered.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Execute Script Action

This command opens the **Execute Script Action** dialog in which you can specify a script that is executed on computers when they become members of a computer group:



Action name:

Supported platforms: ☑ macOS ☐ Windows ☐ Linux

Action description:

Executable type: Unix Shell Script

Script text:

Command line options:

☐ Script requires administrative privileges

Execute as: System account user

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply. This setting is chosen automatically based on the executable type (see below) and cannot be changed manually.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Executable type**: The type of program that is to run on the clients to gather the information for the field:
  - Unix shell script (macOS targets)
  - AppleScript (macOS targets)
  - DOS batch file (Windows targets)
  - Visual Basic script (Windows targets)
  - PowerShell script (Windows targets)

  Depending on the choice made in this pop-up menu, different fields become available in the dialog pane.
- **Script text**: The code of the script to be executed on the target computers.
  Note: LANrev offers syntax verification functions only for AppleScript scripts; we strongly recommend that you test the scripts before entering them here.
- **Command line options**: Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question).

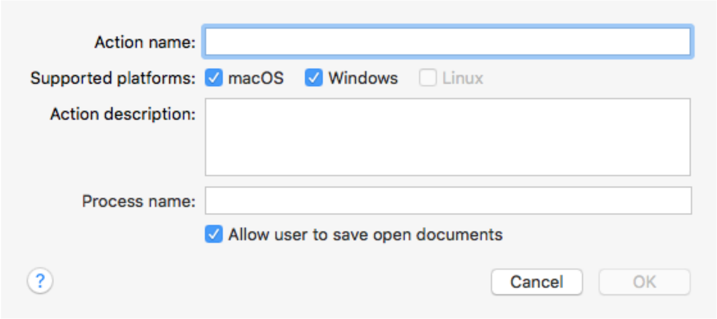
You can include shell variables in the options, as described in "Environment variables" on page 176.

- **Check Syntax**: Clicking this button checks the syntactical correctness of the script in the **Script text** field. (This button is available for the **AppleScript** executable type.)
- **Executable requires administrative privileges**: If this option is checked, the specified script is executed with administrator privileges on the target computers. (This option is available for the **Unix Shell Script** executable type.)
- **Execute as**: This pop-up menu allows you to specify a user account on the target computers with the privileges of which the script is executed. (This option is available for the **Unix Shell Script**, **DOS Batch File**, **Visual Basic Script**, and **PowerShell** executable types.)

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all devices that are currently members of the computer group. It will also be applied to any device that becomes a member of the computer group when it becomes a member.

New Terminate Process Action

This command opens the **Terminate Process Action** dialog in which you can specify a process that is terminated on each computer that becomes the member of a computer group:



Action name:

Supported platforms: ☑ macOS ☑ Windows ☐ Linux

Action description:

Process name:

☑ Allow user to save open documents

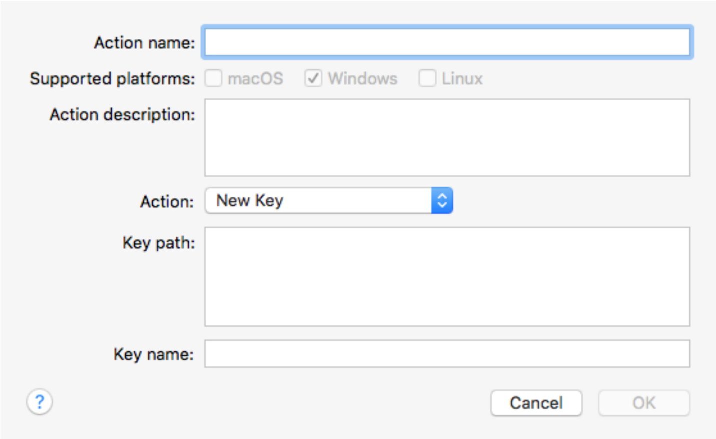
The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Process name**: The name of the process to be terminated. The name must match what is displayed in the process manager of the respective target platform.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all computers that are currently members of the group. It will also be applied to any computer that becomes a member of the group when it becomes a member.

New Edit Windows Registry Action

This command opens the **Edit Windows Registry Action** dialog in which you can specify a modification to the Windows registry that is applied to each Windows computer that becomes the member of a computer group:



Action name:

Supported platforms: □ macOS ☑ Windows □ Linux

Action description:

Action: New Key

Key path:

Key name:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.
- **Action**: This pop-up menu lets you specify the desired action that you want to perform in the target computers' registries. These actions are available:
  - **New Key**: Create a new key at a specified path.
  - **New Value**: Create a new value in a specified key.
  - **Change Value**: Alter a value at a specified location.
  - **Delete Key**: Delete a specified key and all its contents.
  - **Delete Value**: Delete a specified value.
  - **Rename Key**: Change the name of a specified key.
  - **Rename Value**: Change the name of a specified value.

Additional elements let you enter key and value specifications and data. Which of them are visible depends on the chosen action. This is a list of all elements; only a subset is visible in each case:

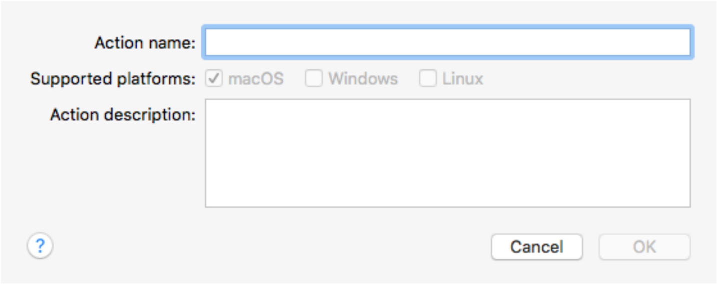
- **Key path**: The path of an existing key in which a new key or value is to be created.
- **Key name**: The name of the new key that you want to create.

- **Value path**: The path of a value that is to be changed.
- **Value type**: The data type of a new value or of a value that is to be changed.
- **Value**: The new data of a value.
- **Path**: The path of a key or value that is to be deleted or renamed.
- **New name**: The new name of a key or value.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all computers that are currently members of the group. It will also be applied to any computer that becomes a member of the group when it becomes a member.

New Remove from MDM Management Action

This command opens the **Remove from MDM Management Action** dialog in which you can specify that a computer is removed from MDM management when it becomes the member of a computer group:



Action name:

Supported platforms: ☑ macOS □ Windows □ Linux

Action description:

The dialog contains these elements:

- **Action name**: The name under which the action is stored in LANrev.
- **Supported platforms**: The operating system platforms to which you want the action to apply.
- **Action description**: A descriptive text explaining the purpose of the action. The text is displayed in LANrev Admin and is intended for your own reference and that of other administrators.

Clicking **OK** saves the action in LANrev. It can then be assigned to a smart computer group, which applies it automatically to all computers that are currently members of the group. It will also be applied to any computer that becomes a member of the group when it becomes a member.

When the action is applied to a computer, LANrev removes the device from MDM management. This action cannot be reversed inside LANrev; the computer must first be enrolled anew. The device is still administered by LANrev through LANrev Agent, however.

Duplicate Action

This command duplicates the selected action and opens the dialog for editing it. Which dialog it opens depends on the type of the duplicated action. See "Actions" on page 742 for an overview of the available dialogs.

New Smart Actions Group

This command is the **New Smart Group** command standard to all browser windows. It creates a smart group that includes all actions meeting the specified criteria. See "Working with actions" on page 178 for more information on actions.

For details on the **Smart Group** dialog, see "New Smart Group" on page 522.

Administrator Setup

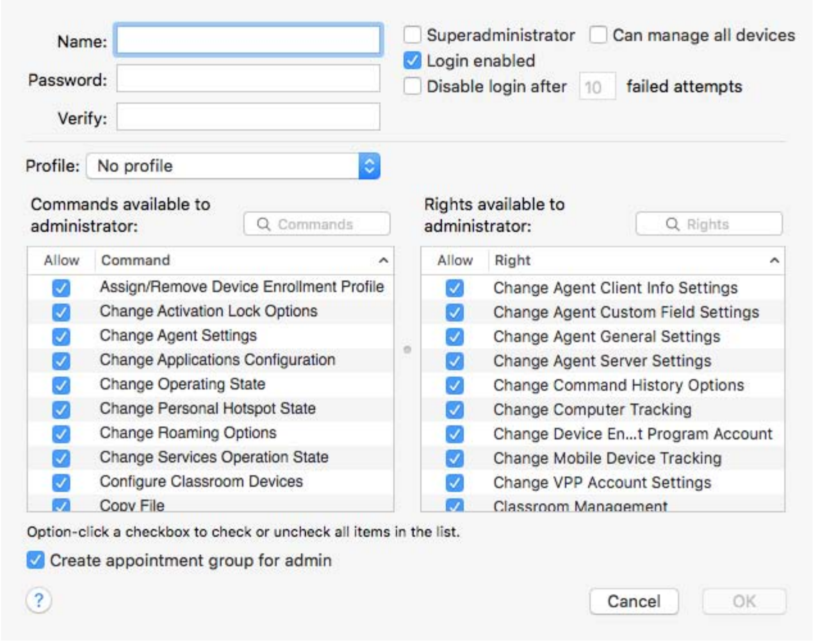
The **Administrator Setup** submenu contains commands for managing administrator accounts as well as administrator and appointment groups:

- **New Administrator** (page 758)
- **Remove Administrator from Group** (page 763)
- **New Administrator Group** (page 763)
- **New Computer Appointment Group** (page 763)
- **New Smart Computer Appointment Group** (page 764)
- **New Mobile Devices Appointment Group** (page 765)
- **New Smart Mobile Devices Appointment Group** (page 765)
- **New Smart Administrator Group** (page 766)
- **Refresh** (page 767)

New Administrator

The **New Administrator** command opens the dialog for creating a new administrator account on the currently connected LANrev server.

Choosing the command opens the **Administrator** dialog:



Name:

Password:

Verify:

☐ Superadministrator ☐ Can manage all devices

☑ Login enabled

☐ Disable login after 10 failed attempts

Profile: No profile

Commands available to administrator:

Allow	Command
☑	Assign/Remove Device Enrollment Profile
☑	Change Activation Lock Options
☑	Change Agent Settings
☑	Change Applications Configuration
☑	Change Operating State
☑	Change Personal Hotspot State
☑	Change Roaming Options
☑	Change Services Operation State
☑	Configure Classroom Devices
☑	Copy File

Rights available to administrator:

Allow	Right
☑	Change Agent Client Info Settings
☑	Change Agent Custom Field Settings
☑	Change Agent General Settings
☑	Change Agent Server Settings
☑	Change Command History Options
☑	Change Computer Tracking
☑	Change Device En...t Program Account
☑	Change Mobile Device Tracking
☑	Change VPP Account Settings
☑	Classroom Management

Option-click a checkbox to check or uncheck all items in the list.

☑ Create appointment group for admin

The dialog contains these elements:

- **Name**: The log-in name of the account.
- **Password**: The password. A password may contain any Unicode character.
- **Verify**: Whenever the password is changed, you need to retype the new password in this field. If the contents of the **Password** and **Verify** fields do not match, an error message is displayed and the password change is rejected.
- **Superadministrator**: When this option is checked, the account has superadministrator privileges, when it is not, it has normal privileges. (Details on administrator privileges are available in “Initial configuration of LANrev Server” on page 17.)
- **Can manage all devices**: If this option is checked, the administrator can access all computers and mobile devices that are managed on the LANrev server. If the option is unchecked, the administrator can mange only devices to which the account has been expressly assigned.
- **Login enabled**: The account is active. If the option is unchecked, the account is temporarily suspended; the user cannot access LANrev Admin.
- **Disable login after**: If this option is checked, only a specified number of wrong passwords are permitted per login attempt. If more incorrect passwords are entered, the account is automatically disabled. To enable it again, another administrator must recheck the **Login enabled** option (see above).
  This option is not available for superadministrator accounts.
- **Profile**: Using this pop-up menu, account settings can be saved as a profile and profiles applied to the account.
  - Profile names: In the upper section of the pop-up menu, all existing profiles are listed. Choosing a profile from the

menu applies its settings to the current administrator account.

Note: Profiles are merely presets: Changing a profile-based account does not affect the profile and vice versa.

- **Commands available to administrator**: The administrator can use all commands checked in this list.
  The individual options in the list correspond to commands from the **Commands** menu.
  Note: Any commands related to mobile devices also require the Manage Mobile Devices right (see below) to be enabled for the administrator to be able to use them.
  Note: Holding down the Option key while clicking a checkbox in this list checks or unchecks all options in the list.
- **Create appointment group for admin**: If this option is checked, LANrev automatically creates two appointment groups in the Server Center's sidebar, one for computers and one for mobile devices. The groups list, respectively, all computers and mobile devices to which the administrator has been assigned and offers a convenient way to assign him or her to additional devices.
- **Rights available to administrator**: The administrator can perform all actions checked in this list. These are the available rights and the corresponding access options in LANrev Admin:
  - **Change Agent Client Info Settings**: Set options in the **Client Information** tab of the **Agent Settings** command window.
  - **Change Agent Custom Field Settings**: Set options in the **Custom Fields** tab of the **Agent Settings** command window.
  - **Change Agent General Settings**: Set options in the **General** tab of the **Agent Settings** command window.
  - **Change Agent Server Settings**: Set options in the **Servers** tab of the **Agent Settings** command window.
  - **Change Command History Options**: Specify in a command window's **Command Options** dialog under which conditions the command will be listed in the command history.
    If an administrator does not have this right, all of his or her commands will be issued with the **Always add to command history** setting.
  - **Change Computer Tracking**: Set and edit computer tracking options using the **Computer Tracking** context menu command from a browser window.
  - **Change Device Enrollment Account**: Set up and modify accounts in Apple's device enrollment program.
  - **Change Mobile Device Tracking**: Set and edit mobile device tracking options.
  - **Change VPP Account Settings**: Set up and modify accounts in Apple's volume purchasing program.
  - **Classroom Management**: Manage classroom-related settings through the **Classroom Management** window and associated functions.
  - **Deploy Agents**: Use the Agent Deployment Center.

- **Enable Computer Tracking Screenshots**: Enable the **Take screenshots** option in the **Computer Tracking** dialog.
- **Enter Custom Field Data**: Enter and edit information in Manual type custom information fields (that is, fields that are not calculated automatically by LANrev).
- **Manage Device Users**: Import and remove device users.
- **Manage Mobile Devices**: Issue commands to mobile devices managed from LANrev through an MDM server. This right is a “master switch” for the administrator account. It is required for the administrator to be able to send commands to mobile devices at all, but any specific commands he or she is to be able to send must also be checked in the **Commands available to administrator** list, (see above).
- **Mobile Remote Control**: Remotely view and manipulate the screen of mobile devices supporting this feature.
- **Modify Computer Groups**: Create, edit, or delete computer groups in the Server Center.
- **Modify Configuration Profiles**: Import or delete configuration profiles for computers in the Server Center.
- **Modify Custom Information Fields**: Create, edit, and delete custom information field definitions on the server.
- **Modify Desktop Actions**: Create, edit, or delete actions that can be applied to computers entering a smart computer group.
- **Modify Device Enrollment Profiles**: Import or delete profiles for enrolling devices in Apple’s device enrollment program.
- **Modify Disk Images**: Create, edit, or delete disk images for reinstalling computers in the Server Center.
- **Modify Distribution Points**: Create, edit, or delete distribution point definitions in the Server Center.
- **Modify Enrollment Users**: Import enrollment users, assign them to devices, and change the tpye of enrolled device (private or company-owned).
- **Modify iBooks Books**: Create, edit, or delete entries for books from the iTunes bookstore for installation on administered mobile devices.
- **Modify License Specifications**: Create, edit, or delete license specifications in the Server Center.
- **Modify Mobile Actions**: Create, edit, or delete actions that can be applied to mobile devices entering a smart policy.
- **Modify Mobile Applications**: Create, edit, or delete application packages for installation on administered mobile devices.
- **Modify Mobile Device Configuration Profiles**: Import or delete configuration profiles for mobile devices in the Server Center.
- **Modify Mobile Device Policies**: Create, edit, or delete policies for administered mobile devices.
- **Modify Mobile Media**: Create, edit, or delete media files to be distributed to administered mobile devices.

- **Modify Samsung KNOX Accounts**: Enter and modify information about Samsung KNOX accounts in the Server Center.
- **Modify Server Settings**: View and change server options in the Server Center or via the **Change Server Registration** command.
- **Modify Software Packages**: Create, edit, or delete software packages in the Server Center.
- **Modify VPP License Management**: Assign or revoke managed licenses for apps and books purchased through Apple's volume purchasing program.
- **Remote Control**: Open a screen-sharing connection to an administered computer using the **Remote Control** command.
- **Remove Computer Records**: Delete a computer from a browser window, for example, using the **Remove from Server** command.
- **Remove History Commands**: Delete entries from the **History** group in the **Commands** window.
- **Remove Inventory Data**: Delete inventory data, for example, using the **Remove Inventory Data** command.
- **Remove License Reports**: Delete log entries from the **License Monitoring** > **Reports** group in the Server Center.
- **Remove Mobile Device History Commands**: Delete entries from the **Commands** group in the **Mobile Devices** window.
- **Remove Mobile Device Records**: Delete a mobile device from the **Mobile Devices** window.
- **Remove SD Log Entries**: Delete log entries from the **Software Distribution** > **Installation Status** group in the Server Center.
- **Reset Software Packages**: Use the **Reset Package** context menu command in the Server Center.
- **Retry Software Packages**: Use the **Retry Package** context menu command in the Server Center.
- **View Administrator Settings**: See administrator-related information in the Server Center.
- **View Commands Window**: Open the **Commands** window and view its contents.
- **View Computer Tracking Data**: See the contents of information items from the **Computer Tracking** category.
- **View Computer Tracking Screenshots**: See the screenshots taken as part of the computer tracking.
- **View Custom Information Fields**: See the contents of custom information fields.
- **View License Monitoring Settings**: Open the **License Monitoring** category in the Server Center and view its contents.
- **View Mobile Device Tracking Data**: See the collected geolocation data of tracked mobile devices.
- **View Server Status**: Open the **Server Monitor** category in the Server Center and view its contents.

- **View Software Distribution Settings**: Open the **Software Distribution** category in the Server Center and view its contents.

Note: Holding down the Option key while clicking a checkbox in this list checks or unchecks all options in the list.

Remove Administrator from Group

The **Remove Administrator from Group** command removes selected administrators from an administrator group.

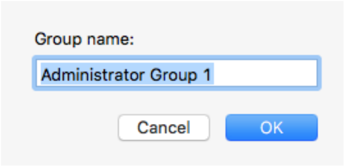
Choosing the command removes the selected administrators from the administrator group in which they were selected. A confirmation alert is displayed first. The administrators remain in the database and they also remain in any other administrator groups of which they may be members.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Administrator Info" command (described on page 482).

New Administrator Group

The **New Administrator Group** command creates a new (non-smart) group for administrator accounts.

Choosing the command opens the **Administrators Group** dialog:


Group name: Administrator Group 1

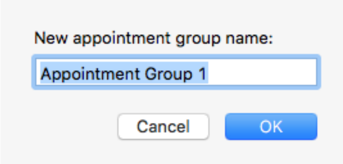
The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Administrator Info" command (described on page 482).

New Computer Appointment Group

The **New Computer Appointment Group** command creates a new (non-smart) appointment group for computers.

Choosing the command opens the **New Appointment Group** dialog:


New appointment group name: Appointment Group 1

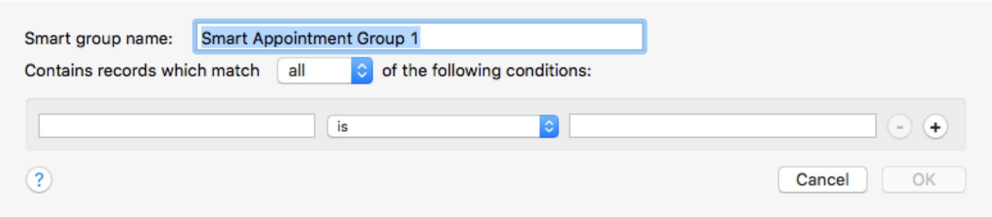
The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Administrator Info” command (described on page 482).

New Smart Computer Appointment Group

The **New Smart Computer Appointment Group** command creates a new appointment group that automatically includes all computers meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart Appointment Group 1
Contains records which match all of the following conditions:
is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

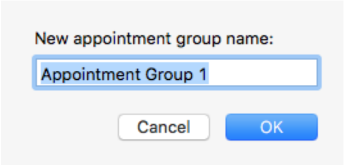
Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Administrator Info" command (described on page 482).

New Mobile Devices Appointment Group

The **New Mobile Devices Appointment Group** command creates a new (non-smart) appointment group for managed mobile devices.

Choosing the command opens the **New Appointment Group** dialog:



New appointment group name: Appointment Group 1

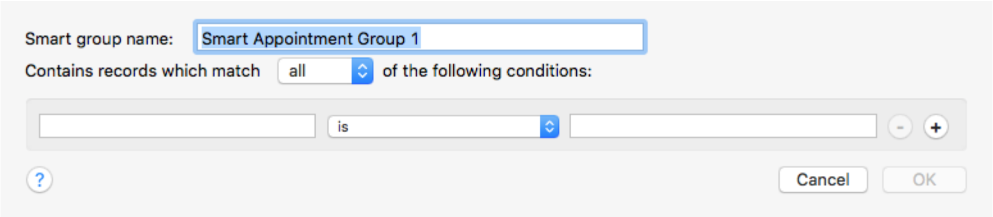
The dialog contains a field for naming the new group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the "Save Administrator Info" command (described on page 482).

New Smart Mobile Devices Appointment Group

The **New Smart Mobile Devices Appointment Group** command creates a new appointment group that automatically includes all mobile devices meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Appointment Group 1

Contains records which match all of the following conditions:

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).

- Conditions area:
  - The left-hand text field lets you enter an information item on which records are to be matched. You can use any information items for mobile devices.
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

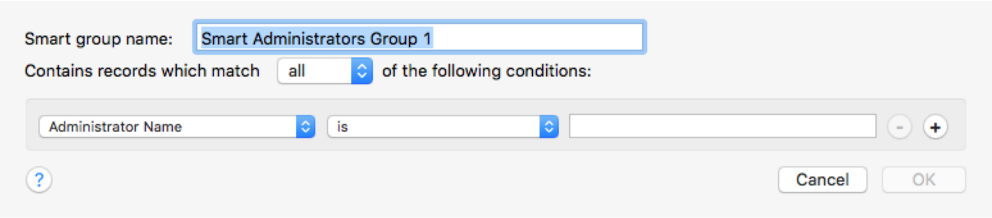
Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the “Save Administrator Info” command (described on page 482).

New Smart Administrator Group

The **New Smart Administrator Group** command creates a new administrator group that automatically includes all administrators meeting the specified criteria.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Administrators Group 1

Contains records which match all of the following conditions:

Administrator Name | is |

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand text field lets you enter an information item on which records are to be matched. You can use any computer-related information item.
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

Clicking **OK** creates the group.

NOTE Any changes become effective only when you commit them to the LANrev server using the “Save Administrator Info” command (described on page 482).

Refresh

The **Refresh** command updates the information displayed in the **Active Directory** section with the current information from the Active Directory servers.

This command is only available when the **Active Directory** category or one of its subcategories is selected.

Custom Information Fields

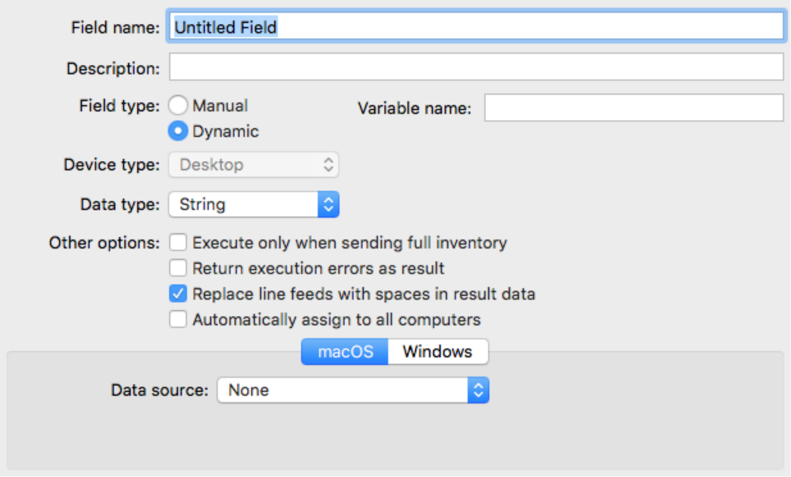
The **Custom Information Fields** submenu contains commands for creating custom information fields:

- **New Custom Information Field** (page 767)
- **Duplicate Custom Information Field** (page 771)
- **Export Selected Fields** (page 772)
- **Import Fields** (page 772)

New Custom Information Field

The **New Custom Information Field** command creates a new custom information field.

Choosing the command displays the setup fields for the newly created field in the Server Center’s main area:



Field name: Untitled Field

Description:

Field type: ○ Manual ● Dynamic

Variable name:

Device type: Desktop

Data type: String

Other options:
□ Execute only when sending full inventory
□ Return execution errors as result
☑ Replace line feeds with spaces in result data
□ Automatically assign to all computers

Data source: None

The dialog contains these elements:

- **Field name**: The name of the custom information field under which it appears in the **Information Items** window.
- **Description**: An optional description of the field which is displayed as a tooltip in the **Information Items** window.
- **Device type**: The type of device for which you create the field, desktop or mobile.
- **Data type**: The type of data that the field contains. Available types include:
  - **String**: Any unformatted text
  - **Number**: Any number. You can choose from several display formats.
  - **Boolean**: True or false
  - **Date**: A point in time
  - **File Version**: A version number according to the conventions of the target platform
  - **IP Address**: An IPv4 address (for example, 192.168.0.1)
  - **Enumeration**: A value from a predefined list. You must specify the list of possible values. (All values are treated as strings.)

  Specifying the proper data type especially helps with sorting the records as expected.
- **Field type**: There are two types of custom information fields:
  - **Manual**: Information in the field is entered manually by you or other administrators.
  - **Dynamic**: Information in the field is automatically calculated by LANrev.
- **Variable name**: If you enter a name here, you can it as a variable to display the content of this custom field. For example, if you specify “myVar” as the variable name, you can display the value of the field in messages, and so on, by inserting `${myVar}`.
  Variables are discussed in “Information variables” on page 175.
  This field is optional.
- **Execute only when sending full inventory**: If this option is checked, the specified scripts are executed only when a full inventory is requested from the agent. (At the first contact, when the agent starts up, or later whenever the **Gather Inventory Information** command is issued with the **Force full inventory** option.)
  If the option is unchecked, the script is executed also when the inventory is incrementally updated.
  This option applies only to dynamic fields.
- **Return execution errors as result**: If this option is checked, any error information that is created during an unsuccessful execution of the specified scripts is returned and entered into the field.
  If the option is unchecked, the field remains empty when the script encounters an execution error.
  This option applies only to dynamic fields.
- **Replace line feeds with spaces in result data**: If this option is checked, LANrev replaces all linebreaks in the results

returned by the script with spaces, turning the result into a single line of text.
This option applies only to dynamic fields.

- **Automatically assign to all computers**: If this option is checked, the custom information field is automatically assigned to all client computers. If it is unchecked, it must be assigned manually to any client computer to which it is to apply.
  This option applies only to dynamic fields.
- **macOS**: This tab lets you the program that is to gather the information for the custom information field on macOS clients. The program must return the desired information as its result. If an action has been defined for the macOS platform, a diamond is displayed on the tab.
  This option applies only to dynamic fields.
  It contains these elements:
  - **Data source**: The type of program or setting that LANrev is to use on the clients to gather the information for the field. Depending on the choice in this pop-up menu, different fields become available in the dialog pane.
  - **File**: The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
    Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to LANrev Server.
  - **Executable**: The field is similar to **File**, described above. (This option is available for the **Other Executable** data source.)
  - **Text**: The text of a script can be entered in this field. The entered script is executed on the target computers. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
    Note: LANrev offers syntax verification or debugging functions only for AppleScript scripts; we strongly recommend that you test the scripts before entering them here.
  - **Command line options**: Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question). You can include shell variables in the options, as described in “Environment variables” on page 176.
    This option is available for the **Unix Shell Script** and **Other Executable** data sources.
  - **Transfer all files in folder containing executable**: If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the script is executed. (This option is available for the **Unix Shell Script** and **AppleScript** data sources.)
    Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).
  - **Execute as**: This pop-up menu allows you to specify a user account on the target computers with the privileges of

which the script is executed. (This option is available for the **Unix Shell Script** and **Other Executable** data sources.)

- **Executable requires administrative privileges**: If this option is checked, the specified script is executed with administrator privileges on the target computers. (This option is available for the **Unix Shell Script** data source.)
- **Location**: The place where the desired plist preferences file is located. (This option is available for the **Property List Value** data source.)
  Note: The **Current Host** *setting refers to preferences stored in* **~/Library/ByHost/**.
- **Domain**: The domain name used as an identifier for the plist file. This is the same as the file name without the .plist extension. (This option is available for the **Property List Value** data source when the **User Preferences** or **System Wide Preferences** location has been chosen.)
  Note: For example, the domain for the Dock's preferences would be com.apple.dock.
- **Full Path**: The full path to the desired plist file. (This option is available for the **Property List Value** data source when the **Full Path** location has been chosen.)
- **Key**: The top-level key in the plist file the value of which LANrev returns as the custom field's contents. (This option is available for the **Property List Value** data source.)
  Note: If you require value from the second or lower levels of a plist file, you have to extract them with a custom script.

- **Windows**: This tab lets you the program that is to gather the information for the custom information field on Windows clients. The program must return the desired information as its result.
  If an action has been defined for the macOS platform, a diamond is displayed on the tab.
  The tab contains these elements:
  - **Data source**: The type of program or setting that LANrev is to use on the clients to gather the information for the field.
    Depending on the choice in this pop-up menu, different fields become available in the dialog pane.
  - **File**: The field can take the path of a file on your computer that is to be executed on the administered computers. You can enter the path manually or select the file using the **Select** button. (This option is available for the **Visual Basic Script**, **DOS Batch File**, and **PowerShell** data sources.)
    Line endings in any scripts you specify are converted to the conventions of the target platform when they are uploaded to LANrev Server.
  - **Executable**: The field is similar to **File**, described above. (This option is available for the **Other Executable** data source.)
  - **Text**: The text of a script can be entered in this field. The entered script is executed on the target computers. (This

option is available for the **Visual Basic Script**, **DOS Batch File**, and **PowerShell** data sources.)
Note: LANrev offers no syntax verification or debugging functions for these scripts; we strongly recommend that you test the scripts before entering them here.

- **Command line options**: Any text entered in this field is passed as a parameter to the specified script (using the usual calling conventions of the script type in question). You can include environment variables in the options, as described in “Environment variables” on page 176.
  This option is available for the **Visual Basic Script**, **DOS Batch File**, **PowerShell**, and **Other Executable** data sources.
- **Transfer all files in folder containing executable**: If this option is checked, all files in the same folder as the specified script file are transferred to the target computers before the script is executed. (This option is available for the **Visual Basic Script**, **DOS Batch File**, **PowerShell**, and **Other Executable** data sources.)
  Note: Line endings in any files that are uploaded because this option is checked are not converted (as are those in scripts, as described above).
- **Execute as**: This pop-up menu allows you to specify a user account on the target computers with the privileges of which the script is executed. (This option is available for all data sources.)
- **Registry Path**: The full path in the registry of the desired value. (This option is available for the **Registry Value** data source.)
  All values are returned as strings, irrespective of the data type of the registry value.
  You can include environment variables in the options, as described in “Environment variables” on page 176.

NOTE The **New Custom Information Field** command can be used only by administrators with the **Modify Custom Information Fields** right. See “New Administrator” on page 758 for details.

Duplicate Custom Information Field

The **Duplicate Custom Information Field** command lets you create a new custom information field based on an existing one.

Choosing the command displays the Custom Information Field dialog that is described in “New Custom Information Field” on page 767.

NOTE Any changes become effective only when you commit them to the LANrev server, for example, using the **Save Custom Information Fields** command (described on page 482).

NOTE The **Duplicate Custom Information Field** command can be used only by administrators with the **Modify Custom Information Fields** right. See “New Administrator” on page 758 for details.

Export Selected Fields

The **Export Selected Fields** command lets you export the definitions for the selected custom information fields to a file.

Choosing the command displays a standard Save dialog where you can specify the name and location for the file.

The command is not available when an external script file or other executable is specified in the definition on the field. (In other words, the command can be used for manual custom information fields and for dynamic fields that are defined using inline scripts, property list values, or registry values.)

NOTE Exported field definitions are stored in a simple XML file with the extension “.lanrevcfdef”. They are intended to be imported into another copy of LANrev Admin using the **Import Fields** command (see below).

Import Fields

The **Import Fields** command lets you import definitions for custom information fields that have previously been exported from LANrev.

Choosing the command displays a standard Open dialog.

New Category

This command is the **New Category** command standard to all browser windows.

For details, see “New Category” on page 523.

Edit <item>

The **Edit <item>** commands let you edit existing items in the Server Center.

The actual name of the command reflects the selected item. If no item or an item that cannot be edited is selected, the command is not available.

Choosing any of the command opens the appropriate dialog. See the descriptions of the corresponding commands for details:

- **Edit Administrator**: **New Administrator**
- **Edit Administrator Group**: **New Administrator Group**
- **Edit Appointment Group**: **New Computer Appointment Group**
- **Edit Configuration Profile**: **New Configuration Profile**
- **Edit Custom Information Field**: **New Custom Information Field**
- **Edit Disk Image**: **New Disk Image**
- **Edit License Specification**: **New License Specification**
- **Edit Payload**: **New Payload**
- **Edit Smart Group**: **New Smart Software Package Group** (or another smart group command)
- **Edit Software Package**: **New Software Package**
- **Edit Distribution Point**: **New Distribution Point**

Duplicate <item>

The **Duplicate <item>** commands let you create copies of existing items in the Server Center and open them for editing.

The actual name of the command reflects the selected item. If no item or an item that cannot be duplicated is selected, the command is not available.

Choosing any of the command opens the appropriate editing dialog. See the descriptions of the corresponding commands for details of these dialogs:

- **Duplicate Configuration Profile**: **New Configuration Profile**
- **Duplicate Custom Information Field**: **New Custom Information Field**
- **Duplicate Disk Image**: **New Disk Image**
- **Duplicate License Specification**: **New License Specification**
- **Duplicate Payload**: **New Payload**
- **Duplicate Software Package**: **New Software Package**
- **Duplicate Distribution Point**: **New Distribution Point**

Remove <item>

The **Remove <item>** commands lets you delete existing items in the Server Center.

The actual name of the command reflects the selected item. If no item or an item that cannot be deleted is selected, the command is not available.

Choosing any of the commands deletes the selected item.

NOTE Any changes become effective only when you commit them to the LANrev server using the appropriate command from the Server menu.

NOTE Using the commands may require specific rights in your administrator account. See “New Administrator” on page 758 for details.

Retrieve Payloads

The **Retrieve Payloads** command lets you download payloads from the distribution point to your local computer.

Choosing the command displays a standard Save dialog in which you can choose a location to which to download the payload file.

NOTE The **Retrieve Payloads** command can be used only by administrators with the **Modify Software Packages** right. See “New Administrator” on page 758 for details.

Retry Package

The **Retry Package** command causes LANrev Server to re-attempt to install a failed software installation. This command is available only in the context menu of the content area and only when software packages, patches, or the **Installation Status** group or one of its subgroups are displayed.

Choosing this command makes LANrev Server retry the installation on all computers where it failed before. It does not re-attempt deferred or refused installations.

NOTE The **Retry Package** command can be used only by administrators with the **Retry Software Packages** right. See “New Administrator” on page 758 for details.

Reset Package

The **Reset Package** command causes LANrev Server to treat the selected package as not yet having been installed on any target computer. This command is available only in the context menu of the content area and only when software packages, patches, or the **Installation Status** group or one of its subgroups are displayed.

Choosing this command causes LANrev Server to install the package on all computers in the distribution groups to which it is assigned, just as if the package was newly created, and irrespective of whether the package has already been installed on a computer or its installation been refused or deferred.

NOTE The **Reset Package** command can be used only by administrators with the **Reset Software Packages** right. See "New Administrator" on page 758 for details.

Export Package

The **Export Package** command lets you export the selected software packages. Exported packages are saved as package files (that is, folders that look like files). When transferred to a Windows computer, they look like folders.

Agent updater packages and patch packages cannot be exported. You cannot export package with changes that have not yet been committed to the server.

NOTE The **Export Package** command can be used only by administrators with the **Modify Software Packages** right. See "New Administrator" on page 758 for details.

Install Selected Software Packages

The **Install Selected Software Packages** command is identical to the **Install Software Packages** command described on page 436, the only difference being that the software packages or metapackages on which you right-click are already selected in the command window.

Export License Specification

The **Export License Specification** command lets you export the selected license specifications. Exported specifications are saved as XML files.

Agent updater packages and patch packages cannot be exported. You cannot export package with changes that have not yet been committed to the server.

NOTE The **Export License Specification** command can be used only by administrators with the **Modify License Specifications** right. See “New Administrator” on page 758 for details.

Repeat Selected Installations

The **Repeat Selected Installations** command becomes available if one or more software installation entries in one of the smart groups in the **Installation Status** section is selected.

Choosing this command causes LANrev to reset the installation status of the selected packages with respect to the selected computers, treating them as if they never had been installed. The packages will be installed on the computers according to their settings.

Show Action Details

This command displays the details on the selected action in the main part of the window. Choosing it is the same as clicking on the action in the **Actions** group in the sidebar of the window.

Duplicate Action

This command opens the selected action in the appropriate **New … Action** dialog with a new name. You can edit the settings as desired and save the duplicate.

The various action editing dialogs are described in “Actions” on page 742.

Edit Action

This command lets you edit the selected action in the appropriate **New … Action** dialog.

The various action editing dialogs are described in “Actions” on page 742.

Remove Action

This command removes the selected action from LANrev. This also removes it from any computer group to which it has been assigned.

If you want to remove an action only from a particular computer group, display that group’s actions and use the **Remove Action from Group** command, described below.

Remove Action from Group

This command removes the selected action from the computer group that is currently displayed.

If you want to delete an action from LANrev, use the **Remove Action** command, described above.

Re-execute This Action for All Devices

Choosing this command treats the selected action as if it has just been assigned to all the computer groups to which it is assigned. It is re-executed on all computers belonging to these groups. Any delays and repetitions specified for the action still apply.

Choosing the command opens an alert in which you can choose between re-executing the action when the computers next check in and immediately re-executing it.

Re-execute This Action for This Group

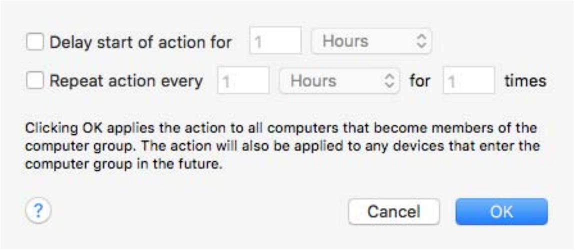
Choosing this command treats the selected action as if it has just been assigned to the displayed computer group. It is re-executed on all computers belonging to the group. Any delays and repetitions specified for the action still apply.

Choosing the command opens an alert in which you can choose between re-executing the action when the computers next check in and immediately re-executing it.

Change Action Schedule

This command lets you change the delay and repetition settings for a particular action in a computer group.

Choosing **Change Action Schedule** opens the **Action Assignment Options** dialog:


□ Delay start of action for 1 Hours

□ Repeat action every 1 Hours for 1 times

Clicking OK applies the action to all computers that become members of the computer group. The action will also be applied to any devices that enter the computer group in the future.

The dialog contains these elements:

- **Delay start of action for**: If this option is chosen, the action will not be performed immediately when a device enters the policy but the specified interval later.
- **Repeat action every**: If this option is chosen, the action is performed repeatedly on the device in the specified interval for the specified number of times. The initial execution is counted as the first repetition, so if you specify that the action is to be repeated two times, the initial action will be executed plus one more execution.

Reset Current Server Load

The **Reset Current Server Load** command causes LANrev Server to reset the count of current connections for the selected distribution point to zero. This does not interrupt any actual connections; it merely changes the bookkeeping information. This command is available only in the context menu of the content area and only when distribution points are displayed.

This command is intended as a troubleshooting tool when the distribution point – perhaps as the consequence of a power outage or other crash – seems to count connections as open that have long since been closed.

Assign Device Enrollment Profile

The **Assign Device Enrollment Profile** command is the same as the **Assign Device Enrollment Profile** command in the **Mobile Devices** window (described on page 627), except that it applies to selected computers.

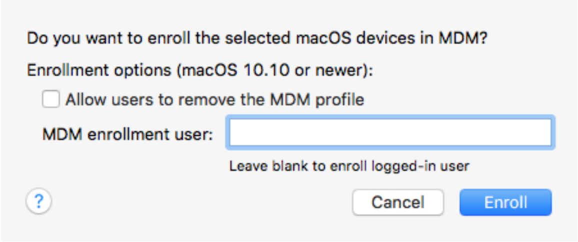
Unassign Device Enrollment Profile

The **Unassign Device Enrollment Profile** command is the same as the **Unassign Device Enrollment Profile** command in the **Mobile Devices** window (described on page 628), except that it applies to selected computers.

Enroll Devices in MDM

The **Enroll Devices in MDM** command lets you enroll a computer running macOS 10.7 or above in MDM. LANrev Agent must already be installed on the computer.

Choosing the command displays the **Enroll Devices in MDM** dialog:



Do you want to enroll the selected macOS devices in MDM?

Enrollment options (macOS 10.10 or newer):

□ Allow users to remove the MDM profile

MDM enrollment user:

Leave blank to enroll logged-in user

The dialog contains these elements:

- **Allow users to remove the MDM profile**: If this option is checked, the enrollment user can delete the MDM profile from the device, thereby removing the device from MDM management. If this option is not checked, the profile cannot be deleted by the user.
  The profile can only be removed on computers running macOS 10.10 or above. (Users of computers running OS X 10.7 through OS X 10.9 can never themselves remove the profiles, irrespective of the setting you choose.)
- **MDM enrollment user**: If a device is used by multiple users, you can specify which of them is enrolled. If this field is left blank, the currently logged-in user is enrolled. If the field is blank and no user is logged in, an error message is displayed.

When you click **OK**, the selected computers are silently enrolled. No additional interaction either by you or by the computers' users is required.

This command is available only to administrators with the "Deploy Agent" right.

Install LANrev Agent via MDM

The **Install LANrev Agent via MDM** command lets you install or update LANrev Agent on computer running macOS 10.10 or above that are managed via MDM.

After you confirm the command, LANrev Agent is silently installed on all selected computers. No additional interaction either by you or by the computers' users is required.

This command is available only to administrators with the "Deploy Agent" right.

Reload Device Enrollment Data

The **Reload Device Enrollment Data** command is the same as the **Reload Device Enrollment Data** command in the **Mobile Devices** window (described on page 629).

Update AD User Information

The **Update AD User Information** command is the same as the **Update AD User Information** command in the **Mobile Devices** window (described on page 634).

Server

The **Server** section in the sidebar of the **Server Center** window contains entries for configuring and monitoring LANrev Server:

- “Server Settings” on page 780
- “Certificate Settings” on page 799
- “Server Monitor” on page 800

Server Settings

The **Server Settings** category lets you view and specify basic settings for the connected LANrev server and set the names of client information fields.

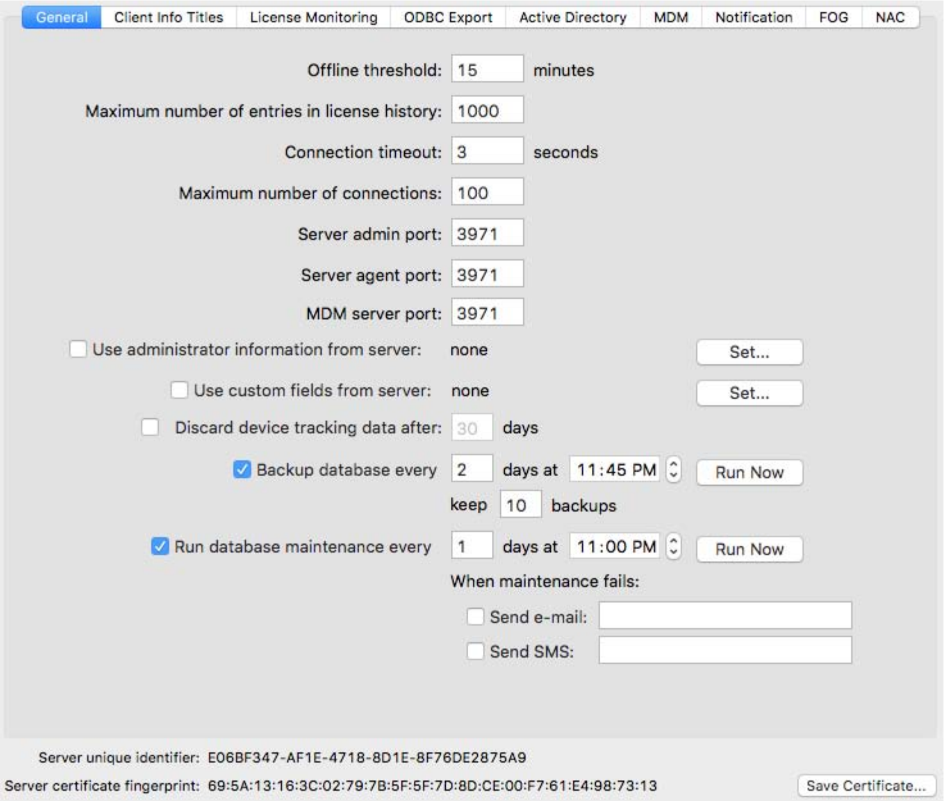
Choosing the command displays the **Server Settings** dialog in the main area of the **Server Center** window. It has these panes:

- **General** (page 781)
- **Client Info Titles** (page 784)
- **License Monitoring** (page 784)
- **ODBC Export** (page 785)
- **Active Directory** (page 786)
- **MDM** (page 787)
- **Notification** (page 795)
- **FOG** (page 798)
- **NAC** (page 798)

NOTE The **Server Settings** command can be used only by administrators with the **Change Server Settings** right. See “New Administrator” on page 758 for details.

General

The **General** pane of the **Server Settings** dialog lets you specify the basic server parameters.



Offline threshold: 15 minutes

Maximum number of entries in license history: 1000

Connection timeout: 3 seconds

Maximum number of connections: 100

Server admin port: 3971

Server agent port: 3971

MDM server port: 3971

□ Use administrator information from server: none

□ Use custom fields from server: none

□ Discard device tracking data after: 30 days

☑ Backup database every 2 days at 11:45 PM

keep 10 backups

☑ Run database maintenance every 1 days at 11:00 PM

When maintenance fails:

□ Send e-mail:

□ Send SMS:

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9

Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13

The **General** pane contains these options:

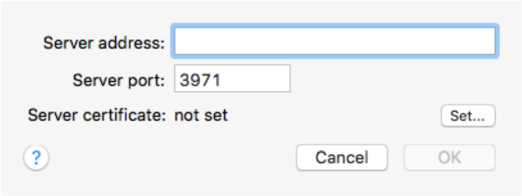
- **Offline threshold**: The interval in which an agent must contact the server. If the server is not contacted by an agent for this time, it considers the agent's computer to be offline.
  Note: This interval should be no shorter than the **Heartbeat Interval** *setting for the agents. (See "Servers" on page 408 for details.)*
- **Maximum number of entries in licensing history**: The maximum number of entries displayed in license history reports. If more entries are generated, only the newest entries are displayed.
  Note: A license history entry records the entire licensing state at a given time, much like a snapshot in a backup history.
- **Connection timeout**: The time after which the server considers an attempt to establish a connection with a LANrev agent or LANrev Admin to have failed.
- **Maximum number of connections**: How many simultaneous connections to agents or admins will this server allow at most?
- **Server admin port**: The port over which the server communicates with LANrev Admin.
- **Server agent port**: The port over which the server communicates with LANrev agents.
- **MDM server port**: The port over which the MDM server communicates.
  Note: The three ports may be the same or different.

- **Use administrator information from server**: By default, each LANrev server contains its own administrator information (accounts, privileges, etc.). When another server is specified here, it instead dynamically gets the information from that server.
  Clicking the **Set** button opens the **Server Properties** dialog where you can specify the server. The dialog is described below.
- **Use custom fields from server**: By default, each LANrev server contains its own custom field definitions. When another server is specified here, it instead dynamically gets the information from that server.
  Clicking the **Set** button opens the **Server Properties** dialog where you can specify the server. The dialog is described below.
- **Discard computer tracking data after**: If this option is checked, LANrev deletes data collected while tracking administered computers after the specified number of days.
- **Backup database every**: This option lets you specify the interval in which the LANrev server's internal database is backed up up as well as the number of backup generations that are kept.
  Clicking the **Run Now** button performs the backup immediately.
  Backup files are stored in the same directory as the database file itself.
- **Run database maintenance every**: This option lets you specify the interval in which the LANrev server's internal database is maintained.
  Maintenance includes compacting the database file and checking it for possible corruption. If corruption is detected, LANrev tries to correct the problem automatically. It informs you whether it appears to have succeeded or not.
  Clicking the **Run Now** button immediately creates a backup.
  Checking **Send e-mail** makes LANrev send an e-mail to the specified address whenever database maintenance is not successful. You can have the e-mails sent to multiple addresses by separating them with commas. (Sending e-mail requires the SMTP information in the **Notification** tab to be filled in.)
  Checking **Send SMS** makes LANrev send a text message (SMS) to the specified phone number whenever database maintenance is not successful. You can enter multiple phone numbers separated by commas to send messages to all of them. (Sending texts requires the SMS information in the **Notification** tab to be filled in.)
- **Server unique identifier**: The unique identifier of the displayed server. You can use this information to verify that you are connected to the correct server.
- **Server certificate fingerprint**: The fingerprint of the SSL certificate with which the displayed server identifies itself. You can use this information to verify that you are connected to the correct server.

- **Save Certificate**: Clicking this button lets you save the server's certificate for use in identifying the server when you assign it to clients.

Server Properties dialog

The **Server Properties** dialog lets you specify a server that supplies administrator account information or custom field information to the server being configured.



Server address:

Server port: 3971

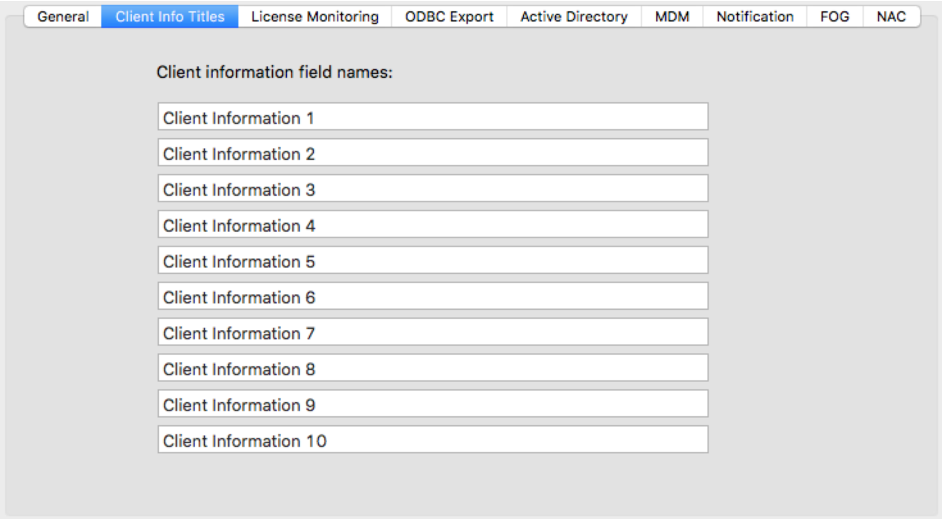
Server certificate: not set

The dialog contains these elements:

- **Server address**: The DNS name or IP address of the desired server.
- **Server port**: The port over which the specified server communicates with agents.
- **Server certificate**: This field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
  Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of the **Save Certificate** button in the **Server Settings** section of the Server Center, as described in "Exporting a server certificate" on page 21.)
  Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

Client Info Titles

The **Client Info Titles** pane of the **Server Settings** dialog contains the names of the ten client information fields in which you can store custom information on the clients.



Client information field names:

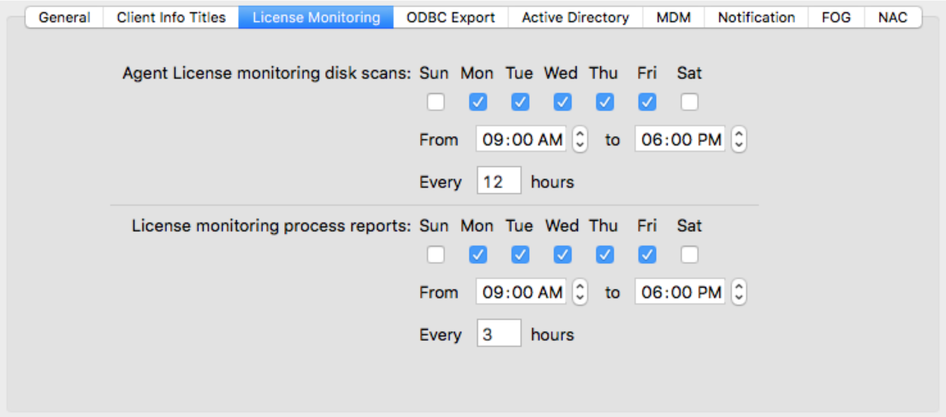
Client Information 1
Client Information 2
Client Information 3
Client Information 4
Client Information 5
Client Information 6
Client Information 7
Client Information 8
Client Information 9
Client Information 10

Editing one of the titles automatically changes the name of that client information field on all agents connected to the server.

NOTE If multiple inventory servers are specified for an agent, it uses the client info titles of the first one in the list in the **Servers** pane of the **Agent Settings** dialog. (For more details, see “Servers” on page 408.)

License Monitoring

The **License Monitoring** tab of the **Server Settings** dialog lets you specify the schedules for the agents’ license monitoring activities.



Agent License monitoring disk scans: Sun □ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □
From 09:00 AM to 06:00 PM
Every 12 hours

License monitoring process reports: Sun □ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □
From 09:00 AM to 06:00 PM
Every 3 hours

In the **Licensing monitoring disk scans** section, you can specify when and how often the Agent should scan the disk for licensed software. The Agent scans at all checked days of the week during the specified hours in the specified interval.

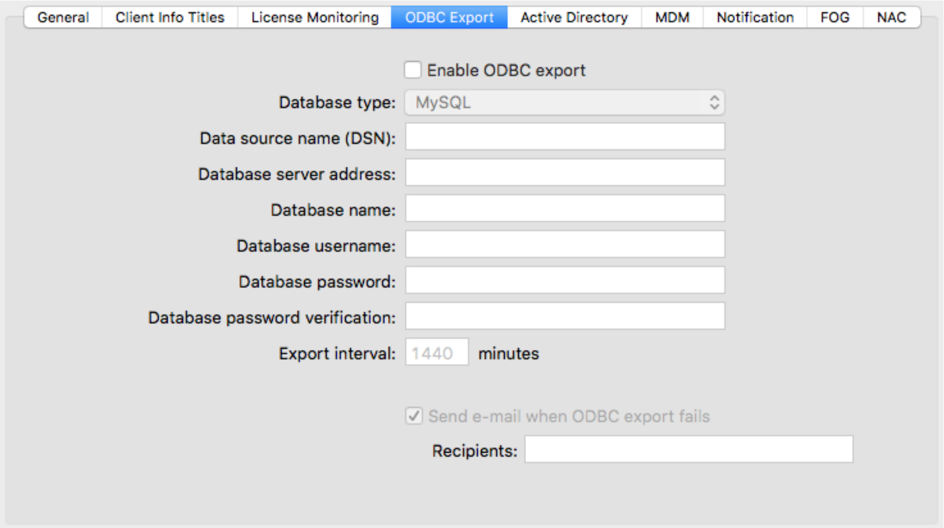
In the **Licensing monitoring process reports** section, you specify when and how often the Agent sends reports on licensed software to the server. Since these reports include both installed software and running software (if there are license specifications that are configured accordingly), it can make sense to send reports more often than disk scans are performed.

Any changes you make here are pushed to the Agents according to the license monitoring update interval settings. (The setting is specified in the **Servers** tab of the **Agent Settings** command window.)

ODBC Export

The **ODBC Export** tab of the **Server Settings** dialog lets you activate and configure link via ODBC to a database into which all data from LANrev's internal database is exported at regular intervals.

NOTE This is a one-way link; no changes to the data in the target database are ever re-imported into LANrev's internal database.



□ Enable ODBC export

Database type: MySQL
Data source name (DSN):
Database server address:
Database name:
Database username:
Database password:
Database password verification:
Export interval: 1440 minutes

☑ Send e-mail when ODBC export fails
Recipients:

The **ODBC Export** pane contains the options listed below. Note that all the database specifications (that is, all options except **Enable ODBC export** and **Data source name**) can be omitted if they are already contained in the specified ODBC data source.

- **Enable ODBC export**: This is the master switch that activates or deactivates the automatic ODBC export.
- **Database type**: The type of the database that is connected via ODBC.
- **Data source name**: The ODBC data source that represents the database.
- **Database server address**: The DNS name or IP address of the server on which the database is hosted.
- **Database name**: A login name for the database. The corresponding account must have sufficient privileges to create tables and write data.
- **Database password** and **Database password verification**: The password for the specified database user account.

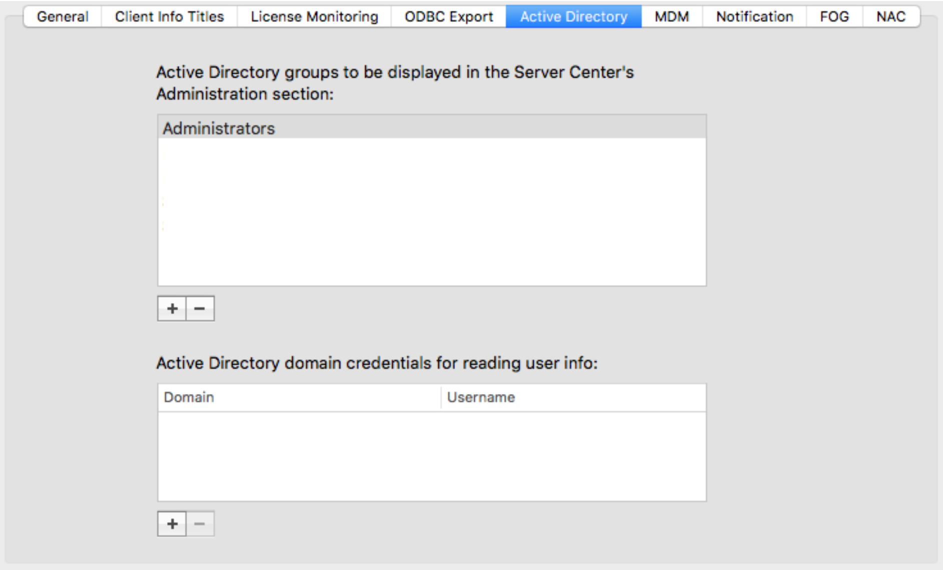
- **Export interval**: The interval in which LANrev is to export data to the database.
- **Send e-mail when ODBC export fails**: If this option is checked, a notification e-mail is sent to the specified addresses. Separate multiple adresses with commas. (Sending e-mail requires the SMTP information in the **Notification** tab to be filled in.)

Active Directory

The **Active Directory** tab of the **Server Settings** dialog lets you specify the Active Directory groups the accounts in which LANrev makes available for creating administrator accounts.

It also lets you specify Active Directory credentials that LANrev uses to request information on users of managed mobile devices from Active Directory. These credentials are needed when your normal Active Directory credentials are not sufficient to request this information. You can specify multiple sets of credentials; LANrev will try all of them until one set turns out to be sufficient to retrieve the information on a user.

NOTE The accounts in the specified groups are not automatically made administrator accounts in LANrev; they are merely available in the **Server Center** window's sidebar for this purpose. Account from groups not specified here are not available.



Active Directory groups to be displayed in the Server Center's Administration section:

Administrators

Active Directory domain credentials for reading user info:

Domain	Username

The tab contains these elements:

- List of groups: The list contains all groups you have so far specified.
- **+**: This button lets you add groups to the list. Clicking the button opens a dialog in which you enter the group's name.
- **-**: Clicking this button removes the selected group from the list.
- List of Active Directory credentials: The list sets of Active Directory credentials used for accessing Active Directory information for users of managed mobile devices.

- **+**: This button lets you add credentials to the list. Clicking the button opens a dialog in which you enter the credentials.
- **-**: Clicking this button removes the selected credentials from the list.

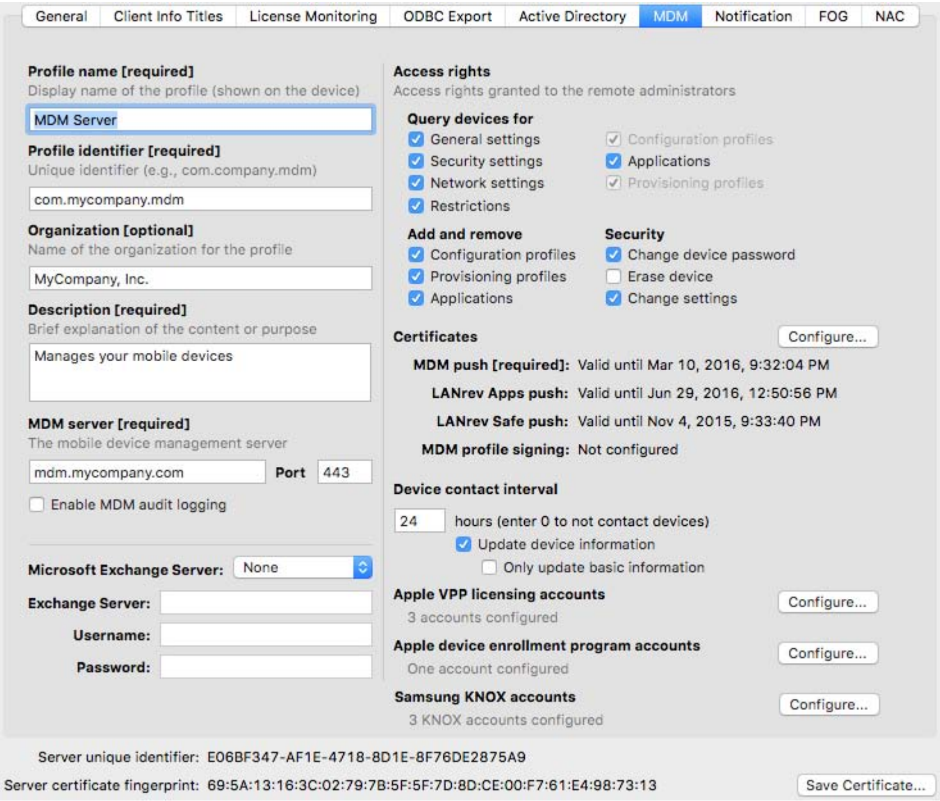
Double-clicking an item in one of the lists opens a dialog that lets you edit the item.

NOTE If an Active Directory account from one of the specified groups is moved out of the group, it will be deleted as an LANrev administrator account.

MDM

The **MDM** tab of the **Server Settings** dialog lets you specify the settings required to manage mobile devices through LANrev.

NOTE Any change in the Access rights section of this dialog has no effect on currently enrolled devices until they are re-enrolled (as described in "Enrolling mobile devices" on page 50).



Profile name [required]
Display name of the profile (shown on the device)
MDM Server

Profile identifier [required]
Unique identifier (e.g., com.company.mdm)
com.mycompany.mdm

Organization [optional]
Name of the organization for the profile
MyCompany, Inc.

Description [required]
Brief explanation of the content or purpose
Manages your mobile devices

MDM server [required]
The mobile device management server
mdm.mycompany.com **Port** 443

□ Enable MDM audit logging

Microsoft Exchange Server: None
Exchange Server:
Username:
Password:

Access rights
Access rights granted to the remote administrators

Query devices for
☑ General settings
☑ Security settings
☑ Network settings
☑ Restrictions
☑ Configuration profiles
☑ Applications
☑ Provisioning profiles

Add and remove
☑ Configuration profiles
☑ Provisioning profiles
☑ Applications

Security
☑ Change device password
□ Erase device
☑ Change settings

Certificates
MDM push [required]: Valid until Mar 10, 2016, 9:32:04 PM
LANrev Apps push: Valid until Jun 29, 2016, 12:50:56 PM
LANrev Safe push: Valid until Nov 4, 2015, 9:33:40 PM
MDM profile signing: Not configured

Device contact interval
24 hours (enter 0 to not contact devices)
☑ Update device information
□ Only update basic information

Apple VPP licensing accounts
3 accounts configured

Apple device enrollment program accounts
One account configured

Samsung KNOX accounts
3 KNOX accounts configured

Server unique identifier: E06BF347-AF1E-4718-8D1E-8F76DE2875A9
Server certificate fingerprint: 69:5A:13:16:3C:02:79:7B:5F:5F:7D:8D:CE:00:F7:61:E4:98:73:13

The tab contains these elements:

- **Profile name**: A descriptive name for the deployment profile. The name will be displayed on the mobile device during the enrollment process.
- **Profile identifier**: A unique identifier for the deployment profile.

- **Organization**: The name of your organization. This information is optional.
- **Description**: A brief description of the purpose of the deployment profile. Users of mobile devices will see this description during the enrollment process.
- **MDM server**: The full DNS name of the mobile device management server into which the profile enrolls the mobile device.
  Also include the port over which the MDM server communicates.
- **Enable MDM audit logging**: If this option is activated, all actions performed on managed mobile devices are automatically logged. The log file is named “LANrev Audit.log” and is located on the MDM server computer at:
  - macOS: ~/Library/Logs/
  - Windows: %Windir%\Temp
- **Microsoft Exchange Server**: Choose the version of the Exchange server you want to use for Windows Phone MDM. If you do not want to manage Windows Phone devices, choose **None**. (This disables the following three items.)
- **Exchange Server**: Enter in this field the Internet address for the Exchange server you want to use.
- **Username**: Enter the username of an account on the Exchange server. Depending on the version of Exchange you are using, the account must have certain privileges.
  Exchange 2007 accounts must have all of these privileges:
  - View-only administrator
  - Recipient administrator
  - Organization administrator
  - Server administrator
  - Local administrator (for the Exchange server used)

  Exchange 2010 accounts must have all of these privileges:
  - Server management
  - Organization management
  - Recipient management

  Irrespective of the Exchange version, the account you specify must be a member of the Admin group on the computer on which LANrev Server is running.
- **Password**: Enter in this field the password name of the specified account.
- **Query devices for**: These checkboxes determine the information from the managed mobile devices that administrators can view:
  - **General settings**: Administrators can view the general settings of an administered mobile device.
  - **Security settings**: Administrators can view the security-related settings of an administered mobile device.
  - **Network settings**: Administrators can view the network settings of an administered mobile device.
  - **Restrictions**: Administrators can view the restrictions in effect on an administered mobile device.
  - **Configuration profiles**: Administrators can view the configuration profiles installed on an administered mobile device. This setting can only be changed when

Configuration profiles is unchecked in the **Add and remove** section (see below).

- **Applications**: Administrators can view the applications that are installed on the mobile device. This includes both applications from an app store and enterprise applications.
- **Provisioning profiles**: Administrators can view the provisioning profiles installed on an administered mobile device. This setting can only be changed when **Provisioning profiles** is unchecked in the **Add and remove** section (see below).

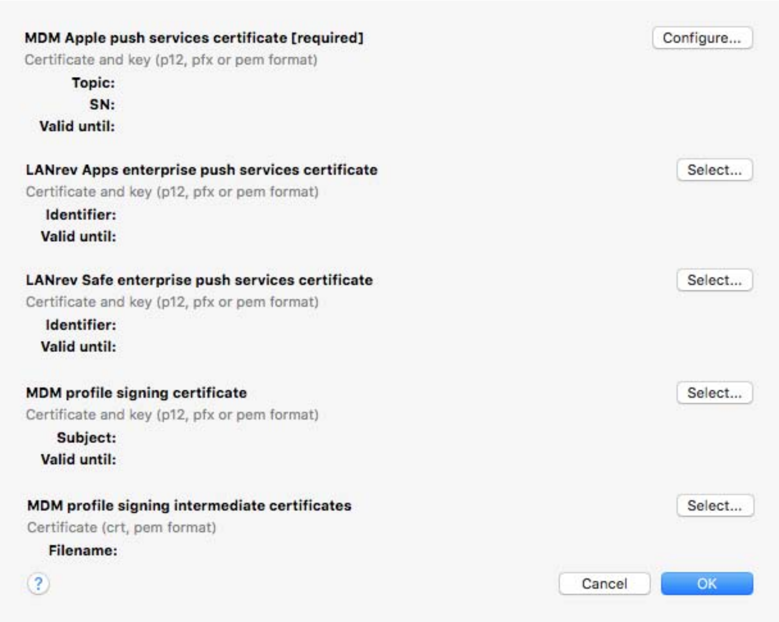
- **Add and remove**: These checkboxes determine the which kind of profiles administrators can delete from the device or add to it:
    - **Configuration profiles**: The administrators can add or delete configuration profiles. Only administrators with the Modify Mobiel Device Configuration Profiles privilege can do so.
    - **Provisioning profiles**: The administrators can add or delete provisioning profiles. Only administrators with the Modify Mobile Applications privilege can do so.
    - **Applications**: The administrators can install apps on the device using the **Install Application** command and delete them using **Delete Application**. This feature is not available for devices running iOS 4.x.
- **Security**: These checkboxes determine the which kind of security-related operation the administrators with the Manage Mobile Devices privilege can perform on the mobile device:
    - **Change device password**: The administrators can set a new password for the device.
    - **Erase device**: The administrators can remotely erase the entire contents of the mobile device.
      This resets the device to its factory condition. Note that this also removes the MDM settings from the device, so that it is no longer possible to access it from LANrev.
      Change settings: The administrators can remotely change certain settings on the mobile device, such as roaming options. In contrast to specifying these settings via profiles, the settings are changed directly and can be changed back by the user of the managed device.
- **Certificates**: This section displays the expiration times of the specified push and MDM signing certificates. Clicking the **Configure** button opens the **Push Services Certificates** dialog (see “Push Services Certificates dialog” on page 791), in which you can see more information on the certificates and select new ones.
- **Device contact interval**: The interval in which the MDM server sends a request to managed mobile devices to contact the server and updates its status.
  These contact requests are sent through Apple’s notification servers and are subject to a timeout on these servers; that is, when there is no contact to the mobile device for a certain time, the contact request is removed without having been delivered to the device. The length of the timeout is unknown but believed to be a few days. We therefore recommend to set the contact interval no higher than 48 hours to ensure that the

timeout period does not cause contact requests to fail, for example, for devices that are switched off for long periods of time.

- **Update device information**: If this option is checked, the information about the device stored in the LANrev database is updated each time the device contacts the MDM server. (This information includes data on hardware, operating system, network used, and installed software.)
  If the option is off, the information stored on the device is never updated.
- **Only update basic information**: If this option is checked, automatic device information updates include only basic device information, not data about security, applications, profiles and so on.
  This option is relevant only if **Update device information** is checked.
- **Apple VPP licensing accounts**: This section lists the number of accounts for Apple's volume purchasing program (VPP) that have been configured in LANrev.
  Clicking **Configure** opens the **Apple VPP Licensing Accounts** dialog (see "Apple VPP Licensing Accounts dialog" on page 792) in which you can add or remove accounts. This button is only available to administrators with the **Change VPP Account Settings** privilege.
  A warning icon ⚠ beside the button indicates that at least one of the currently configured VPP accounts is being managed by a different tool (see "Setting up VPP license management" on page 211 for background information) or has other issues. Click the **Configure** button for details.
- **Apple device enrollment program**: This section lists the number of accounts for Apple's device enrollment program that have been configured in LANrev.
  Clicking **Configure** opens the **Apple Device Enrollment Program Accounts** dialog (see "Apple Device Enrollment Program Accounts dialog" on page 794) in which you can add or remove accounts. This button is only available to administrators with the **Change Device Enrollment Program Account Settings** privilege.
- **Samsung KNOX accounts**: This section lists the Samsung KNOX accounts that have been configured in LANrev.
  Clicking **Configure** opens the **Samsung KNOX Accounts** dialog (see "Samsung KNOX Accounts dialog" on page 794) in which you can add or remove accounts. This button is only available to administrators with the **Modify Samsung KNOX Accounts** privilege.

Push Services Certificates dialog

This dialog is opened by clicking the **Configure** button in the **Certificates** section of the **MDM** server settings tab. (This button is available only to superadministrators.)



MDM Apple push services certificate [required]
Certificate and key (p12, pfx or pem format)
Topic:
SN:
Valid until:

LANrev Apps enterprise push services certificate
Certificate and key (p12, pfx or pem format)
Identifier:
Valid until:

LANrev Safe enterprise push services certificate
Certificate and key (p12, pfx or pem format)
Identifier:
Valid until:

MDM profile signing certificate
Certificate and key (p12, pfx or pem format)
Subject:
Valid until:

MDM profile signing intermediate certificates
Certificate (crt, pem format)
Filename:

The dialog displays the currently loaded certificates and lets you load new certificates:

- **MDM Apple Push Services certificate**: Clicking the **Configure** button lets you create or select a certificate for validating the MDM server for push notifications.
Clicking the button opens an assistant in which you can either select an existing certificate (which must be located as a file on your computer) or create a new one.
- **LANrev Apps enterprise push services certificate**: The certificate needed for the server to inform devices of new and updated enterprise applications available in the LANrev Apps app and send them messages.
This certificate is needed only for the enterprise version of LANrev Apps, not for the version downloaded from the App Store.
You can obtain an app push services certificate from Apple’s iPhone Provision Portal.
- **LANrev Safe enterprise push services certificate**: The certificate needed for the server to inform devices of new and updated media available in the LANrev Safe app.
This certificate is needed only for the enterprise version of LANrev Safe, not for the version downloaded from the App Store.
You can obtain an app push services certificate from Apple’s iPhone Provision Portal.
- **MDM profile signing certificate**: The signing certificate for signing the bootstrap file and configuration profile for MDM enrollment. When you select the certificate, you must also specify the private key.

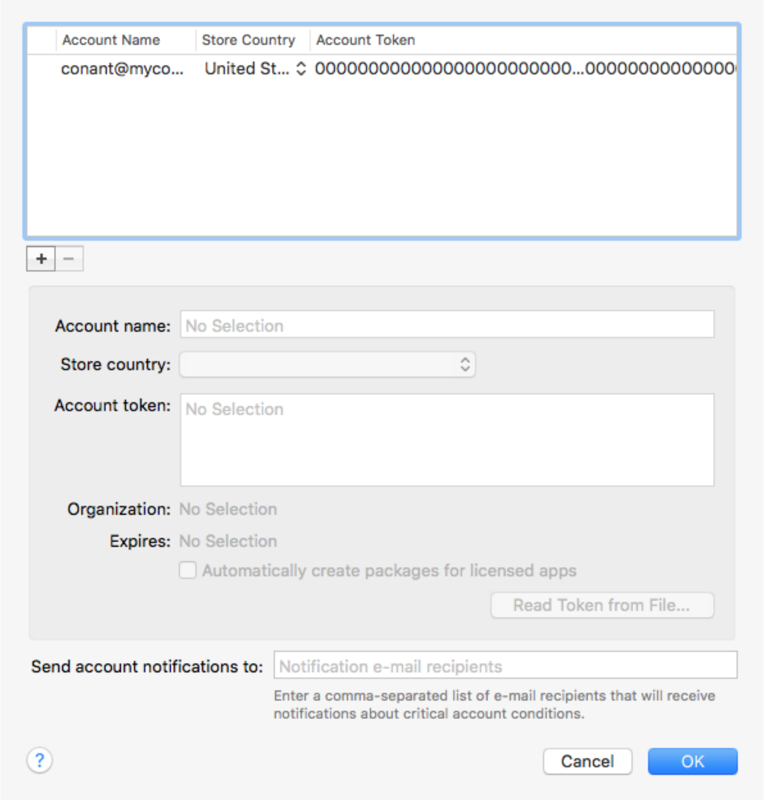
This certificate is used only for enrolling devices into MDM. Enrolling works also without the certificate, but then user of mobile devices encounter alerts about untrusted certificates during the enrollment process.
If the certificate requires an additional intermediate certificate, you must specify that as well (see below). Contact the issuing authority if you are unsure.

- **MDM profile signing intermediate certificate**: The intermediate certificate required by the signing certificate if any.

To choose a certificate (other than the push services certificate), click the corresponding **Select** button. To remove a certificate, press the Option key and click **Remove**.

Apple VPP Licensing Accounts dialog

This dialog is opened by clicking the **Configure** button in the **Apple VPP licensing accounts** section of the **MDM** server settings tab.



	Account Name	Store Country	Account Token
	conant@myco...	United St... ⇕	000000000000000000000000...00000000000000

Account name: No Selection
Store country:
Account token: No Selection
Organization: No Selection
Expires: No Selection
□ Automatically create packages for licensed apps

Send account notifications to: Notification e-mail recipients
Enter a comma-separated list of e-mail recipients that will receive notifications about critical account conditions.

The dialog contains these elements:

- **Apple VPP licensing accounts configured**: This list contains all your organization’s VPP accounts that have been configured in LANrev.
The leftmost column is a status column. If it is empty, there are no issues with that account. If there are issues, it displays one of these icons:

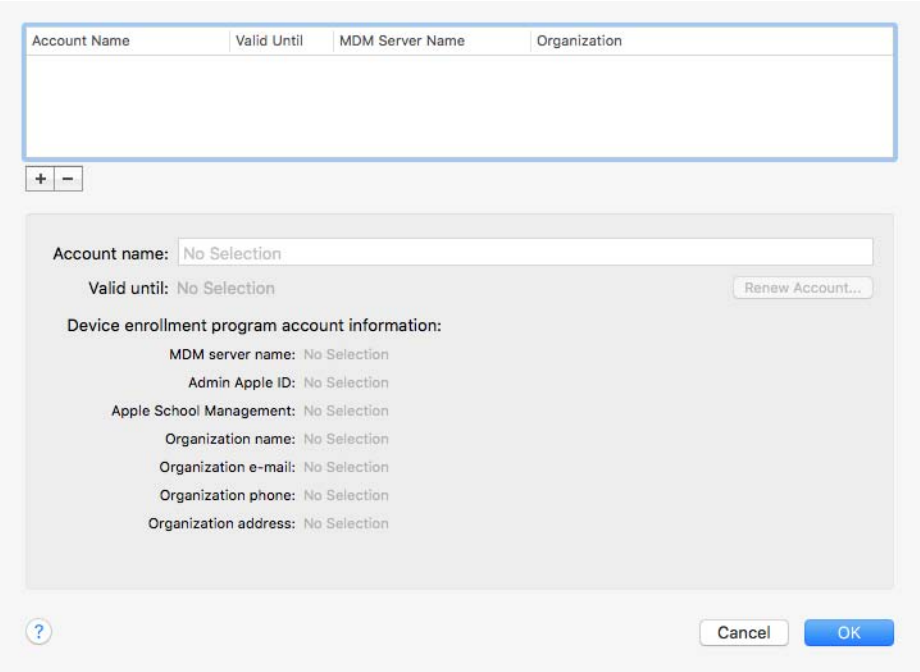
  - ⚠️: The account is disabled because it is currently being managed by a different tool, or the account token is invalid or has expired.
  - 🧹: The account is currently being reset.
  - 🚫: The account is scheduled to be deleted. The account is no longer editable.

  You can add and remove accounts using the **+** and **-** buttons below the list.

- **Account name**: The name under which the account is listed in LANrev. You can choose this name freely.
- **Store country**: The country of the App Store to which the account belongs.
- **Account token**: The identification token for the account which you have recieved from Apple.
  Clicking the **Read Token from File** button lets you import a token file.
- **Automatically create packages for licensed apps**: If this option is checked, LANrev automatically creates a package for any application or book for which you have purchased a volume license. When you later purchase licenses for additional apps or books, LANrev creates packages for them as well.
- **Send account notifications to**: The e-mail addresses of any people that you want LANrev to notify when there are serious issues with the VPP account, such as the account is claimed by a different server.
  To notify multiple people, enter their e-mail addresses separated by commas. Leave the field empty to not send any notifications.

Apple Device Enrollment Program Accounts dialog

This dialog is opened by the **Configure** button in the **Apple device enrollment program section** of the **MDM** server settings tab.



Account Name	Valid Until	MDM Server Name	Organization

Account name: No Selection

Valid until: No Selection

Device enrollment program account information:

MDM server name: No Selection

Admin Apple ID: No Selection

Apple School Management: No Selection

Organization name: No Selection

Organization e-mail: No Selection

Organization phone: No Selection

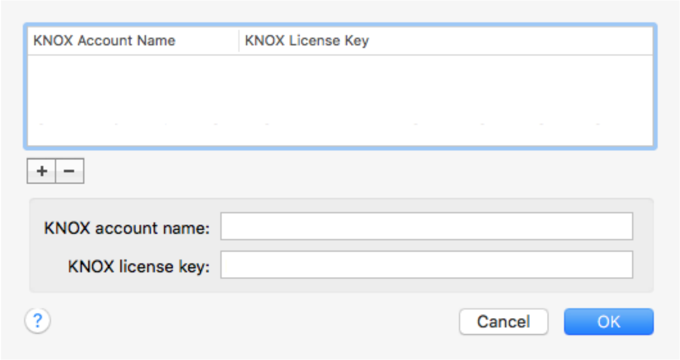
Organization address: No Selection

The dialog contains these elements:

- The list at the top of the dialog contains all your organization’s device enrollment program accounts that have been configured in LANrev. You can add and remove accounts using the **+** and **-** buttons below the list.
  Clicking the **+** button opens an assistant that guides you through the steps necessary to set up an account.
- **Account name**: The name under which the account is listed in LANrev. You can edit this name as desired.
- The rest of the dialog displays the expiration date and other details of the account as well as information about your organization you provided when setting up the account.
- **Renew Account**: Clicking this button lets you update the account information stored in LANrev. In particular, you can import a new credentials file when you have renewed the account with Apple.

Samsung KNOX Accounts dialog

This dialog is opened by the **Configure** button in the **Samsung KNOX accounts** of the **MDM** server settings tab. It lets you specify the KNOX accounts that can be used to create KNOX workspaces on managed mobile devices.



KNOX account name:

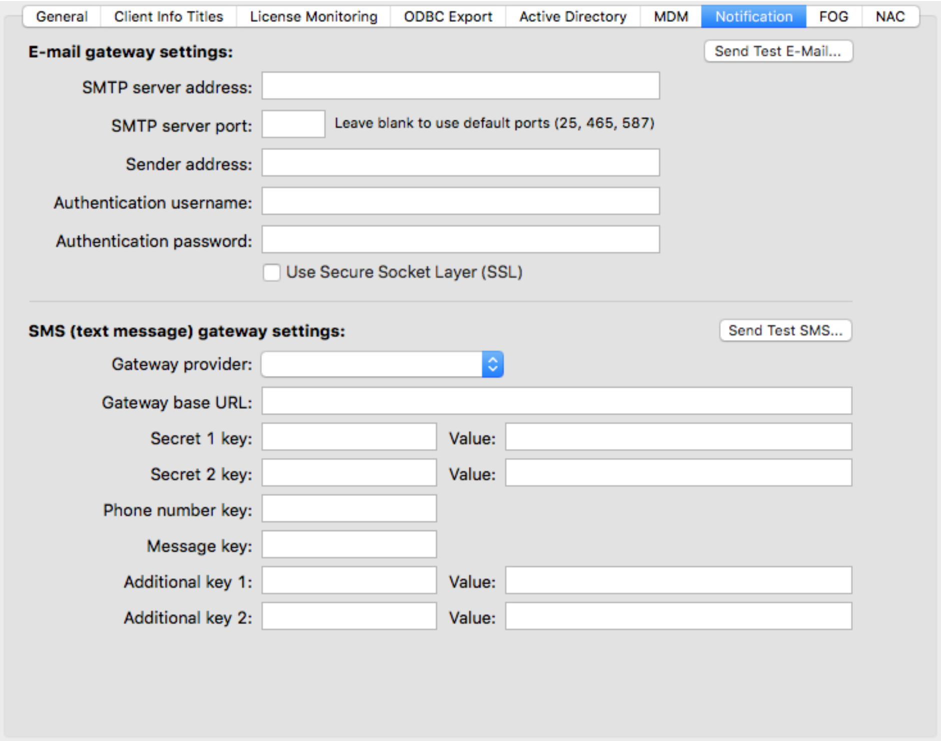
KNOX license key:

The dialog contains these elements:

- The list at the top of the dialog contains all your organization's KNOX accounts that have been configured in LANrev. You can add and remove accounts using the **+** and **-** buttons below the list.
- **KNOX account name**: The name under which the account is listed in LANrev. You can edit this name as desired.
- **KNOX license key**: The account license key you have received from Samsung.

Notification

The **Notification** tab of the **Server Settings** dialog contains the SMTP and SMS server settings required for sending e-mails and SMS (texts) to managed mobile devices and notifications about issues in automatic database processes to administrators.



Leave blank to use default ports (25, 465, 587)

□ Use Secure Socket Layer (SSL)

The tab contains these elements:

- **Send Test E-Mail**: When all fields in the **E-mail gateway settings** section of the tab are filled in, clicking this button sends a test e-mail to verify that the setup is working.
- **SMTP server address**: The IP address or DNS name of the SMTP server over which e-mails are to be sent.
- **SMTP server port**: The port on which the SMTP server accepts incoming connections. If this field is left empty, LANrev uses the standard ports (25 or 587, for unsecure and secure connections, respectively).
- **Sender address**: The "From" address used in the e-mails. Note that some SMTP servers do not allow custom sender addresses and replace them with the address of the account used for sending the e-mail.
- **Authentication username**: If the SMTP server requires a username and password for authentication before accepting e-mails, enter the username in this field.
- **Authentication password**: The password for the SMTP server account.
- **Use Secure Socket Layer (SSL)**: If this option is checked, LANrev uses SSL to communicate with the SMTP server.
- **Send Test SMS**: When all fields in the **SMS (text message) gateway settings** section of the tab are filled in, clicking this button sends a test text message to verify that the setup is working.
- **Gateway provider**: This pop-up menu contains predefined providers. Choosing one fills all fields with the appropriate

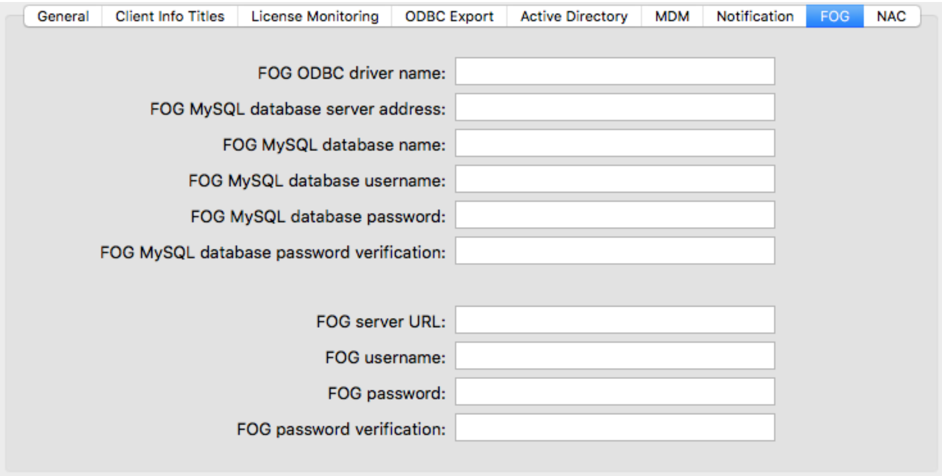
settings to send texts though that provider. (You can still edit the values.) You still need to enter the information for the **Value** fields, which are specific to your account.
Choosing **Custom** lets you specify the for a provider that is not listed. The details for the required keys and values must come from your provider.

- **Gateway base URL**: The constant part of the URL over which you can send texts over your provider's gateway.
  LANrev adds the keys and values discussed below to this base URL and sends the result to the gateway. (It expects the gateway to return the HTTP code 200; any other reply is considered to indicate an error.)
- **Secret 1 key**: The keyword for the first item of information you need to identify yourself with the gateway (for example, "account_name").
  Enter the information itself (in this example, the name of your account) in the **Value** field to the right. This information is encrypted before being sent to the gateway.
- **Secret 2 key**: The keyword for the second item of information you need to identify yourself with the gateway (for example, "password").
  Enter the information itself (in this example, the password for your account) in the **Value** field to the right. This information is encrypted before being sent to the gateway.
- **Phone number key**: The keyword that the gateway specifies for submitting the target phone number.
- **Message key**: The keyword that the gateway specifies for submitting the text of the SMS you are sending.
- **Additional key 1**: An optional keyword for additional information that your provider supports or requires.
  Enter the information itself in the **Value** field to the right.
- **Additional key 2**: An optional keyword for additional information that your provider supports or requires.

  Enter the information itself in the **Value** field to the right.

FOG

The **FOG** tab of the **Server Settings** dialog lets you specify the settings for reinstalling administered computers with the **Reinstall Windows Computer** command.



FOG ODBC driver name:

FOG MySQL database server address:

FOG MySQL database name:

FOG MySQL database username:

FOG MySQL database password:

FOG MySQL database password verification:

FOG server URL:

FOG username:

FOG password:

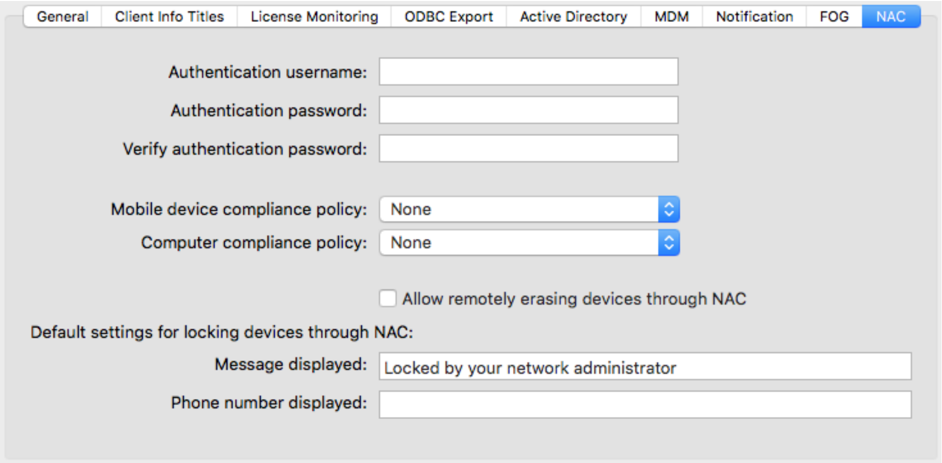
FOG password verification:

The tab contains these elements:

- **FOG ODBC driver name**: The name of the ODBC driver which the LANrev server computer is to access the MySQL database of the FOG server.
- **FOG MySQL database server address**: The IP address or DNS name of the computer on which the FOG MySQL database server is running.
- **FOG MySQL database name**: The name of the MySQL database used by the FOG software.
- **FOG MySQL database username**: The account name that LANrev Server is to use to access the FOG MySQL database.
- **FOG MySQL database password**: The password for the account.
- **FOG MySQL database password verification**: The password for the account repeated, to guard against typos.
- **FOG server URL**: The IP address or DNS name of the computer on which the FOG server (that is, the FOG software itself, not the MySQL database server it is using) is running and the path of the FOG management directory on that computer. For example: http://myfogserver.company.com/fog/management/.
- **FOG username**: The account name that LANrev Server is to use to access the FOG server.
- **FOG password**: The password for the account.
- **FOG password verification**: The password for the account repeated, to guard against typos.

NAC

The **NAC** tab of the **Server Settings** dialog lets you specify the access credentials for a Cisco ISE server, the criteria by which the compliance of a device is determined, and settings related to locking and erasing devices.



Authentication username:

Authentication password:

Verify authentication password:

Mobile device compliance policy: None

Computer compliance policy: None

□ Allow remotely erasing devices through NAC

Default settings for locking devices through NAC:

Message displayed: Locked by your network administrator

Phone number displayed:

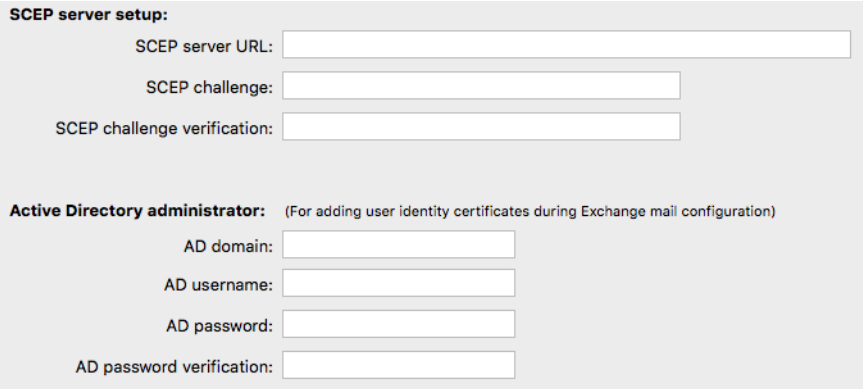
The tab contains these elements:

- **Authentication username**: The username the Cisco ISE server must provide to be able to send compliance queries.
- **Authentication password**: The password that the Cisco ISE server must provide. Repeat the password in the **Verify authentication password** field.
- **Mobile device compliance policy**: The policy for determining the compliance of mobile devices. All mobile devices that are part of this policy are considered compliant for purposes of getting network access through the Cisco ISE system. All mobile devices that are not part of this policy are considered noncompliant.
- **Computer compliance policy**: The computer group for determining the compliance of mobile devices. All computers that are part of this group are considered compliant for purposes of getting network access through the Cisco ISE system. All computers that are not part of this group are considered noncompliant.
- **Allow remotely erasing devices through NAC**: If this option is checked, devices can be erased using Cisco ISE. If the option is unchecked, LANrev does not support such erasing.
- **Message displayed**: The default message that is displayed on a device that is locked using Cisco ISE. This field can be left empty.
- **Phone number displayed**: The default contact phone number that is displayed on a device that is locked using Cisco ISE. This field can be left empty.

Certificate Settings

The **Certificate Settings** category in the **Server Center** window lets you specify the access credentials that LANrev Server needs for SCEP (Simple Certificate Enrollment Protocol) support.

Selecting the category displays the required input fields in the main area of the **Server Center** window:



SCEP server setup:

SCEP server URL:

SCEP challenge:

SCEP challenge verification:

Active Directory administrator: (For adding user identity certificates during Exchange mail configuration)

AD domain:

AD username:

AD password:

AD password verification:

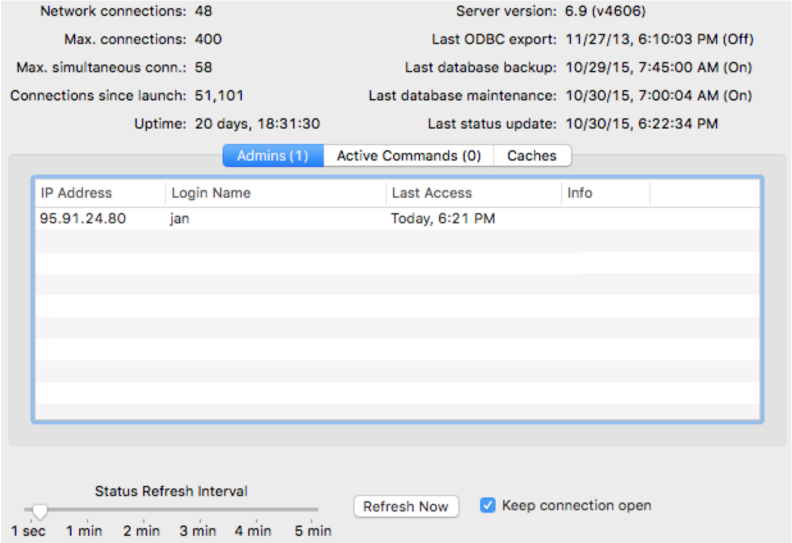
The dialog contains these elements:

- **SCEP server URL**: The DNS name or IP address of the SCEP server.
- **SCEP challenge**: The challenge with which LANrev Server can verify itself as a legitimate client to the SCEP server.
- **SCEP challenge verification**: The same challenge, to guard against typos.
- **AD domain**: The Active Directory domain in which LANrev Server has an account.
- **AD username**: The username of the Active Directory account that LANrev Server is to use. This must be an account with administrator privileges.
- **AD password**: The password of the Active Directory account.
- **AD password verification**: The same password, to guard against typos.

Server Monitor

The **Server Monitor** category in the **Server Center** window lets you view current server activities.

Selecting the category displays a range of information in the main area of the **Server Center** window:



Network connections: 48
Max. connections: 400
Max. simultaneous conn.: 58
Connections since launch: 51,101
Uptime: 20 days, 18:31:30

Server version: 6.9 (v4606)
Last ODBC export: 11/27/13, 6:10:03 PM (Off)
Last database backup: 10/29/15, 7:45:00 AM (On)
Last database maintenance: 10/30/15, 7:00:04 AM (On)
Last status update: 10/30/15, 6:22:34 PM

IP Address	Login Name	Last Access	Info
95.91.24.80	jan	Today, 6:21 PM	

Status Refresh Interval: 1 sec

☑ Keep connection open

The monitor contains these elements:

- **Network connections**: The number of active network connections of the server.
- **Max. connections**: The maximum number of connections that is configured on this server. (This is the total number of connections; the **Maximum number of connections** field in the LANrev Server's **Server Settings** dialog specifies only the number of outgoing agent connections.)
- **Max. simultaneous conn.**: The maximum number of simultaneous network connections on this server since it was last launched.
- **Connections since launch**: The total number of network connections on this server since it was last launched.
- **Uptime**: The amount of time that has elapsed since the last time the server was launched.
- **Server version**: The version number of the server.
- **Last ODBC export**: The time when the last ODBC export was performed. If ODBC exports are not activated, "Disabled" is displayed.
- **Last database export**: The time when the last database backup was performed. If database backups are not activated, "Disabled" is displayed.
- **Last database maintenance**: The time when the database maintenance was performed. If database maintenance is not activated, "Disabled" is displayed.
- **Last status update**: The time when the information displayed in the server monitor was last updated.
- **Admins**: The number of administrators who have been logged in on this server since the last time the server was restarted (including administrators who are currently logged in). Clicking this tab displays an overview of these admins.
- **Active commands**: The number of commands that are currently being executed on the server.

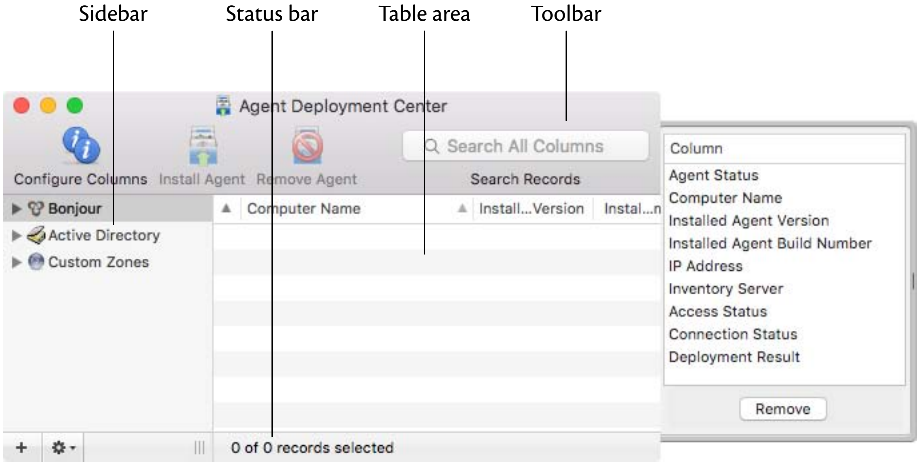
Clicking this tab displays a list of the commands.

- **Caches**: Clicking this tab displays a breakdown of the requests by type as well as the maximum numbers of agent request or inventory requests that were cached at the same.
- **Status Refresh Interval**: The interval for automatic updates of the information displayed in the server monitor.
- **Refresh Now**: Clicking this button updates the the information displayed in the server monitor irrespective of the refresh interval.
- **Keep connection open**: If this option is checked, the connection to the server is not closed after the data has been refreshed. This helps reduce network overhead in case of frequent updates.

Chapter 25 Agent Deployment Center

The Agent Deployment Center is a module of the LANrev system that lets you install and update agents on supported computers in the network without having to physically visit these computers. It is controlled from the **Agent Deployment Center** window in LANrev Admin.

NOTE The Agent Deployment Center can be used only by administrators with the **Deploy Agents** right. See “New Administrator” on page 758 for details.



The elements of the **Agent Deployment Center** window are described below:

- **Toolbar** (page 804)
- **Table columns** (page 805)
- **Sidebar** (page 806)
- **Action menus** (page 806)
  - **New Custom Zone** (page 807)
  - **Edit Custom Zone** (page 810)
  - **Remove Custom Zone** (page 810)
  - **Search Zone** (page 811)
  - **Cancel Search** (page 811)
  - **Refresh** (page 811)
  - **New Smart Group** (page 811)
  - **Edit Smart Group** (page 812)
  - **Remove Smart Group** (page 812)
  - **Import Zones File** (page 812)
- **Context menu** (page 813)
  - **Copy** (page 813)
  - **Copy “<information item>”** (page 814)
  - **New Smart Group from “<information item>”** (page 814)
  - **Install Agent** (page 814)
  - **Remove Agent** (page 816)
  - **Set Inventory Server** (page 817)

- **Refresh Status** (page 820)

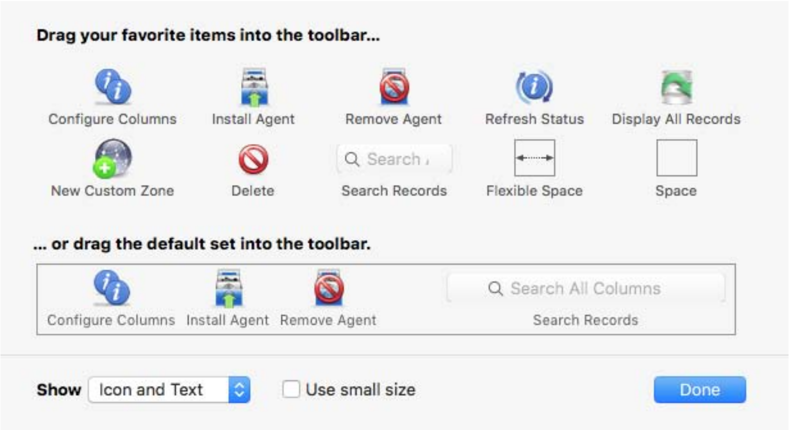
The + button in the lower left-hand corner is not separately described; clicking it creates a new custom zone as if you had chosen **New Custom Zone**.

Toolbar

The **Agent Deployment Center** window has a toolbar that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar can contain these elements:



The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** through **Print**).

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Install Agent

The **Install Agent** button installs LANrev Agent on the selected computers.

It has the same effect as the **Install Agent** command described on page 814.

Remove Agent

The **Remove Agent** button uninstalls LANrev Agent from the selected computers.

It has the same effect as the **Remove Agent** command described on page 816.

Refresh Status

The **Refresh Status Info** button updates the information display for the selected network devices.

It has the same effect as the **Refresh Status** command described on page 820.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

It has the same effect as the **Display All Records** command described on page 397.

New Custom Zone

The **New Custom Zone** button opens the dialog for specifying a new smart computer group.

It has the same effect as the **New Custom Zone** command described on page 807.

Delete

The **Delete** button deletes the selected objects from the window.

It has the same effect as the **Delete** command described on page 392.

Search Records

The **Search Records** field lets you quickly restrict the display to records that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Pressing Return executes the search.

Table columns

The main table in the **Agent Deployment Center** window displays network devices found in the zones that have been searched. The columns in the table display information items that are mostly described in “Agent Deployment Center” on page 890.

In addition, to the named columns displaying information items, the first column indicates the status of the device:

🟢 A green dot indicates that the current version of LANrev Agent is installed on the computer.

🟡 A yellow dot indicates that an outdated version of LANrev Agent is installed on the computer.

🔴 A red dot indicates that LANrev Agent is not installed on the computer but could be installed.

⚪ A grey dot indicates a device that does not support LANrev Agent, that is, one of the following:

- A computer with an incompatible operating system (that is, Windows when you are installing from a macOS Admin)
- A non-computer device (such as a router or printer)
- A computer that could support LANrev Agent but on which the required connection protocol (SSH for the macOS Admin) is disabled.

Sidebar

The **Agent Deployment Center** window contains a sidebar with predefined and custom zones reflecting the network structure:

- **Bonjour**: All Bonjour (previously known as Rendezvous, an implementation of ZeroConfig) zones.
- **Active Directory**: All Active Directory zones in your network. If there are no Active Directory servers in your network, this sidebar entry is missing.
- **Custom zones**: All zones that you have defined.

Clicking on any zone displays the network devices that have been found in that zone.

Action menus

The action menu of the **Agent Deployment Center** window contains commands for managing custom zones.

The commands are described in detail in the following sections.

- “New Custom Zone” on page 807
- “Edit Custom Zone” on page 810
- “Remove Custom Zone” on page 810
- “Search Zone” on page 811
- “Cancel Search” on page 811
- “Refresh” on page 811
- “New Smart Group” on page 811
- “Edit Smart Group” on page 812

- “Remove Smart Group” on page 812
- “Import Zones File” on page 812

New Custom Zone

The **New Custom Zone** command creates a new zone in the **Custom Zones** section and lets you specify automatic scanning of this zone for computers and installation of agents on them.

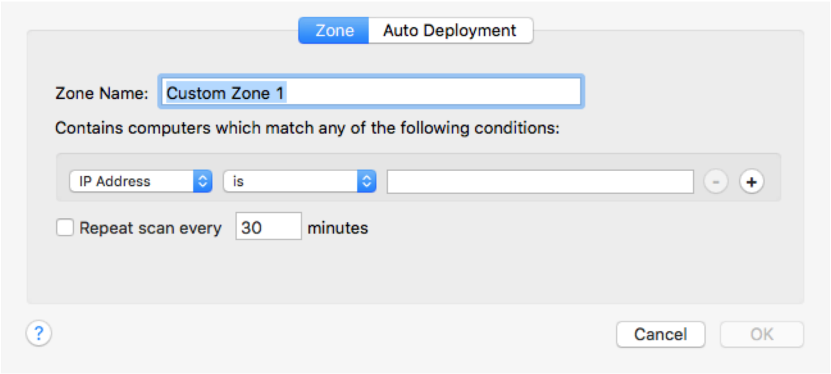
Choosing the command opens the **Custom Zone** dialog, which has two panes:

- **Zone**
- **Auto Deployment**

Both are described below.

Zone

The **Zone** pane of the **Custom Zones** dialog lets you define a virtual network zone that LANrev uses to search for computers and for deploying agents:



Zone Name: Custom Zone 1

Contains computers which match any of the following conditions:

IP Address | is

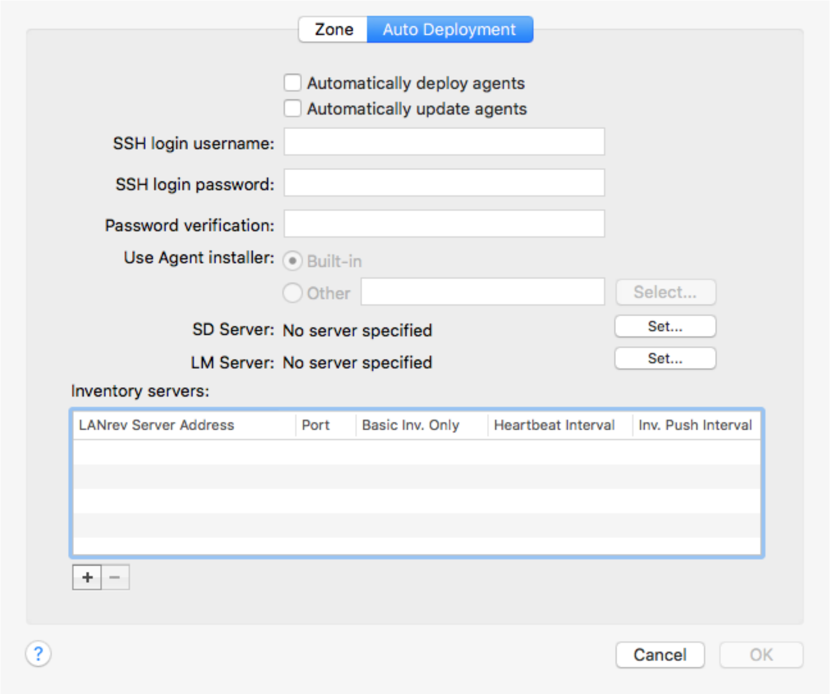
□ Repeat scan every 30 minutes

The pane contains these elements:

- **Zone Name**: The name under which your custom zone will be displayed.
- Condition area: Choose between including computers in zones by IP address or by host name. For IP addresses, you can choose between single addresses or address ranges by means of the second pop-up menu. The text field lets you enter the address or name to look for.
  The **+** and **–** buttons let you add new conditions or remove existing ones. A zone includes all computers that match any of the specified conditions (Boolean OR).
- **Repeat scan every**: Check this option and enter a number of minutes to have LANrev scan this zone automatically for new computers in the specified interval.
  Note: This setting is particularly useful in combination with automatic deployment of agents, as described below.

Auto Deployment

The **Auto Deployment** pane of the **Custom Zones** dialog lets you specify whether and how to automatically install agents on computers found in the zone on which no agent is present:



□ Automatically deploy agents
□ Automatically update agents

SSH login username:

SSH login password:

Password verification:

Use Agent installer: ● Built-in ○ Other

SD Server: No server specified

LM Server: No server specified

Inventory servers:

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

NOTE Automatic installation is possible only on computers running the same operating system as your administrator workstation (or to Linux from macOS). That is, if you are running LANrev Admin on macOS, you can automatically deploy only to client computers running macOS or Linux. And from LANrev Admin for Windows, automatic deployment is only possible to computers running Windows.

The pane contains these elements:

- **Automatically deploy agents**: If this option is checked, LANrev automatically installs LANrev agents on computers found in this zone that do not already have them.
- **Automatically update agents**: If this option is checked, LANrev automatically updates any LANrev agents found on computers in this zone when they are outdated.
- **SSH login username**: The username that is to be used for SSH login on the selected computers. The account names (as well as the passwords) are case-sensitive. You must use the abbreviated username.
- **SSH login password**: The password for the SSH account.
- **Password verification**: Re-enter the password to guard against typos.
- **Use Agent installer**: Choose **Built-in** if the installer embedded in LANrev Agent is to be used for installing the Agent. Choose **Other** to specify a custom installer using the **Select** button.

- **SD Server**: The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described below in “Server Properties dialog” on page 810.
- **SM Server**: The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 810.
- **Inventory servers**: This table lists all known LANrev inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.

  The list contains these columns:
  - **LANrev Server Address**: The IP address or DNS name of the server.

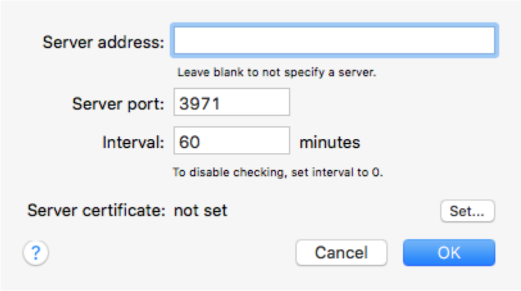
    Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).
  - **Port**: The port over which the server communicates with agents.
  - **Basic Inv. Only**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
  - **Heartbeat Interval**: The interval in which the agents are to contact the server to let it know that they are still available.

    Note: This interval should not be longer than the Agent Offline Threshold setting of the LANrev server. (See “Server Settings” on page 780 for details.)
  - **Inv. Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

  Double-clicking a server displays a dialog for editing its settings. The dialog is described in “Inventory Server Properties dialog” on page 819.
- Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described in “Inventory Server Properties dialog” on page 819. Clicking the **–** button removes the selected server.

Server Properties dialog

The **Server Properties** dialog lets you specify a software distribution or license monitoring server.



Server address:

Leave blank to not specify a server.

Server port: 3971

Interval: 60 minutes

To disable checking, set interval to 0.

Server certificate: not set

The dialog contains these elements:

- **Server address**: The IP address or DNS name of the server. *Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer's network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).*
- **Server port**: The port over which the server communicates with agents.
- **Interval**: The interval in which the agents are to check the software distribution server for new installation packages or check the license monitoring server for changes to the license specifications, respectively.
- Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of the **Save Certificate** button in the **Server Settings** section of the Server Center, as described in "Exporting a server certificate" on page 21.)
  The certificate is required for specifying the server.

Edit Custom Zone

The **Edit Custom Zone** command lets you edit an existing custom zone.

Choosing the command opens the **Custom Zone** dialog that is described in "New Custom Zone" on page 807.

Remove Custom Zone

The **Remove Custom Zone** command deletes a custom zone.

Choosing the command deletes the selected custom zones. A confirmation alert is displayed first.

Search Zone

The **Search Zone** command searches the selected zone for network devices.

Choosing the command makes LANrev Admin scan the network range specified in the zone for client computers.

While a zone scan is in progress, the command changes to **Cancel Search**, described below.

NOTE It takes approximately a tenth of the server connection timeout set in the **Preferences** dialog (see "Preferences" on page 366) to scan one IP address when there is no device present at that address; that is, about a second at the default timeout of ten seconds. When a device is present, scanning is usually faster.

Cancel Search

The **Cancel Search** command terminates the current scan of the selected zone.

This command replaces the **Search Zone** command, described above, while a zone scan is under way.

Refresh

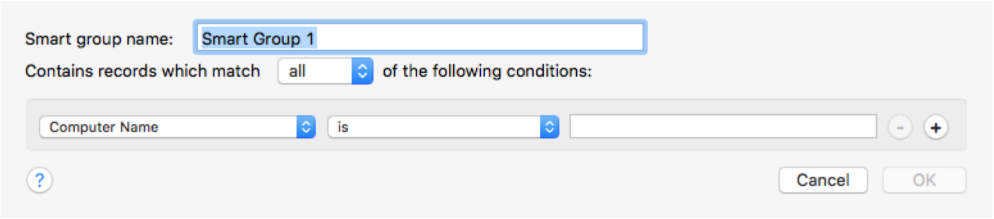
The **Refresh** command recreates the Windows Networking domains and workgroups and redisplays the computers within them.

This command is only available when the **Windows Networking** category is right-clicked, which is not supported in LANrev Admin for macOS.

New Smart Group

The **New Smart Group** command creates a new smart group for found network devices.

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Group 1

Contains records which match all of the following conditions:

Computer Name is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched.
  - The pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

NOTE Devices may appear multiple times in smart groups when they were found using more than one method (for example, through Bonjour and by scanning an IP range.)

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the **Smart Group** dialog described in “New Smart Group” on page 811.

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Import Zones File

The **Import Zones File** command lets you import zones definitions from a text file.

Choosing the command adds the zones specified in the text file to the currently existing zones. To avoid ending up with duplicate zones, you may need to delete existing zones before importing the file.

Files may include the following specifications:

- Zone names are standard text on a line by themselves.
  Zone names must contain at least one character.
  The specification of what is to be included in the zone follows in the lines below the zone name. Anything up to the next zone name is considered to belong to the zone's definition.
  Available specifications include single addresses, address ranges, subnets, and named domains, as described below.
- An IP address indicates a single computer to include in the zone.
  Example: 10.7.23.123
- Two IP addresses divided by a hyphen indicate an address range.
  Example: 10.7.33.1 - 10.7.33.127
- An IP address and a network mask connected by an ampersand indicate a subnet.
  Example: 10.7.23.123 & 255.255.0.0
- Text included in quotation marks is considered a domain.
  Example: "poleposition-sw.com"
- Text following a semicolon (;), number sign (#), or two slashes (/ /) up to the end of the line is considered a comment and is ignored.
  Example: // This is a comment

Context menu

The context menu of the **Agent Deployment Center** window contains commands for installing and uninstalling LANrev Agent and refreshing the display.

The commands are described in detail in the following sections.

- "Copy" on page 813
- "Copy "<information item>"" on page 814
- "New Smart Group from "<information item>"" on page 814
- "Install Agent" on page 814
- "Remove Agent" on page 816
- "Set Inventory Server" on page 817
- "Refresh Status" on page 820

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 392.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (for example, **Copy “Inventory Server”**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Group from “<information item>”

The **New Smart Group from “<information item>”** command lets you create a smart group with prefilled criteria.

Choosing the command opens the **Search Zone** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

Install Agent

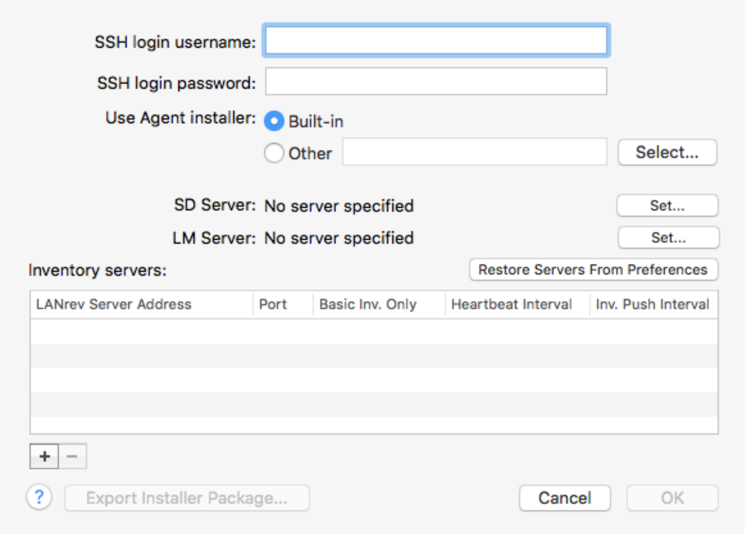
The **Install Agent** command installs LANrev Agent on the selected computers. If an older version of LANrev Agent is already present on the computer, it is updated.

You can install LANrev agents only on the same platform on which your copy of LANrev Admin is running, that is, you cannot deploy Windows agents from macOS or vice versa.

The command is available only if LANrev Agent can be installed on the selected computer.

NOTE SSH must be active on the target computer for this installation to work.

Choosing the command opens the **Agent Deployment Settings** dialog:



SSH login username:

SSH login password:

Use Agent installer: ● Built-in ○ Other

SD Server: No server specified

LM Server: No server specified

Inventory servers:

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

The dialog contains these elements:

- **SSH login username**: The username that is to be used for SSH login on the selected computers. The account names (as well as the passwords) are case-sensitive. You must use the abbreviated username.
- **SSH login password**: The password for the SSH account.
- **Use Agent installer**: Choose whether the installer embedded in LANrev Agent or a custom installer that you provide is to be used for installing the Agent.
  You can create a custom installer using the **Export Installer Package** button in the **Deployment Center** tab of the **Preferences** dialog.
- **Select**: Clicking this button lets you select a custom installer.
- **SD Server**: The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 810.
- **SM Server**: The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 810.
- **Restore Servers from Preferences**: Clicking this button selects the inventory servers that have been specified in the **Deployment Center** pane of the **Preferences** dialog.
- **Inventory servers**: This table lists all known LANrev inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.
  The list contains these columns:
  - **LANrev Server Address**: The IP address or DNS name of the server.
    Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully

qualified DNS names (that is, ones that include the full domain).

- **Port**: The port over which the server communicates with agents.
- **Basic Inv. Only**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
- **Heartbeat Interval**: The interval in which the agents are to contact the server to let it know that they are still available. *Note: This interval should not be longer than the Agent Offline Threshold setting of the LANrev server. (See "Server Settings" on page 780 for details.)*
- **Inv. Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

Double-clicking a server displays a dialog for editing its settings. The dialog is described in "Inventory Server Properties dialog" on page 819.

- Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described in "Inventory Server Properties dialog" on page 819. Clicking the **–** button removes the selected server.
- **Export Installer Package**: Clicking this button lets you save a custom installer package that includes both the server settings you have specified in this dialog as well as the required certificates.
  You can use this installer package in the **Use agent installer** section of this dialog.

Except for the servers to assign, the presets in all fields are specified in the **Preferences** dialog (see page 366).

NOTE If the built-in macOS firewall is active on a client computer, installing LANrev Agent automatically opens the agent port as specified in the **Preferences** dialog (usually port 3970).

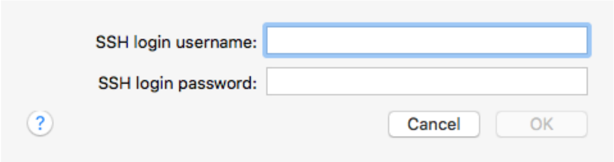
Remove Agent

The **Remove Agent** command removes LANrev Agent from the selected computers.

You can remove LANrev agents only from the same platform on which your copy of LANrev Admin is running, that is, you cannot remove Windows agents from an admin running on macOS or vice versa.

The command is available only if LANrev Agent is installed on the selected computer. It is not available if no agent is present or if SSH is disabled on the target computer.

Choosing the command opens the **Remove Agent** dialog:



The dialog contains these elements:

- **SSH login username**: The username that is to be used for SSH login on the selected computers. The account names (as well as the passwords) are case-sensitive. You must use the abbreviated username.
- **SSH login password**: The password for the SSH account.

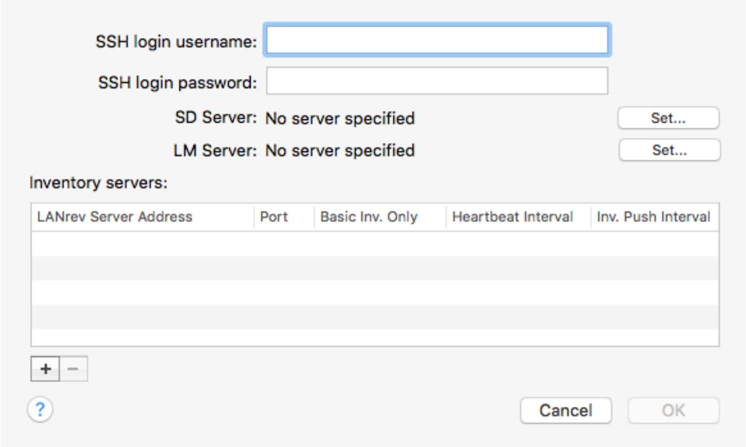
The presets in all fields are specified in the Preferences dialog (see page 366).

Set Inventory Server

The **Set Inventory Server** command assigns LANrev servers to selected computers.

The command is available only if LANrev Agent is installed on a selected computer and remote login is enabled. It is not available if no agent is present or if the selected computer does not run macOS.

Choosing the command opens the **Inventory Server Properties** dialog:



SD Server: No server specified

LM Server: No server specified

LANrev Server Address	Port	Basic Inv. Only	Heartbeat Interval	Inv. Push Interval

The dialog contains these elements:

- **SSH login username**: The SSH username for connecting to the client.

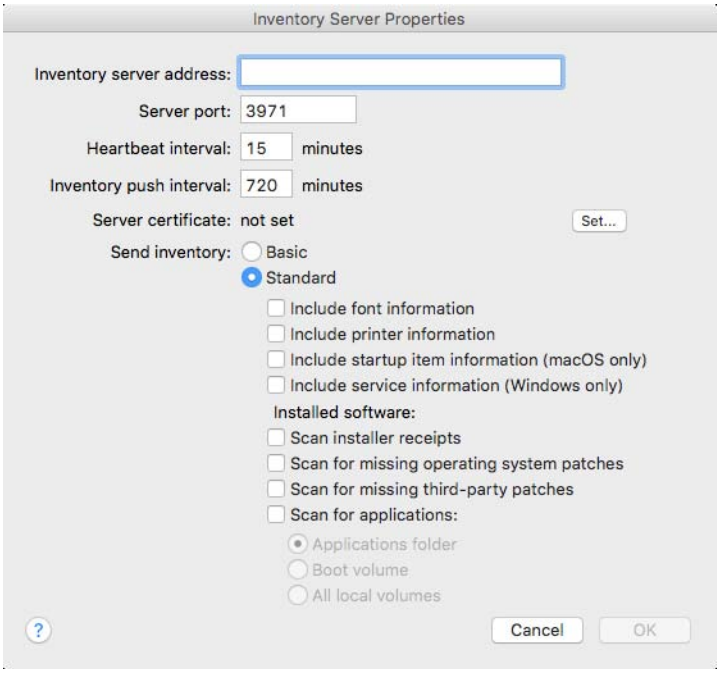
- **SSH login password**: The password for the specified SSH account.
- **SD Server**: The software distribution server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 810.
- **LM Server**: The license monitoring server to be used for this Agent. Clicking **Set** lets you specify a server, as described in “Server Properties dialog” on page 810.
- **Inventory servers**: This table lists all known LANrev inventory servers. Any servers selected in this list are assigned to the selected agents when you click **OK**.
  The list contains these columns:
  - **LANrev Server Address**: The IP address or DNS name of the server.
    Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).
  - **Port**: The port over which the server communicates with agents.
  - **Basic Inv. Only**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
  - **Heartbeat Interval**: The interval in which the agents are to contact the server to let it know that they are still available.
    Note: This interval should not be longer than the Agent Offline Threshold setting of the LANrev server. (See “Server Settings” on page 780 for details.)
  - **Inv. Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)

  Double-clicking a server displays a dialog for editing its settings. The dialog is described below.
  Clicking the **Up** button moves the selected entry up in the list, clicking the **Down** button moves it down.

Clicking the **+** button adds a new server to the list. A dialog is displayed in which you can edit the server's setting; the dialog is described below. Clicking the **–** button removes the selected server.

Inventory Server Properties dialog

The **Inventory Server Properties** dialog lets you specify details about how an agent interacts with an inventory server.



Inventory Server Properties

Inventory server address:

Server port: 3971

Heartbeat interval: 15 minutes

Inventory push interval: 720 minutes

Server certificate: not set

Send inventory: ○ Basic

● Standard

☐ Include font information

☐ Include printer information

☐ Include startup item information (macOS only)

☐ Include service information (Windows only)

Installed software:

☐ Scan installer receipts

☐ Scan for missing operating system patches

☐ Scan for missing third-party patches

☐ Scan for applications:

● Applications folder

○ Boot volume

○ All local volumes

The dialog contains these elements:

- **Inventory Server Address**: The IP address or DNS name of the server.
  Note: If you enter an abbreviated DNS name (that is, one that relies on being completed with the default domain you have specified in your computer’s network settings), make sure that all agents have the same default domain set. To avoid problems, we recommend that you use only fully qualified DNS names (that is, ones that include the full domain).
- **Server Port**: The port over which the server communicates with agents.
- **Heartbeat interval**: The interval in which the agents are to contact the server to let it know that they are still available.
  Note: This interval should not be longer than the Agent Offline Threshold setting of the LANrev server. (See “Server Settings” on page 780 for details.)
- **Inventory Push Interval**: The interval in which the agents are to send updated information on their computers to the server. (To save network bandwidth, only the changes are sent, not complete inventories.)
- **Inventory server certificate**: This field indicates whether a valid certificate for the server has been provided. If no valid certificate is available, the server cannot be saved.
  Note: Make sure that you are using a certificate that has been created after the last time the server has been installed. A certificate that has been created before a server has been reinstalled is indicated to be valid but will not allow a connection to the server.

Clicking the **Set** button lets you choose an SSL certificate for identifying the server. (Certificates can be created by means of the **Save Certificate** button in the **Server Settings** section of the Server Center, as described in “Exporting a server certificate” on page 21.)

- **Send inventory**: This lets you specify the amount of inventory information the agent sends by default:
  - **Basic**: If this option is checked, the agents send only basic inventory information (as opposed to complete inventory information) to this server. This option is intended for servers that act only as software distribution or license monitoring servers and thus have no need for full inventory information. Restricting these servers to basic information can save significant network bandwidth in large installations.
  - **Standard**: If this option is checked, the agents send the usual complete range of information to the server. We recommend that you use this option for administered clients.
  - **Include font information**: The agent automatically includes information on installed fonts when sending inventory information to the server.
  - **Include printer information**: The agent automatically includes information on connected printers when sending inventory information to the server.
  - **Include startup item information**: The agent automatically includes information on installed startup items when sending inventory information to the server.
  - **Include service information**: The agent automatically includes information on running services when sending inventory information to the server.
  - **Scan installer receipts**: The agent automatically scans the installer receipts on the computer when it is requested to determine the installed software.
  - **Scan for missing operating system patches**: If this option is checked, LANrev scans target computers for operating system patches. The Agent queries the operating system for any applicable patches that are available but not yet installed and reports them back to LANrev Server.
  - **Scan for missing third-party patches**: As part of determining the installed software, the agent automatically scans the computer to determine whether any available patches for monitored third-party applications have not yet been installed. A list of supported applications is available in article 22276 in the knowledge base.
  - **Scan for application**: You can specify the default location where the agent looks for installed applications when requested to do so.

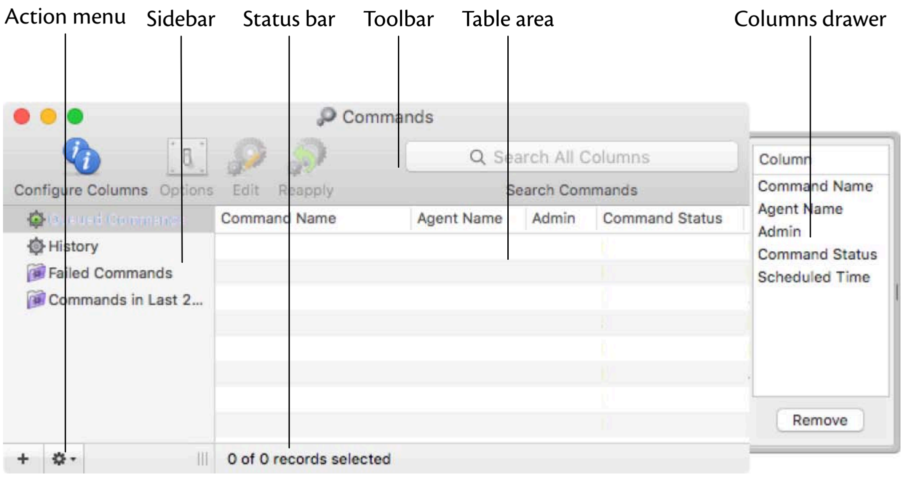
Refresh Status

The **Refresh Status** command updates the displayed information for the selected network devices.

Choosing the command causes LANrev Admin to query the device and update the displayed information.

Chapter 26 Commands window

The **Commands** window lists all commands that are pending, that are being executed, that have been executed and those that have failed. It lets you reschedule and edit these commands or re-execute completed commands.



The elements of the **Commands Center** window are described below:

- **Toolbar** (page 823)
- **Table columns** (page 824)
- **Sidebar** (page 825)
- **Action and context menus** (page 825)
  - **Copy** (page 826)
  - **Copy "<information item>"** (page 826)
  - **New Smart Command Queue Group from "<information item>"** (page 826)
  - **New Smart Command History Group from "<information item>"** (page 826)
  - **New Smart Command Queue Group** (page 827)
  - **New Smart Command History Group** (page 827)
  - **Edit Smart Group** (page 828)
  - **Remove Smart Group** (page 828)
  - **Scheduling Options** (page 829)
  - **Execute Command Now** (page 829)
  - **Edit Command** (page 829)
  - **Reapply Command** (page 829)
  - **Remove Command** (page 829)
  - **Show Command Result** (page 830)

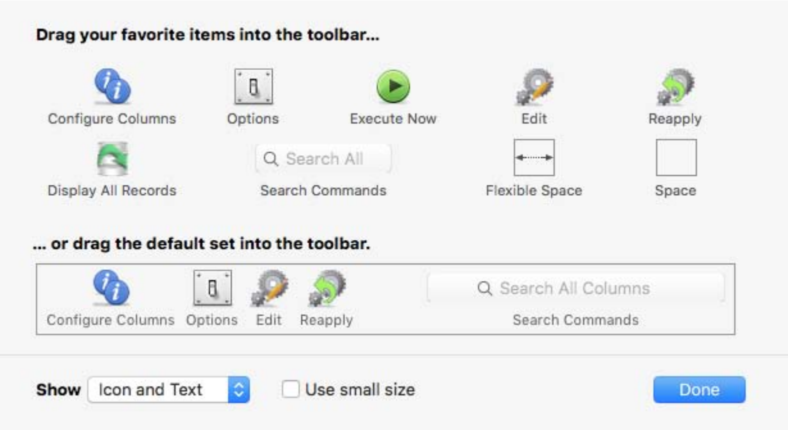
The + button in the lower left-hand corner is not separately described. Clicking it creates a new queue smart group as if you had chosen **New Smart Command Queue Group**; clicking it with the Option key held down acts like you had chosen **New Smart Command History Group**.

Toolbar

The **Commands** window has a toolbar that allows quick access to common actions.

NOTE The toolbar can be customized by means of the **Customize Toolbar** command described on page 398. After such customization, not all of the buttons described below may be present in the toolbar.

The toolbar can contain these elements:



Drag your favorite items into the toolbar...

... or drag the default set into the toolbar.

Show Icon and Text

□ Use small size

The elements are explained below, except for those that are not specific to LANrev Admin (**Flexible Space** through **Print**).

Configure Columns

The **Configure Columns** button opens the columns drawer or closes it when it is already open.

It has the same effect as the **Configure Columns** command described on page 397.

Options

The **Options** button lets you reschedule a pending command and change other command options. It is not available for commands that are already executing or have been completed.

Clicking the **Options** button opens the **Options** dialog that is described in “Options” on page 403, although the **Command description** field is not available.

Execute Now

The **Execute Now** button lets you immediately execute a pending or deferred command. It is not available for commands that are already executing or have been completed.

Clicking the button executes the selected commands immediately, irrespective of their scheduling options.

Edit

The **Edit** button lets you change the settings of a command that has not yet been executed.

Clicking the **Edit** button opens the selected command's command dialog, as described in "Commands menu" on page 399. This is similar to choosing the **Edit Command** command from the context menu.

Reapply

The **Reapply** button lets you execute a command one more time. If you reapply a command that has not yet been executed, a second copy of the command is created in the command queue, leaving the original command unchanged.

Clicking the **Reapply** button opens the selected command's command dialog, as described in "Commands menu" on page 399. This is similar to choosing the **Reapply Command** command from the context menu.

Display All Records

The **Display All Records** button downloads any records from the server that are not displayed because the number of initially displayed records has been limited in the preferences.

It has the same effect as the **Display All Records** command described on page 397.

Search Commands

The **Search Commands** field lets you quickly restrict the display to commands that contain the search text. The pop-up menu lets you specify whether all columns should be searched or just one particular column.

Pressing Return executes the search.

Table columns

The columns displayed in the **Commands** window are described in "Commands" on page 871.

Sidebar

The **Commands** window contains a sidebar with predefined and custom groups displaying commands by their execution status:

- **Queued Commands**: All commands that are pending execution, either because they have been scheduled for a future date or because they have been deferred.
- **History**: All commands that have already been completed, successfully or unsuccessfully. Because the history includes the results for each command (in the **Command Result Error** and **Command Error Info** columns), it also provides a command log.
- **Failed Commands**: All commands that LANrev has attempted to execute but that have failed. (Does not include deferred commands, that is, commands that could not yet be executed because the target computer is unavailable.)
- **Commands in Last 24 hours**: All commands that have been completed, successfully or unsuccessfully, in the last 24 hours.

Any additional smart groups that you define are displayed below these groups.

Action and context menus

The action and the context menus of the **Commands** window contains commands for managing commands and smart groups.

The commands are described in detail in the following sections.

- “Copy” on page 826
- “Copy “<information item>”” on page 826
- “New Smart Command Queue Group from “<information item>”” on page 826
- “New Smart Command History Group from “<information item>”” on page 826
- “New Smart Command Queue Group” on page 827
- “New Smart Command History Group” on page 827
- “Edit Smart Group” on page 828
- “Remove Smart Group” on page 828
- “Scheduling Options” on page 829
- “Execute Command Now” on page 829
- “Edit Command” on page 829
- “Reapply Command” on page 829
- “Remove Command” on page 829
- “Show Command Result” on page 830

For information on the rest of the commands in the context menu, see “Commands menu” on page 399. (The **Favorite Commands** context menu item corresponds to the **Favorites** submenu in the **Commands** menu.)

Copy

The **Copy** command copies the selected records as tab-delimited text to the clipboard.

If multiple records are selected, all are copied.

The **Copy** context menu command has the same effect as the **Copy** command from the **Edit** menu described on page 392.

Copy “<information item>”

The **Copy “<information item>”** command copies the contents of one particular information item of the selected records as text to the clipboard. The information from the item on which you are right-clicking is copied; the title of that information item is noted in the context menu command (for example, **Copy “Command Name”**).

If multiple records are selected, the contents of the information item from all of them are copied.

New Smart Command Queue Group from “<information item>”

The **New Smart Command Queue Group from “<information item>”** command lets you create a smart group with prefilled criteria.

Choosing the command opens the **New Smart Command Queue Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

New Smart Command History Group from “<information item>”

The **New Smart Command History Group from “<information item>”** command lets you create a smart group with prefilled criteria.

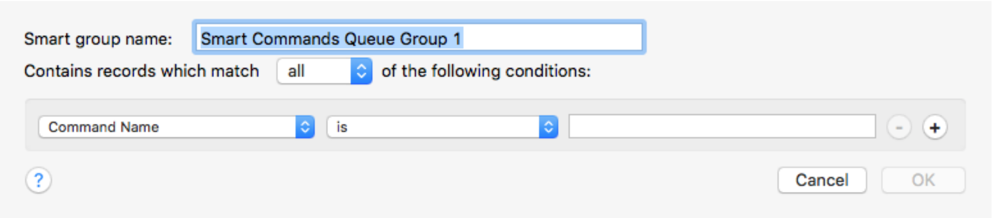
Choosing the command opens the **New Smart Command History Group** dialog with one or more criteria already specified. The specified criteria are taken from the selected records and the information item column in which you have right-clicked: The information item is used as the selection criterion, and the contents of the item in the selected records are used as the comparison values.

You can edit these criteria, add new ones, or delete them as desired before saving the smart group.

New Smart Command Queue Group

The **New Smart Command Queue Group** command creates a new smart group for pending or running commands (that is, commands that have not yet finished executing).

Choosing the command opens the **Smart Group** dialog:


Smart group name: Smart Commands Queue Group 1

Contains records which match all of the following conditions:

Command Name | is

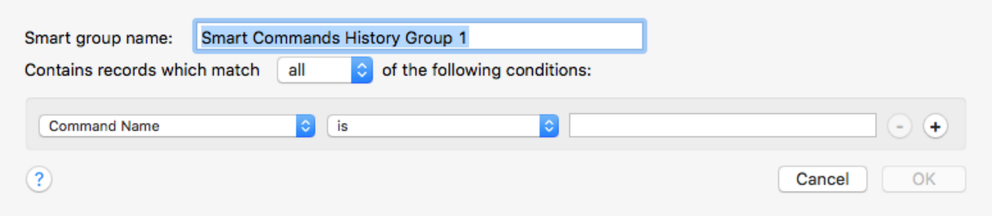
The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
  - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in "Commands" on page 871, "General" on page 831, and "Administration" on page 873.
  - The second pop-up menu contains the possible comparison operators.
  - The right-hand text field lets you specify the value to compare record values against.
  - The **+** and **–** buttons let you add new conditions or remove existing ones.

New Smart Command History Group

The **New Smart Command History Group** command creates a new smart group for completed commands (that is, commands that have been executed successfully or with a failure).

Choosing the command opens the **Smart Group** dialog:



Smart group name: Smart Commands History Group 1

Contains records which match all of the following conditions:

Command Name is

The dialog contains these elements:

- **Smart group name**: The name for the smart group.
- **Contains records which match**: When **all** is chosen from this pop-up menu, records are found that match all specified conditions (Boolean AND). If **any** is chosen, records are found that match at least one of the specified conditions (Boolean OR).
- Conditions area:
    - The left-hand pop-up menu lets you choose an information item on which records are to be matched. The available information items are described in “Commands” on page 871, “General” on page 831, and “Administration” on page 873.
    - The second pop-up menu contains the possible comparison operators.
    - The right-hand text field lets you specify the value to compare record values against.
    - The **+** and **–** buttons let you add new conditions or remove existing ones.

Edit Smart Group

The **Edit Smart Group** command lets you edit the name and selection conditions for the selected smart group.

Choosing the command opens the specification dialog for the type of smart group that is selected. For details, see the command for creating that type of smart group:

- “New Smart Command Queue Group” on page 827
- “New Smart Command History Group” on page 827

Remove Smart Group

The **Remove Smart Group** command deletes smart groups.

Choosing the command deletes the selected smart groups. A confirmation alert is displayed first. The contents of the smart groups is not deleted.

Scheduling Options

The **Scheduling Options** command lets you reschedule a pending command. It is not available for commands that are already executing or have been completed.

Choosing the command opens the **Scheduling Options** dialog that is described in “Options” on page 403, although the **Command description** field is not available.

Execute Command Now

The **Execute Command Now** command lets you execute a pending command immediately. It is not available for commands that are already executing or have been completed.

Choosing the command immediately executes all chosen commands, regardless of their scheduling settings. A confirmation message is displayed first.

Edit Command

The **Edit Command** command lets you change the settings of a command that has not yet been executed. It is not available for commands that are already executing or have been completed.

Choosing the command opens the selected command’s command dialog, as described in “Commands menu” on page 399.

Reapply Command

The **Reapply Command** command lets you execute a command again. A new copy of the command is created in the command queue.

Choosing the command opens the selected command’s command dialog, as described in “Commands menu” on page 399.

Remove Command

The **Remove Command** command deletes a command from the command table. If the command is pending, it will not be executed. A confirmation message is displayed first.

NOTE In the command history, the **Remove Command** command can be used only by administrators with the **Remove History Entry** right. See “New Administrator” on page 758 for details.

Show Command Result

The **Show Command Result** command displays the results of script commands executed on administered computers. It applies only to instances of the **Execute Script** commands that have already been completed.

Choosing the command opens an editable text window displaying the result that has been returned by the executed script. You can save the result using the **Save As** command.

Chapter 27 Information items

LANrev can display numerous aspects of the state and configuration of administered devices. It does so in information items, which are analogous to database fields.

This chapter contains a complete listing of all information items, sorted by subject matter.

NOTE If you are looking for an information item by name, you can easily find it in the **Index**.

Information items cover these areas:

- "Agent Information" on page 831
- "Hardware Information" on page 836
- "Software Information" on page 852
- "Commands" on page 871
- "Server Center" on page 872
- "Agent Deployment Center" on page 890
- "Installed Software Statistics" on page 891
- "Missing Patch Statistics" on page 892
- "Compliance Reports" on page 892
- "Mobile Device Information" on page 894
- "iBooks Books" on page 933
- "Windows Reinstallation Tasks" on page 934
- "Classroom Management" on page 936

Agent Information

Information items in the **Agent Information** section contain information on the Agent properties and settings. There are three subcategories:

- **General** (page 831)
- **Agent Settings** (page 833)
- **Custom Fields** (page 836)

General

The **General** category contains information items related to the version and identifying information of LANrev Agent.

Agent Name The name under which the computer on which LANrev Agent is installed is displayed in LANrev.

NOTE If **Use Custom Agent Name** is "Yes", this information item is the same as **Custom Agent Name**. If **Use Custom Agent Name** is "No", it is the same as **Computer Name**.

Agent Version

The version number of the LANrev agent.

Agent Build Number

The build number of the LANrev agent.

Agent Serial Number

The unique serial number of the LANrev agent.

Agent Active IP

The IP address that LANrev Server recorded for the agent at the time of the last successful contact. This is the IP address of the computer on which LANrev Agent is installed. If the computer has multiple IP address, this information item contains “n/a”.

Computer Enrollment Date

The date, if any, when this computer was enrolled in MDM management through LANrev. This information is available only for computers enrolled in MDM.

Computer Enrolled in MDM

Whether this computer has been enrolled in MDM management through LANrev.

Computer Enrollment MDM User

The name of the user account on the computer that has been enrolled into MDM.

This information is not available for devices for which the most recent MDM enrollment was performed with a version of LANrev prior to 6.9.1. For devices that have been enrolled via the agent with no user logged in, the information will be not available until the first time that a user logs in after enrollment.

Computer Enrolled via Enrollment Program

Whether this computer was enrolled via an enrollment program (as opposed to having been enrolled by other means). This information is available only for computers enrolled in MDM.

Computer Enrollment Program Registration Date

The date when the computer was registered in the enrollment program. This information is available only for computers enrolled in MDM.

Computer Enrollment Profile Assignment Date

The date when the current enrollment profile was assigned to the computer. This information is available only for computers enrolled in MDM.

Computer Enrollment Profile Installation Date

The date when the enrollment profile was installed on this computer. This information is available only for computers enrolled in MDM.

Computer Enrollment Profile UUID

The UUID of the enrollment profile assigned to this computer. This information is available only for computers enrolled in MDM.

Computer Enrollment Status

Whether and in what way the computer is part of Apple’s device enrollment program. This information item can have these values:

- **not in enrollment program**: The device has not been entered into any enrollment program.
- **not assigned**: The device is part of an enrollment program, but no enrollment profile is durrently assigned to it.

- **assigned**: An enrollment profile has been assigned to the device but the device has not yet been enrolled in the MDM.
- **installed**: The enrollment profile has been installed on the device; that is, the device has been enrolled in MDM and the profile options have taken effect.

Computer Device Identifier (UDID)
The target identifier (a unique internal ID) of the managed computer. This information is available only for computers enrolled in MDM.

Computer Online
Whether the computer has sent its last scheduled heartbeat signal. (In the **Computers** window, this information is indicated by a green or red dot in front of the computer's row.)

Computer Online (Icon)
A graphical information on whether the computer has sent its last scheduled heartbeat signal: A green dot indicates that it has; a red dot, that it has not. (This is the same as the online status column in the **Computers** window.)

Computer Ownership
The kind of owner the computer has – the company, the user, or a guest.

Last Heartbeat
The time when the last heartbeat signal has been received from this agent.

NOTE The heartbeat is a regular signal by the agent indicating that it is still running.

Last Contacted by Server
The most recent time when the agent received information or some other signal from the server.

Record Creation Date
The time when the record for this computer was created in the server.

Agent Settings

The **Agent Settings** category contains information items related to the current settings of LANrev agents.

Servers

The **Servers** subcategory contains information about server-related settings of LANrev agents. If an agent communicates with multiple servers, one row per server is generated for each agent.

Server Address
The address of all LANrev servers with which the LANrev agent is set to communicate, not including any servers that are software distribution or license monitoring servers for the agent but not inventory servers.

Server Port
The port on the LANrev server with which the LANrev Agent communicates.

Server Unique ID

The unique ID of the LANrev server with which the LANrev agent communicates. The ID stays constant even when the server’s network address changes.

Heartbeat Interval

The interval, in minutes, in which the LANrev agent contacts the server to let it know that its computer is still running.

Inventory Push Interval

The interval, in minutes, in which the LANrev agent transmit any changes to the state or parameters of its computer to the server.

Basic Inventory Only

Whether this server has been configured in the **Agent Settings** to request only basic inventory information from this agent.

Is Primary Inventory Server

Whether this server is the primary inventory server for this agent.

The primary inventory server is the one to which the agent sends power management information. It also serves certain internal functions with respect to the agent. It is listed as the first inventory server in the **Agent Settings** command dialog.

Inventory with Fonts

Whether this inventory server collects font information from this agent during normal inventory information collection.

Inventory with Printers

Whether this inventory server collects printer information from this agent during normal inventory information collection.

Inventory with Startup Items

Whether this inventory server collects startup item information from this agent during normal inventory information collection.

Inventory with Windows Services

Whether this inventory server collects Windows service information from this agent during normal inventory information collection.

Scan for Installer Receipts

Whether this inventory server scans this agent for installer receipts when determining installed software.

Scan for Missing OS Patches

Whether this inventory server scans this agent for available operating system patches that are not installed when determining installed software.

Scan for Missing Third-Party Patches

Whether this inventory server scans this agent for available third-party patches that are not installed when determining installed software.

Scan for Applications

Whether this inventory server scans this agent for application executables when determining installed software.

Application Scan Options

The scope where the agent’s computer is scanned for applications – in the applications folder, on the boot volume, or on all local volumes.

Client Information

The **Client Information** subcategory contains information about user-definable information stored on administered computers.

Client Information 1 … 10

The first through tenth of the information fields for user-definable information. The contents of these fields can be any text, as specified by administrators or local users.

NOTE The actual fields may have names that differ from those of these information items, when you have edited the field names in the **Server Settings** dialog.

Client Info Locked

Whether the client information fields are locked on this computer. If fields are locked, only administrators can edit their contents, not local users.

Ungrouped fields

The **Agent Settings** information items category contains a number of ungrouped fields.

Custom Agent Name

A custom name for this computer just for use within the LANrev system, as specified in the **Agent Settings** dialog's **General** tab.

Use Custom Agent Name

Whether the custom agent name (see above) is to be used to indicate the computer within the LANrev system.

SD Server Address

The IP address or DNS name of the software distribution server specified for this computer.

SD Server Port

The port on the software distribution server that is specified for this computer.

SD Server Unique ID

The unique ID of the software distribution server assigned to this agent. The ID stays constant even when the server's network address changes.

SD Server Check Interval

The interval, in minutes, in which the LANrev agent is set to check the software distribution server for new installation packages.

LM Server Address

The IP address or DNS name of the license monitoring server specified for this computer.

LM Server Port

The port on the license monitoring server that is specified for this computer.

LM Server Unique ID

The unique ID of the license monitoring server assigned to this agent. The ID stays constant even when the server's network address changes.

LM Server Check Interval

The interval, in minutes, in which the LANrev agent checks for changes to the license specifications on the license monitoring server.

Agent Port

The local port on which the agent can be reached by the server.

Connect Timeout

The time, in seconds, which the agent waits for responses from the server before it considers a connection attempt to have failed.

Included in OS Patch Management

Whether this agent is set to check for operating system and software patches from Apple or Microsoft and install them using LANrev's software distribution feature.

Included in Third-Party Patch Management

Whether this agent is set to check for software patches for supported third-party software and install them using LANrev's software distribution feature.

Use Only LANrev for OS Updates

This information item displays "True" if the **Use only LANrev for OS updates** option in the **Agent Settings** dialog is checked for the agent.

LANrev Remote Enabled

Is the screen-sharing function that is built into the Agent enabled on this computer?

LANrev Remote Port

The port over which the Agent accepts screen-sharing connections.

LANrev Remote User Confirmation Required

Whether screen-sharing requests must be accepted by the user before the Agent establishes the connection.

LANrev Remote SSL Enabled

Whether the Agent is configured to use SSL for screen-sharing connections.

Computer Is Tracked

Is this computer currently being monitored via LANrev's computer tracking feature?

Custom Fields

The **Custom Fields** category contains all custom information fields for desktop devices that have been defined on the currently connected server.

The exact contents of this category and the functions of the individual fields depend entirely on the specific local configuration of the site and cannot be described further here.

NOTE Double-clicking a custom information item in the **Information Items** window lets you edit its specifications.

Hardware Information

Information items in the **Hardware Information** section contain information on the client computer hardware. There are nine subcategories:

- **System Information** (page 837)
- **Memory Slots** (page 846)
- **Volumes** (page 846)
- **ATA Devices** (page 847)
- **SCSI Devices** (page 848)

- **FireWire Devices** (page 849)
- **USB Devices** (page 849)
- **PCI Devices** (page 850)
- **Displays** (page 851)

System Information

The **System Information** category contains information on the computer itself (as opposed to installed and peripheral devices.)

CPU Information

The **CPU Information** subcategory contains processor-related information.

Physical Cores

The total number of main processor cores installed in the computer.

NOTE Due to a limitation in Windows, LANrev cannot report physical cores that have been disabled during the boot process or in Task Manager.

Active Cores

The number of currently enabled main processor cores in the computer.

This number may be lower than **Physical Cores**, above, when individual cores are disabled, for example, to lower power consumption.

NOTE Due to a limitation in Windows, LANrev cannot report processors that have been disabled in Task Manager.

Physical Processors

The number of physical main processors installed in the computer.

Only physically discrete processors are counted; a processor supporting hyperthreading or multiple cores is counted as one processor.

NOTE Due to a limitation in Windows, LANrev cannot report processors that have been disabled during the boot process or in Task Manager.

Cores per Processor

How many cores does the main processor have?

Processor Speed

The processor’s clock rate.

Processor Type

The main processor’s series and version.

Processor Vendor

The main processor’s manufacturer.

Processor Is 64-bit

Is the main processor a 64-bit processor.

Processor ID String

Intel-compatible processors only: The processor type string as reported by the operating system.

Processor Architecture A string briefly describing the basic processor type (Intel, AMD, or PowerPC) and data word size (32 bit or 64 bit).

Processor L1 Data Cache The size of the processor’s level 1 cache for data.

Processor L1 Instruction Cache The size of the processor’s level 1 cache for instructions.

Processor L2 Data Cache The size of the processor’s level 2 cache for data.

Processor L2 Instruction Cache The size of the processor’s level 2 cache for instructions.

Processor L3 Cache The size of the processor’s level 3 cache.

Bus Speed The clock speed the processor’s front-side bus.

Processor Family The family ID of the main processor, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers.

Processor Model The model ID of the main processor within its family, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers

Processor Stepping The stepping ID of the main processor within its model, as specified by the manufacturer. This information is not available for PowerPC-based Macintosh computers

Processor Has MMX Does the processor support the MMX instruction set?

Processor Has 3DNow Does the processor support the 3DNow instruction set?

Processor Has SSE Does the processor support the SSE instruction set?

Processor Has SSE2 Does the processor support the SSE2 instruction set?

Processor Has SSE3 Does the processor support the SSE3 instruction set?

Processor Supports Hyperthreading Does the processor support hyperthreading?

Processor Hyperthreading Enabled Is hyperthreading currently enabled?

NOTE Due to a limitation in Windows, LANrev may misreport hyperthreading to be off when processors have been disabled in Task Manager.

Battery Information

The **Battery Information** subcategory contains information related to the batteries of administered laptops.

AC Charger Connected

Laptops only: Is the laptop’s AC power adapter currently providing mains power?

AC Charger Charging

Laptops only: Is the laptop’s AC power adapter currently charging the laptop’s battery?

Battery Installed

Laptops only: Is a battery currently present in this laptop?

Battery Fully Charged

Laptops only: Is the laptop’s battery currently reported by the computer as being fully charged?

Original Battery Capacity

Laptops only: The rated original capacity of the battery in mAh (milliampere-hours).

Maximum Battery Capacity

Laptops only: The current maximum capacity of the battery in mAh (milliampere-hours), as reported by the laptop’s power management.

Remaining Battery Capacity

Laptops only: The currently remaining power in the battery in mAh (milliampere-hours), as reported by the laptop’s power management.

Battery % of Original Capacity

Laptops only: The battery’s current maximum capacity as a percentage of its original rated capacity.

Battery Load Cycles

Laptops only: The total number of load cycles of this battery, as reported by the laptop’s power management.

Battery Type

Windows laptops only: The basic type of the laptop’s battery (for example, “Lithium Ion”).

Battery Manufacturer

Laptops only: The manufacturer of the battery. (This information is not available for PowerPC-based Macs.)

Battery Manufacturing Date

Laptops only: The date when the battery was manufactured. (This information is not available for PowerPC-based Macs.)

Battery Device Name

Laptops only: The device name of the battery as provided by the operating system.

Battery Serial Number

Laptops only: The serial number of the battery. (This information is not available for PowerPC-based Macs.)

Battery Temperature

Laptops only: The current temperature of the battery in degrees Celsius.

Power Management

The **Power Management** subcategory contains information related to the power management settings and capabilities of administered computers.

Power-on Avg/Day

The average number of hours that the computer has been powered up per day. (The average is calculated for the entire period during which LANrev has monitored this computer.)

Power-on Avg/Week

The average number of hours that the computer has been powered up per week. (The average is calculated for the entire period during which LANrev has monitored this computer.)

Power-on Avg/Month

The average number of hours that the computer has been powered up per month. (The average is calculated for the entire period during which LANrev has monitored this computer. A month is considered to have 30 days.)

Power-on Avg/Year

The average number of hours that the computer has been powered up per year. (The average is calculated for the entire period during which LANrev has monitored this computer. A year is considered to have 365 days.)

Power-on Yesterday

The average number of hours that the computer has been powered up yesterday. (This information is only available if LANrev has started monitoring this computer before yesterday.)

Power-on Last 7 Days

The average number of hours that the computer has been powered up during the last seven calendar days. (This information is only available if LANrev has started monitoring this computer more than seven days ago.)

Power-on Last 30 Days

The average number of hours that the computer has been powered up during the last 30 calendar days. (This information is only available if LANrev has started monitoring this computer more than 30 days ago.)

Power-on Last 365 Days

The average number of hours that the computer has been powered up during the last 365 calendar days. (This information is only available if LANrev has started monitoring this computer more than 365 days ago.)

Power-on Tracking Start

The date when LANrev has started tracking this computer’s power management.

System Sleep Timer

The number of minutes of inactivity before the administered computer is set to go to sleep.

System Hibernate Timer

Windows only: The number of minutes of inactivity before the administered computer is set to go into hibernation.

Disk Sleep Timer

The number of minutes of inactivity before the administered computer is set to spin down the hard disks.

Display Sleep Timer

The number of minutes of inactivity before the administered computer is set to turn off the display.

Action on Power Button

The action the administered computer performs when the power button is pressed. This does not apply to Macintosh laptops.

Action on Clamshell Close

Windows only: The action the administered computer performs when the clamshell case is closed. This applies only to laptops.

Action on Sleep Button

Windows only: The action the administered computer performs when the sleep button is pressed.

Wake on AC Change

Is the administered computer set to wake up when the power adapter is connected or disconnected? This applies only to laptops.

Wake on Clamshell Open

Is the administered computer set to wake up when its clamshell case is opened? This applies only to laptops.

Automatic Restart on Power Loss

Is the administered computer set to restart automatically after being affected by a power outage?

Display Sleep Uses Dim

Does the administered computer reduce the screen brightness after a certain period of inactivity, but before going to sleep?

Display Reduces Brightness

Is the display brightness automatically reduced when the computer is on battery power?

TTYs Keep Awake

macOS only: Do activities on remote terminal connections count as activities to reset the sleep timer?

Hibernation Mode

The kind of hibernation the computer enters when it goes to sleep.

UPS Installed

Is a UPS (uninterruptible power supply) connected to the administered computer?

NOTE LANrev only detects a UPS that is properly registered with the operating system.

Sudden Motion Sensor

macOS only: Is the administered computer equipped with a sudden motion sensor?

Power Management Schedules

The **Power Management Schedules** subcategory contains information on the power management schedules that have been set up in LANrev for the administered computers.

PM Schedule Name

The name of the power management schedule.

PM Settings For

The type of power supply (for example, battery or power adapter) to which the schedule applies.

PM Action
The scheduled action.

PM Trigger
The trigger for the action.

PM Inactivity Timer
The inactivity period in minutes after the specified action is to be performed.

PM Time
The time at which the specified action is to be performed.

PM Only When No User Logged In
Is this scheduled to be performed only when no user is logged in?

PM Schedule Count
The number of the power management schedule rules applied to a computer. If no power management is active on the computer, the value is 0.

Note that this information does not apply to power management schedule records (as do the other information items in this subcategory) but to computer records.

Ungrouped fields

The **Hardware Information** information items category contains a number of ungrouped fields.

Physical Memory
The amount of actual RAM installed in the computer.

Computer Type
For PCs, “PC Compatible” is displayed. For Macs, the exact model is displayed.

Computer Identifier
Macs only: The internal identifier used by Apple to indicate this Macintosh model. For example, “MacBookPro5,2” is a 17" MacBook Pro sold between February 2009 and June 2010.

Boot ROM Information
The information string from the computer’s boot ROM. The exact contents and formatting of this string depends on the ROM vendor.

Primary MAC Address
The MAC address of the computer’s current primary network connection.

Date & Time
The date and time of the computer’s internal clock.

This information is current as of the last ‘heartbeat’ contact from the agent with LANrev Server. It is not updated in real time.

You can find out the difference between the client’s local clock and the server’s clock by comparing the **Date & Time** and **Last Heartbeat** information items: Both display the same point in time but the first a measured by the client’s clock and the second as measured by the server’s.

Computer Production Date
Macs only: The date when the computer was manufactured.

Computer Production Factory

Macs only: The site where the computer was manufactured.

Computer Serial Number

The serial number of the computer.

NOTE Some Windows computers may not have a serial number.

Computer Boot Time

The date and time when the computer was last booted.

Computer Boot Duration

Windows Vista and above or Windows Server 2008 and above only: The amount of time that the last boot process of the computer took, from switching it on (or resetting it) to a usable desktop.

This is the same duration that the built-in Windows diagnostics report.

Computer Uptime

The time since the computer was last booted, in hours and minutes.

This information is current as of the last inventory update. To find out the uptime now, trigger an inventory update using the **Gather Inventory Information** command.

Computer Age

Macs only: The age of the computer, that is, the time that has elapsed since its production.

Computer Color

Macs from Apple’s device enrollment program only: The case color of the computer.

SMC Version

Intel-based Macs only: The version number of the computer’s SMC firmware.

Apple Product Name

Macs only: The official product name Apple uses for this type of Macintosh.

NOTE The content of this information item is downloaded from an Apple server, based on the client computer’s serial number. It is therefore available only if the client computer had a working Internet connection at least once after LANrev Agent has been installed on it. This information item is updated every ten days as long as the client computer can reach Apple’s server.

Computer Purchase Date

The date when the computer was purchased, according to the manufacturer’s files.

NOTE This information is retrieved from a server of the computer’s vendor and faces restrictions similar to those noted under “Apple Product Name”, above. In addition, not all vendors provide this information.

Computer Warranty Info
The computer’s current warranty status.

NOTE This information is retrieved from a server of the computer’s vendor and faces restrictions similar to those noted under “Apple Product Name”, above. In addition, not all vendors provide this information.

Computer Warranty End
The date when the warranty for the computer will end. A value of “n/a” indicates either that no information is available or that the warranty has expired.

NOTE This information is retrieved from a server of the computer’s vendor and faces restrictions similar to those noted under “Apple Product Name”, above. In addition, not all vendors provide this information.

Unique Computer ID
Macs only: A UUID given the computer by Apple that uniquely identifies it.

BIOS Date
Windows only: The creation date of the computer’s BIOS, as stored in the BIOS.

BIOS Vendor
Windows only: The creator of the computer’s BIOS.

BIOS Version
Windows only: The version number of the computer’s BIOS.

BIOS Type
Windows only: The type of BIOS active on the computer, legacy or UEFI.

SMBIOS Version
Windows only: The version number of the computer’s System Management BIOS.

Mainboard Manufacturer
Windows only: The vendor of the mainboard used in the computer.

Mainboard Product Name
Windows only: The mainboard’s name as specified by its vendor.

Mainboard Serial Number
Windows only: The mainboard’s serial number.

Mainboard Type
Windows only: The type of the mainboard used in the computer, as specified by its vendor.

Mainboard Version
Windows only: The version number of the mainboard used in the computer.

Mainboard Asset Tag
Windows only: The asset tag of the computer’s main board.

System Enclosure Manufacturer
Windows only: The vendor of the computer’s case.

System Enclosure Serial Number

Windows only: The serial number of the computer’s case.

System Enclosure Type

Windows only: The type of the computer’s case.

System Enclosure Version

Windows only: The version number of the computer’s case.

System Enclosure Asset Tag

Windows only: The asset tag of the computer’s case.

Computer Manufacturer

Windows only: The producer of the computer system.

Computer Version

Windows only: The version number of the computer system.

Computer Model

Windows only: The model name of the computer system.

Computer Service Tag

Windows only: The service tag of the computer system.

Computer Express Service Tag (Dell)

Dell systems only: The express service tag of the computer system.

Swap Space Total

The size of the swap space that is currently reserved on the hard disk.

Swap Space Used

The current amount of data that has been swapped to disk.

Swap Space Free

The amount of swap space that has been reserved but is currently unused.

Swap Space Encrypted

macOS only: Whether encryption for the swap file has been enabled.

Memory Slots

The number of slots for RAM on the computer’s motherboard.

Memory Module Count

The number of RAM modules installed in the computer.

Volume Count

The number of volumes that are mounted on the computer.

ATA Device Count

The number of ATA devices that are connected to the computer and powered on.

SCSI Device Count

The number of SCSI devices that are connected to the computer and powered on.

FireWire Device Count

The number of FireWire devices that are connected to the computer and powered on.

USB Device Count

The number of USB devices that are connected to the computer.

PCI Device Count

The number of PCI cards that are installed in the computer.

Display Count The number of display devices that are connected to the computer and have been recognized by it.

Memory Slots

The **Memory Slots** category contains information items related to individual memory slots.

Memory Slot Name The label of the memory slot.

Memory Size The RAM size of the memory module installed in the slot.

Memory Speed macOS only: The clock rate with which the memory module is accessed.

Memory Type The general type of memory installed in the memory slot, such as SDRAM, DDR SDRAM, etc.

Volumes

The **Volumes** category contains information items related to individual volumes mounted on the administered computer.

Volume Name The name of the volume. (On Windows computers, this may be empty.)

Size The formatted capacity of the volume. (Total space, whether free or used.)

Format The file system with which the volume is formatted – NTFS, FAT32, Mac OS Extended, etc. (See also **Journaled**, below.)

Volume Type The general type of volume – hard disk, removable, or server.

NOTE On Windows client computers, it is possible to recognize CD-ROMs and RAM disks. This information is not available on macOS clients where these media are listed just as “removable”.

Free Space The unused capacity of the volume in absolute terms.

Free Space % The unused capacity of the volume as a percentage of the total formatted capacity.

Drive Letter Windows only: The drive letter that is currently assigned to the volume.

Volume Serial Number Windows only: The serial number of the volume.

Object Count macOS only: The total number of objects – files and folders, visible and invisible – on the volume. This information is not available for server volumes.

Folder Count macOS only: The total number of directories – both visible and invisible – on the volume. This information is not available for server volumes.

Creation Date macOS only: The date and time when the volume was last formatted.

Modification Date macOS only: The date and time when the volume was last modified.

Backup Date macOS only: The date and time when the volume was last backed up. If no backup has yet been made, the date is “n/a”.

NOTE Not all backup applications set this date when they back up a volume.

Checked Date macOS only: The date when the hard disk was last checked by a hard disk utility.

NOTE Not all such utilities set this date when they check a volume.

Boot Volume Is this the volume from which the computer has booted?

Compressed Windows only: Is the data on this volume compressed by the operating system?

Journaled macOS only: Is this volume journaled?

Case-sensitive Are file names on this volume case-sensitive? (That is, would “File.txt” and “file.txt” considered to be two different names?)

Locked by Hardware macOS only: Is this volume write-protected through a hardware setting?

Locked by Software macOS only: Is this volume write-protected through a software setting?

NOTE Due to a limitation in macOS, volumes that are write-protected by hardware, such as CD-ROMs, may be displayed as being write-protected by software.

Unix Mount Point macOS only: The mount point of the volume on the computer.

ATA Devices

The **ATA Devices** category contains information items related to individual ATA devices connected to the administered computer. Only devices that are powered on are listed.

ATA Bus Number The number of the ATA bus on which the device is located.

ATA Unit Number The unit number of the ATA device on its bus.

ATA Manufacturer The company who has manufactured this ATA device.

ATA Model The model number of the ATA device, as specified by the manufacturer.

ATA Device Type The general type of the ATA device, such as hard disk, CD-ROM/DVD-ROM, etc.

ATA Serial Number The serial number of the ATA device, as specified by the manufacturer.

NOTE Not all ATA devices have serial numbers.

ATA SMART Status The status of the SMART hard disk monitoring system for the ATA device.

NOTE This information is available only for hard disks.

ATA Revision The revision (version) number of the ATA device, as specified by the manufacturer.

ATA Protocol The type of ATA protocol used by the computer to communicate with this device.

ATA Capacity The formatted capacity of the ATA device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

ATA Socket Type macOS only: The type of interface by which the ATA device is connected to the computer.

ATA Bay Name macOS only: The name of the drive bay in which the ATA device is located.

SCSI Devices

The **SCSI Devices** category contains information items related to individual SCSI devices connected to the administered computer. Only devices that are powered on are listed.

SCSI Bus Number The number of the SCSI bus on which the device is located.

SCSI Unit Number The SCSI ID of the device.

SCSI Manufacturer The company who has manufactured this SCSI device.

SCSI Model The model number of the SCSI device, as specified by the manufacturer.

SCSI Device Type The general type of the SCSI device, such as hard disk, CD-ROM/DVD-ROM, etc.

SCSI Revision The revision (version) number of the SCSI device, as specified by the manufacturer.

SCSI Capacity The formatted capacity of the SCSI device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

SCSI Transfer Width The width, in bits, of the SCSI bus over which the device is connected.

FireWire Devices

The **FireWire Devices** category contains information items related to individual FireWire devices connected to the administered computer. Only devices that are powered on are listed.

FireWire Manufacturer The company who has manufactured this FireWire device.

FireWire Model The model number of the FireWire device, as specified by the manufacturer.

FireWire Firmware Revision macOS only: The revision (version) number of the FireWire device's firmware, as specified by the manufacturer.

FireWire Software Version macOS only: The version of the core FireWire software that is integrated in the firmware.

FireWire Speed macOS only: The maximum speed of the FireWire bus over which the device is connected.

FireWire Capacity The formatted capacity of the FireWire device.

For removable drives, the formatted capacity of the current medium is given. In the case of CDs and DVDs, this may be significantly less than the maximum capacity of a medium of this type.

FireWire Vendor ID The ID number for the vendor of the FireWire device.

FireWire Model ID The ID that the device's vendor has assigned to this type of model.

USB Devices

The **USB Devices** category contains information items related to individual USB devices connected to the administered computer.

USB Vendor The company who has manufactured this USB device.

USB Model The model name of the USB device, as specified by the manufacturer.

USB Serial Number The serial number of the USB device, as assigned by the manufacturer.

NOTE Many USB devices do not have serial numbers.

USB Max. Power The highest power draw, measured in mA (milliampere), that this device can have.

NOTE This value is taken from the device’s firmware. Depending on how accurately the manufacturer specifies this value, the actual peak consumption may exceed this value.

USB Device Speed The maximum connection speed that the USB device supports.

NOTE The device may not actually be able to transfer data at this rated speed.

USB Capacity macOS only: The nominal data capacity of a USB device. If the device does not store data, it’s capacity is given as “n/a”.

NOTE Some data storage devices do not properly announce their capacity, in which case the information item also contains “n/a”.

USB Vendor ID macOS only: The ID number for the vendor of the USB device.

USB Product ID macOS only: The ID that the device’s vendor has assigned to this type of model.

USB Product Version The version of the USB product, as specified by the manufacturer.

USB Device Protocol An identifier for the protocol that the USB device uses to communicate with its driver. The meaning of the identifier depends on the USB device.

USB Device Class The general type of the USB device, for example hub or mouse.

USB Device Subclass An identifier to distinguish different subtypes of one type of USB device.

PCI Devices

The **PCI Devices** category contains information items related to individual PCI cards installed in the administered computer.

PCI Name The name of the PCI device, as specified by the manufacturer.

PCI Type The general type of the PCI device, for example, “display” (graphics card).

PCI Slot macOS only: The label of the PCI slot in which the device is installed.

PCI ROM Revision macOS only: The revision (version) of the PCI device’s firmware, as specified by the manufacturer.

PCI Device ID The ID number for the PCI device model.

PCI Vendor ID The ID number for the vendor of the PCI device.

PCI Revision ID The revision of the PCI device's firmware.

Displays

The **Displays** category contains information items related to individual displays connected to the administered computer. Only displays that have been recognized by the computer are listed.

Display Type The general type of the display.

NOTE This information item may display "CRT" for LCD displays connected to an analog interface.

Display Vendor The manufacturer of the display.

Display Product Name The model name of the display.

Display Manufacture Date The date on which the display was produced.

Display Serial Number The serial number of the display.

Resolution The current horizontal and vertical size of the display, in pixels.

NOTE This information item displays the current setting. It does not, for example, display the natural resolution of an LCD display if it is set to a different resolution.

Depth The color depth to which the display is set, expressed as bits per pixel.

Refresh Rate The screen refresh rate to which the display is currently set.

Main Display Is this the computer's main display? (On macOS computers, the main display is the one containing the menu bar; on Windows computers it is the one with the Start menu.)

Mirror macOS only: Is this display currently being mirrored?

Display Online Whether the frame buffer is connected to a monitor.

Display Is Built-in Whether the display is an internal display, that is, built into the computer.

Quartz Extreme macOS only: Is Quartz Extreme active for this display?

VRAM Size The amount of video RAM being used for this display.

Display Serial Number (internal) macOS only: The internal serial number of the display device. This is usually, but not always, the same number as Display Serial Number, above.

Display Model ID macOS only: The ID number for the display model.

Video Card Model The model name of the video card to which the display is connected.

Software Information

Information items in the **Hardware Information** section contain information on the operating systems on the client computers, their network settings, processes, and files. There are seven subcategories:

- **System Information** (page 852)
- **Network Adapters** (page 859)
- **Fonts** (page 861)
- **Printers** (page 861)
- **Startup Items** (page 862)
- **Windows Services** (page 862)
- **Installed Software** (page 863)
- **Installed Configuration Profiles** (page 864)
- **Missing Patches** (page 865)
- **Processes** (page 866)
- **Files** (page 867)
- **Registry Entries** (page 870)
- **Computer Tracking** (page 870)

System Information

The **System Information** category contains information on the operating system and its settings.

Computer Name The name of the computer, as defined in the operating system.

Current User Name The full name of the user who is currently logged in on the computer. (For example, “Jane Doe”.) If no user is logged in, an empty string is displayed.

Current User Account The name of the current user’s account under which he or she is logged in. (For example, “janedoe” on macOS or “COMPUTER/JaneDoe” on Windows.)

Current User Is Admin Whether the currently logged-in user has administrator rights on the computer.

Last User Account The name of the account under which the current user is logged in on the computer. If no user is logged in, the name of the account of the last user who was logged in is displayed.

Last User Name The full name of the user who is currently logged in on the computer. If no user is logged in, the name of the user who was last logged in is displayed.

Idle Time

The time for which the client computer had been idle when its information was last updated on the LANrev server.

OS Platform

The general type and flavor of the operating system, for example, Windows XP Professional or macOS.

OS Version

The operating system's version number.

OS Build Number

The build number of the operating system.

OS Service Pack

Windows only: The latest operating system service pack installed on the computer.

OS Language

The user interface language of the operating system. For single-language operating systems like standard Windows XP installation, this is the installed language. For operating systems that can change the interface language dynamically, like macOS or Windows Vista, this is the currently chosen language.

OS Installation Date

Windows only: The date when this copy of the operating system was installed.

OS Activated

Windows only: Whether this copy has already been activated. This information item does not apply to Windows 2000.

OS Activation Grace Period

Windows only: The end of the grace period before which the operating system must be activated. This information item does not apply to Windows 2000.

OS Serial Number

Windows only: The serial number of this copy of the operating system.

OS Product ID

Windows only: The serial number of the individual copy of the operating system on this computer.

This is the ID number that is displayed in the **System** control panel's **General** tab.

OS Is Volume-Licensed

Windows only: Whether this copy of the operating system has been activated as part of a volume license. This information item applies to the same operating systems as the **OS Activated** information item described above.

Security Identifier

Windows only: The unique ID that Windows generates for use with Active Directory and other security-related purposes.

Virtual Machine

Windows only: The type of virtual machine inside which the agent is running. LANrev can currently identify Parallels, Virtual PC, and VMware. If the agent is not running inside a virtual machine, "native" is reported.

AD Computer Name

The name of the computer as specified in Active Directory.

AD Computer Organizational Unit The name of the Active Directory organizational unit to which the computer belongs.

AD Computer Organizational Unit Path The path of the Active Directory organizational unit to which the computer belongs.

AD User Organizational Unit The name of the Active Directory organizational unit to which the computer’s current user belongs.

AD User Organizational Unit Path The path of the Active Directory organizational unit to which the computer’s current user belongs.

AD User Is Member Of The Active Directory groups to which the computer’s current user belongs. Multiple groups are separated by commas.

AD Computer Is Member Of The Active Directory groups to which the computer belongs. Multiple groups are separated by commas.

Computer Is Behind NAT Is there a NAT router between the computer and the LANrev server?

NOTE This information item indicates whether the client has a NAT connection as viewed from the LANrev server, not as viewed from the Internet.

Darwin Version macOS only: The version of Darwin that is part of the operating system.

Daylight-Saving Time Is daylight-saving time in effect on the computer?

GMT Delta The difference between UTC (Universal Time, commonly known as GMT) and the computer’s clock.

Defender Installed Windows only: Is Windows Defender installed on this computer?

Defender Enabled Windows only: Is Windows Defender currently enabled on this computer?

Defender Real-Time Protection Windows only: Is Windows Defender’s real-time protection enabled on this computer?

Defender Auto Scan Enabled Windows only: Is Windows Defender’ automatic scanning feature enabled on this computer?

Defender Engine Version Windows only: The version number of the Windows Defender software.

Defender Definition Version Windows only: The version number of the malware definitions used by Windows Defender.

FileVault Supported

macOS only: Whether FileVault is available on this computer.

FileVault Enabled

macOS only: Whether FileVault is enabled on this computer.

FileVault Authenticated Restart Supported

macOS only: Whether this computer can be restarted remotely without entering a password locally when the FileVault recovery key is presented.

FileVault Has Personal Recovery Key

macOS only: Whether the computer has a standard, locally generated FileVault recovery key.

FileVault Has Institutional Recovery Key

macOS only: Whether an institution-wide FileVault recovery key has been set for this computer.

FileVault Unlocked Using Recovery Key

macOS only: Whether the computer is running and the last restart has been performed using the FileVault authenticated restart option.

FileVault Recovery Key Stored on Server

macOS only: Whether the FileVault recovery key for this computer is stored in LANrev Server. In addition to “Yes” and “No,” the value can be “Yes, not verified.” This indicates that a recovery key for this computer is stored on the server, but it is unknown whether this key is still valid. (For example, the user may have set a different key in the meantime.)

Disk Encryption Product

The name of the disk encryption software, if any, used on the administered computer.

This information is reported for Windows XP and Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.

Disk Encryption Version

The version of the disk encryption software used.

This information is reported for Windows XP and Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.

Disk Encryption Status

The state of the disk encryption on the administered computer as reported by disk encryption software.

This information is reported for Windows XP and Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.

Disk Encryption Algorithm

The encryption algorithm used by disk encryption software, as reported by the software.

This information is reported for Windows XP and Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.

Disk Encryption Key Size

The length, in bits, of the encryption key used, as reported by the software.

This information is reported for Windows XP and Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.

Fast User Switching Enabled Is fast switching between user accounts (that is, without having to close all applications and logging out before using a different account) enabled on this computer?

Firewall Enabled Is the operating system’s built-in firewall enabled on this computer?

Personal File Sharing macOS only: Is Personal File Sharing enabled on the computer?

Windows File Sharing macOS only: Is file sharing for Windows enabled active on the computer?

Personal Web Sharing macOS only: Is Personal Web Sharing enabled on the computer?

Remote Login macOS only: Is remote login enabled on the computer?

FTP Access macOS only: Is FTP access enabled on the computer?

Remote Apple Events macOS only: Is the Remote Apple Events service enabled on the computer?

Printer Sharing macOS only: Is Printer Sharing enabled on the computer?

Remote Management macOS only: Is Apple Remote Desktop remote management access (apart from screen sharing) enabled?

Remote Desktop Screen Sharing Is screen sharing via Apple Remote Desktop or Microsoft Remote Desktop, respectively, enabled on the computer?

Timbuktu Access Can this computer be remotely controlled via Timbuktu?

VNC Access Can this computer be remotely controlled via VNC?

PC Anywhere Access Can this computer be remotely controlled via PC Anywhere?

DameWare Access Can this computer be remotely controlled via DameWare?

Allow Remote Assistance Windows only: Is Remote Assistance enabled on this computer?

Allow Remote Control via Assistance Windows only: Is controlling this computer via Remote Assistance enabled?

Wake on LAN Enabled macOS only: Is Wake on LAN (waking from sleep on administrative network access) enabled on the computer?

Wake on LAN Supported macOS only: Does this computer support Wake on LAN?

OS Update Utility Enabled Is the local update utility of the operating system (that is, Software Update on macOS and Windows Update on Windows computers) enabled on this client?

Time Machine Auto Backup Enabled

macOS 10.5 or later only: Whether Time Machine is currently set to make automatic backups. (This is equivalent to the master switch in the Time Machine control panel to be set to **On**.)

Time Machine Status

macOS 10.5 or later only: The status – idle or performing a backup – of Time Machine on this computer.

Time Machine Backup Disk

macOS 10.5 or later only: The name of the volume to which Time Machine is currently set to back up.

Time Machine Latest Backup

macOS 10.5 or later only: The time when the most recent Time Machine backup was performed.

Time Machine Oldest Backup

macOS 10.5 or later only: The time when the first Time Machine backup was performed.

Time Machine Snapshot Count

macOS 10.5 or later only: The number of snapshots in the Time Machine backup on this computer.

NOTE This is not the number of snapshots that Time Machine has taken but only the number of those that are currently retained. For example, Time Machine takes hourly backups but after a day or so discards all of a day’s backups except for one.

Time Machine Disk Size

macOS 10.5 or later only: The formatted capacity of the Time Machine backup disk.

Time Machine Disk Free

macOS 10.5 or later only: The current unused capacity of the Time Machine backup disk.

Computrace Identifier

The Computrace identification number of the computer (formerly know as ESN). This information is only available for computers on which a Computrace client is installed.

Computrace Agent Last Call Time

The time and date when the Computrace client on this computer contacted the Computrace server. This information is only available for computers on which a Computrace client is installed.

Computrace Agent Next Call Time

The time and date when the Computrace client on this computer is scheduled to contact the Computrace server the next time. This information is only available for computers on which a Computrace client is installed.

Inventory Received

The time when the most recent contact regarding inventory information was made with this agent. (Note that the contact may also have been a notification by the agent that nothing has changed since the last contact.).

Inventory Updated

The time when the most recent update of the inventory information for this computer was performed on the LANrev server.

Font Info Updated

The time when the most recent update of the installed font information for this computer was performed on the LANrev server.

Printer Info Updated

The time when the most recent update of the printer information for this computer was performed on the LANrev server.

Startup Item Info Updated

macOS: The time when the most recent update of the startup item information for this computer was performed on the LANrev server.

Installed Software Info Updated

The time when the most recent update of the installed software information for this computer was performed on the LANrev server.

Missing Patches Info Updated

The time when the most recent update of the missing patches information for this computer was performed on the LANrev server.

Windows Services Info Updated

Windows only: The time when the most recent update of the Windows services information for this computer was performed on the LANrev server.

Computer Tracking Info Updated

The time when the most recent update of the computer tracking information for this computer was performed on the LANrev server.

Process Info Updated

The time when the most recent update of the process information for this computer was performed on the LANrev server.

Custom Info Items Updated

The time when the most recent update of the custom information items for this computer was performed on the LANrev server.

Network Adapter Count

The number of active network adapters currently of the computer.

Font Count

The number of fonts installed on the computer that are included in the Fonts table in the LANrev database.

NOTE Collecting or updating font information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include font information” checked.

Printer Count

The number of printers defined on the computer that are included in the Printers table in the LANrev database.

NOTE Collecting or updating printer information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include printer information” checked.

Software Information

Startup Item Count

macOS only: The number of startup items on the computer that are included in the Startup Item table in the LANrev database.

NOTE Collecting or updating startup item information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include startup item information” checked.

Windows Service Count

Windows only: The number of services from this computer that are included in the LANrev database.

NOTE Collecting or updating service information is not automatic but has to be explicitly triggered by the **Gather Inventory Information** command with the option “Include service information” checked.

Installed Software Count

The number of installed software items from this computer that are included in the Installed Software table in the LANrev database.

NOTE Collecting or updating installed software information is not automatic but has to be explicitly triggered by the **Gather Installed Software** command.

Missing Patches Count

The number of software patches missing from this computer.

NOTE Collecting or updating information about installed (or missing) patches is not automatic but has to be explicitly triggered by the **Gather Installed Software** command.

Process Count

The number of processes running on the computer that are included in the Processes table in the LANrev database.

NOTE Collecting or updating process information is not automatic but has to be explicitly triggered by the **Gather Process Information** command.

File Count

The number of files located on the computer that are included in the Files table in the LANrev database.

NOTE Collecting or updating file information is not automatic but has to be explicitly triggered by the **Find File** command. Only files found by this command are stored in the LANrev database, not all files on searched target computers.

Network Adapters

The **Network Adapters** category contains information on the active network adapters of a computer. (Active adapters are those currently assigned an IP address.)

Adapter Name
The label of the network adapter, for example, Ethernet or AirPort.

Adapter IP Address
The IP address assigned to the network adapter.

Adapter Subnet Mask
The subnet mask assigned to the network adapter.

Adapter MAC Address
The MAC address of the network adapter.

Router Address
The IP address of the router assigned to the network adapter.

DHCP Server Address
The IP address of the DHCP server, if any, that currently supplies the IP address to the network adapter.

DNS Servers
The IP addresses of all DNS servers which the network adapter is set to contact to resolve names into IP addresses. If multiple DNS servers are specified, their IP addresses are separated by commas.

Search Domains
macOS only: The default search domains specified for the network adapter. If multiple domains are specified, they are separated by commas.

Configuration Type
The way in which the network adapter has been configured, for example, DHCP or manually.

TCP Implementation
macOS only: The general type of TCP stack in use on the network adapter.

Primary Interface
Is this the network adapter currently being used as the main IP interface of this computer?

Device Name
The logical name of the network adapter.

Link Status
Whether the network link on this network adapter is up or down.

Adapter Speed
The nominal data rate on this network adapter’s current connection.

Full Duplex
macOS only: Is the network adapter currently operating in full duplex mode (as opposed to half duplex)?.

MTU
macOS only: The MTU (maximum transmission unit) size that is currently specified on the network adapter.

Adapter Vendor
The manufacturer of this network adapter.

Hardware
The hardware category of the network adapter.

Scope ID
Windows only: The scope ID that is set for this network adapter.

DNS Suffix
Windows only: The TCP domain that is currently assigned to this network adapter.

Host

Windows only: The name that is displayed for this computer in the network connected to this network adapter.

WINS Resolution

Windows only: The mode for resolving WINS (Windows Internet Name Service) addresses specified for this network adapter.

WINS Server

Windows only: The servers specified on this network adapter for resolving WINS addresses.

Enable DNS for WINS Resolution

Windows only: Can this computer use DNS in addition to WINS to resolve network addresses in the network connected to this adapter?

Enable LMHOST Lookup

Windows only: Can this computer use the LMHOST file to resolve network addresses in the network connected to this adapter?

Fonts

The **Fonts** category contains information on the fonts installed on a computer.

NOTE The information items in this category do not list all fonts on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include font information”.

Font Name

The name of the font.

Font Type

The general font format, such as bitmap, TrueType, PostScript, etc.

Sizes

The type sizes in which this font is available. This is relevant only for bitmap fonts; for vector fonts, “All Sizes” is displayed.

Printers

The **Printers** category contains information on the printers defined on a computer.

NOTE The information items in this category do not list all printers on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option “Include printer information”.

Printer Name

The name under which the printer is defined.

Printer Model

A description of the make and model of the printer.

Location

The location of the printer, as specified in the printer definition. If the user did not specify a location, some drivers provide default location information.

Printer Host Name

If the printer is connected to a print server, this is the network name or address of the server. Otherwise, the localhost is displayed.

Printer State macOS only: The current state of the printer.

Default Is this the default printer on the administered computer?

Remote Is this the printer connected via a print server?

PostScript macOS only: Does this printer support PostScript (Adobe PostScript or an emulation)?

Driver Version macOS only: The version number of the printer driver used for this printer. This information is not available for all printer drivers.

URI macOS only: The uniform resource identifier of the printer.

Printer ID The locally unique ID that the operating system assigns to the printer.

Startup Items

The **Startup Items** category contains information on the startup items specified on a computer. This category applies only to administered macOS computers.

NOTE The information items in this category do not list all startup items on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option "Include startup item information".

Startup Item Name macOS only: The file name of the startup item.

Provides macOS only: The name of the service that the startup item offers.

Startup Item Description macOS only: A brief description of the startup item, supplied by the startup item's developer in the file.

Path macOS only: The path of the startup item's file.

Uses macOS only: any other services that this startup item requires.

Windows Services

The **Windows Services** category contains information on the services available on a computer. This category applies only to administered Windows computers.

NOTE The information items in this category do not list all services on administered computers but only those that have explicitly been collected by means of the **Gather Inventory Information** command with checked option "Include service information".

Service Name Windows only: The internal name of the service.

Service Display Name Windows only: The name of the service as it is displayed to the user.

Service Description Windows only: A brief description of the service, supplied by the service's developer in the file.

Service Status Windows only: The current operating state of the service (started or stopped).

Service Startup Type Windows only: The startup type currently set for the service (automatic, manual, or disabled).

Service Log On As Windows only: The user account in which the service is running.

Service Executable Path Windows only: The location on the client's hard disk of the service's executable file.

Installed Software

The **Installed Software** category contains information on installed software that has been found by the **Gather Installed Software** command.

NOTE For summary information on installed software, see "Installed Software Statistics" on page 891.

Inst. Software Name The name of the software.

Inst. Software Company Windows only: The name of the company that produced the software.

Inst. Software Version String The full version information for the software.

Inst. Software Version Number The version number of the software. This may be "n/a" if no valid version number can extracted from the version string (see above).

Inst. Software Size The size of the installed software on the disk.

Inst. Software Installation Date The date and time when the software has been installed on the client computer.

Inst. Software Info macOS only: Additional information from the software's version information file.

Inst. Software File Architecture macOS only: The instruction architecture used by the code contained in a file. This information is not available for installed software that has been found using installer receipts.

The range of possible values is the same as for the **File Architecture** information item described on page 868.

Uninstallable Windows only: Is there an uninstallation entry for the software on the client computer?

Is Hotfix Windows only: Is this software marked as a hotfix?

Identification Type The method by which LANrev has found this software.

Install Location The path of the software on the client computer. This information is not available for software that has been identified by its installer receipt.

Inst. Software Product ID For macOS software this is the software's bundle identifier. For Windows software, it is the ID noted in the registry.

Registered Company Windows only: The company to which this product has been registered. (Which usually will be the name of your company or organization.)

Registered Owner Windows only: The person to which this product has been registered.

Installed By Windows only: The name of the user account under which the software has been installed.

Uninstall String Windows only: The command string that will be used by the installer for removing the software. (If and when it is so directed by a user.)

Installer Receipt ID The identifier of the installer receipt by which the software was identified. This information is available only for software that has been found through its installer receipt.

Installed Configuration Profiles

The **Installed Configuration Profiles** category contains information about configuration profiles that are installed on administered computers.

These information items can be used in the **Server Center** window.

Installed Profile Name The name of the configuration profile.

Installed Profile Description The optional description string of the profile.

Installed Profile Organization The optional name of the organization which has provided the profile.

Installed Profile Identifier The identifying string of the profile.

Installed Profile UUID The unique identifier of the profile.

Installed Profile for User The user for whom this profile has been installed. For device profiles, this information items contains "n/a".

Installed Profile Installation Date The date and time when this profile was installed on the administered computer.

Installed Profile Type The type of profile – device profile or user profile. Device profiles contain settings that always apply to the device on which they are installed, user profiles contain settings that apply only when the corresponding user account is used.

Installed Profile Allow Removal
Whether the profile can be removed remotely.

Installed Profile Verification State
Whether the signature of the profile, if any, could be verified. Possible values include “unsigned”, “verified”, “not verified” (which may indicate an unauthorized change), and “unknown”.

Installed Profile Status
Whether the profile is installed with no change pending (“installed”) or will be removed once the user to which it applies logs back in to the computer.

Missing Patches

The **Missing Patches** category contains information on operating system and third-party patches that are missing on client computers.

NOTE The information items in this category list only those missing patches that have been collected by means of the **Gather Installed Software** command.

Missing Patch Name
The name of the missing patch.

Missing Patch Version
The version number of the missing patch.

Missing Patch Release Date
Windows patches and third-party patches only: The date when this patch was released by the software vendor.

Missing Patch Install Deadline
Windows only: The date recommended by Microsoft by which this patch should be installed.

Missing Patch Is Mandatory
Windows only: Whether Microsoft has marked this patch as mandatory.

Missing Patch Action
Windows only: Whether this patch includes an install or an uninstall action.

Missing Patch Is Beta
Windows only: Is this patch marked as beta-level software?

Missing Patch Superseded by Package
Windows only: Whether a later patch is available that supersedes this patch.

Missing Patch Language
Windows only: The operating system language for which this patch is intended.

Missing Patch Description
Windows patches and third-party patches only: The description of the patch, as provided by the source of the patch.

Missing Patch Severity

Windows and third-party patches only: The rated severity of this patch. This information is supplied by the source of the patch and may not be present for all patches.

Missing Patch Security Bulletin Numbers

Windows patches only: The number of the security bulletin describing the patch. If there are multiple numbers, they are separated by commas.

Missing Patch Is OS Patch

Is this patch an operating system patch? Patches that are not operating system patches are third-party patches.

Processes

The **Processes** category contains information on the processes running on a computer.

NOTE The information items in this category do not list all processes on administered computers but only those that have explicitly been collected by means of the **Gather Process Information** command.

Process Name

The name of the process. The names of zombie processes on macOS are enclosed in parentheses.

Process File Type

macOS only: The file type code of the file from which the process has been launched.

NOTE Not all files on macOS computers have file type codes.

Process File Creator

macOS only: The file creator code of the file from which the process has been launched.

NOTE Not all files on macOS computers have file creator codes.

Process ID

The ID number of the process.

User ID

The ID of the user account from which the process was launched.

Username

The name of the user account from which the process was launched.

Session ID

Windows only: The ID of the session to which the process belongs. This applies only to PCs with multiple users.

Process Executable Path

The path the to file from which the process has been launched.

NOTE Not all processes are launched from files.

Process Architecture

macOS only: The instruction architecture used by the process, Intel or PowerPC.

Group ID

macOS only: The ID of the group to which the user account belongs from which the process was launched.

Group Name

macOS only: The name of the group to which the user account belongs from which the process was launched.

Parent Process ID

The ID number of the process that has launched this process.

Parent Process Name

The name of the process that has launched this process.

Real User ID

macOS only: The process' real user ID, that is, the ID of the user who launched the process.

Real Username

macOS only: The process' real username, that is, the account name of the user who launched the process.

Real Group ID

macOS only: The process' real group ID, that is, the ID of the group to which the user belongs who launched the process.

Real Group Name

macOS only: The process' real group name, that is, the name of the group to which the user belongs who launched the process.

Launch Date

The date and time when the process was launched.

Background Only

macOS only: Is this process an interfaceless background process?

Virtual Memory

Windows only: The amount of virtual memory that has been allocated to the process.

Threads

Windows only: The number of threads of which this process consists.

Page Faults

Windows only: The number of page faults that this process has generated since it has been launched.

Process Priority

Windows only: The priority that the process has on the computer, from 0 through 31. Higher numbers denote higher priorities.

Files

The **Files** category contains information on the files and folders that have been found on a computer.

NOTE The information items in this category do not list all files and folders on administered computers but only those that have explicitly been searched for by means of the **Find File** command.

File Name

The name of the file, including any extensions.

File Path

The path of the file, including the file name.

File Type macOS only: The type code of the file.

NOTE Not all files on macOS computers have file type codes.

File Creator macOS only: The creator code of the file.

NOTE Not all files on macOS computers have creator codes.

File Bundle Identifier macOS only: The unique identifying string for the file bundle, if any. (For example: com.apple.systempreferences.)

NOTE Not all files on macOS computers have file creator codes.

File Size The amount of data in the file.

File Creation Date The date and time when the file was first created.

File Modification Date The date and time when the file was last modified.

File Access Date The date and time when the file was last opened.

File Backup Date macOS only: The date and time when the file was last backed up.

NOTE Some backup utilities may not set this date when backing up a file.

File Version The version number of the file, as stored in the file.

NOTE When you use the File Version information item in specifications for smart groups and for other comparison purposes, LANrev uses the comparison string to determine the operating system platform you target: If the version number you specify to compare the information item’s contents with has fewer than three dots, it is considered a macOS version. With three dots, LANrev assumes it to be a version of a Windows file. It is not possible to specify a search condition that works on both platforms.

File Version String macOS only: A textual description of the file version that is available for some files. This information item can sometimes help to differentiate between two different versions with the same version number or provide version information when no proper version number is available.

File Build Number The build number of the file, as stored in the file.

File Architecture macOS only: The instruction architecture used by the code contained in a file. This information is available only for executable files.

These values are supported:

- Universal (Intel, PowerPC)
- Universal (Intel, PowerPC/64bit)
- Universal (Intel, PowerPC, PowerPC/64bit)
- Universal (PowerPC, PowerPC/64bit)
- Intel
- PowerPC
- PowerPC/64bit
- PowerPC (CFM)
- Shell Script
- Classic
- Unknown

Unix Permissions macOS only: The read, write and execute permissions set for the file, in both letter and numeric notation.

Unix Owner macOS only: The user account who is the file’s owner.

Unix Group macOS only: The user group to which the file is assigned.

Is Alias Is this file an alias (or, on Windows, a shortcut)?

Is Application Is this file an application file (including macOS application packages)?

Is Classic App macOS only: Is this file an application file that must run in the Classic environment?

Is File Is this a file (as opposed to a package or a folder)?

Is Hard Link macOS only: Is this a Unix hard link file?

Is Invisible Is this file marked as being invisible?

Is Locked macOS only: Is this file locked against modification?

Is Open macOS only: Is this file currently open?

Is Package macOS only: Is this file a macOS package (a folder looking like a file)?

Is Stationery macOS only: Is this file marked as stationery?

Is Symbolic Link macOS only: Is this a Unix symbolic link file?

Is Scriptable macOS only: Is this file an application that can be controlled through AppleScript?

Has Custom Icon macOS only: Does this file have a custom icon (an icon for this file only, as opposed to an icon for all files of this type)?

File Found Has this file been found during the last update of file information for this computer?

File Record Modification Date
The last time that this file record was modified.

Registry Entries

The **Registry Entries** category contains information on the registry entries that have been found client computers.

NOTE The information items in this category do not list all registry entries on administered computers but only those that have explicitly been searched for by means of the **Search Windows Registry** command.

Registry Name
Windows only: The name of the found registry entry.

Registry Value Type
Windows only: The data type of the found registry value. For registry keys, this is "n/a".

Registry Value
Windows only: The data of the found registry value. For registry keys, this is "n/a".

Full Registry Path
Windows only: The path of the found registry entry in the registry.

Registry Value Number
Windows only: The data of the found registry value if the value has the type Number.

Registry Value String
Windows only: The data of the found registry value if the value has the type String.

Registry Value Binary
Windows only: The data of the found registry value if the value has the type Binary.

Registry Entry Found
Windows only: Whether the specified registry entry was actually found on the target computer. When searching registries, it is possible to specify that an entry with the value "No" in the **Registry Entry Found** information item is added for a computer on which the specified entry was not found.

Registry Record Modification Date
Windows only: The date and time when this registry record in the LANrev database was last updated.

Computer Tracking

The **Computer Tracking** category contains information on tracked client computers.

Tracked Computer Time Stamp
The date and time (according to the LANrev server's clock) of the last contact with the tracked computer.

Tracked Computer Address
The IP address that the tracked computer currently has in the local network in which it is located.

Tracked Computer Router Address
The IP address of the router that the tracked computer is currently using.

Tracked Computer Public Address The IP address that the tracked computer currently has in the Internet.

Tracked Computer GMT Delta The current time difference between the tracked computer's internal clock and universal time (GMT).

Tracked Computer Current User Name The name of the current user who is active on the tracked computer. (See "Current User Name" on page 852.)

Tracked Computer Current User Account The full name of the account that is currently active on the tracked computer. (See "Current User Account" on page 852.)

Tracked Computer Resolved Address The DNS name that the tracked computer currently has in the local network in which it is located.

Tracked Computer Resolved Router Address The DNS name of the router that the tracked computer is currently using.

Tracked Computer Resolved Public Address The DNS name that the tracked computer currently has in the Internet.

Tracked Computer Time The date and time (according to the tracked computer's local clock) of the last contact with the tracked computer.

Commands

Information items in the **Commands** section contain information on related to commands that you have issued to the clients. There are three subcategories:

- **Commands** (page 871)
- **Command Queue** (page 872)
- **Command History** (page 872)

Commands

The **Commands** category contains information item related to commands sent from LANrev Admin to administered computers. They can be used only in the **Commands** window.

Command Name The name of the command. This is the menu item in the **Commands** menu with which the command is initiated.

Command Description The description of the command, as entered in the **Command description** field in the command scheduling dialog. If the command has no individual description, a default description is displayed.

Is Repeating Command Whether this command has been marked as a repeating command in its **Options** dialog.

Interval The interval in which the command is specified to be executed.

Interval Unit

The unit for the execution interval (see **Interval**, above).

Creation Time

The date and time when the command was entered in the command queue (when the **Execute** button in the command window was clicked).

Command Queue

The **Command Queue** category contains information items related to commands sent from LANrev Admin to administered computers that have not yet been completed. They can be used only in the **Queued Commands** view of the **Commands** window and other smart groups in that window that display queued (not yet completed) commands.

Scheduled Time

The date and time when the command is scheduled to be executed. In the case of deferred commands, this time may lie in the past.

Command Status

The current execution status of the command – scheduled, deferred, or executing.

Command History

The **Command History** category contains information item related to commands sent from LANrev Admin to administered computers that have been completed. They can be used only in the **History**, **Failed Commands**, and **Commands in Last 24 Hours** views of the **Commands** window as well as in other smart groups in that window that display completed commands.

Start Time

The date and time when the execution of the command has started.

Finish Time

The date and time when the execution of the command was completed.

Command History Status

The success or otherwise of the command execution.

Command Result Error

The error that was generated by the command. If the command was executed successfully, this is “No error”.

Command Error Info

Additional information on the nature of the error that is available for some errors.

Server Center

Information items in the **Server Center** section contain information on software distribution, license monitoring, and administrator accounts. There are these subcategories:

- **Administration** (page 873)
- **Actions** (page 877)
- **Software Distribution** (page 878)
- **License Monitoring** (page 886)
- **Computer Groups** (page 890)

Administration

Information items in the **Administration** category contain information on the administrators assigned to computers. There are three subcategories:

- **Administrators** (page 873)
- **Appointments** (page 876)
- **Active Directory Users** (page 877)

Administrators

The **Administrators** category contains information about administrator accounts. They can be used only in the **Server Center** window.

Administrator Name

The account name of this administrator account.

This information item can also be added to tables that list managed computer or mobile devices. In that case, it lists the administrators that are appointed to manage the devices.

Is Superadmin

Does this administrator account have superadministrator privileges?

Can Manage All Devices

Is is possible to manage all administered computers and mobile devices from this administrator account, even those to which the account is not expressly assigned?

Account Enabled

Can users currently log in to this administrator account? (That is, is the account currently enabled?)

Limit Number of Incorrect Login Attempts

Will this account be locked if a specified number of incorrect passwords are entered in a row?

Failed Login Attempts

How many times has an incorrect password been specified for this account since the last successful login? (If the last login attempt was successful, this number is zero.)

Maximum Login Attempt Failures

The maximum number of incorrect passwords that may be entered in a row before the account is disabled. When the value in the Failed Login Attempts field reaches this value, and Limit Number of Incorrect Login Attempts is “Yes”, the account is disabled.

Deploy Agents

Can LANrev Agent be installed and other Agent Deployment Center functions be used by this administrator account?

View Software Distribution Settings

Can the software distribution settings be displayed using this administrator account?

View License Monitoring Settings

Can the license monitoring settings be displayed using this administrator account?

View Administrator Settings

Can the administrator settings be displayed using this administrator account?

View Custom Information Fields
Can custom information field definitions be displayed using this administrator account?

View Server Status
Can the server status be displayed using this administrator account?

View Commands Window
Can the **Commands** window be opened using this administrator account?

View Computer Tracking Data
Can computer tracking information be displayed using this administrator account?

View Computer Tracking Screenshots
Can screenshots taken as part of the computer tracking be displayed using this administrator account?

Modify Server Settings
Can server settings be modified using this administrator account?

Modify Custom Information Fields
Can custom information field definitions be modified using this administrator account?

Enter Custom Field Data
Can the contents of custom information fields be edited using this administrator account?

Modify Software Packages
Can software packages be edited using this administrator account?

Modify Disk Images
Can disk images for the Software Distribution Center be edited using this administrator account?

Modify Computer Groups
Can computer groups be edited using this administrator account?

Modify Distribution Points
Can distribution point specifications be edited using this administrator account?

Modify Configuration Profiles
Can configuration profiles be edited using this administrator account?

Modify Desktop Actions
Can this administrator create and edit actions for assignment to smart computer groups?

Reset Software Packages
Can software packages be reset (as per the **Reset Package** command) using this administrator account?

Retry Software Packages
Can software packages be retried (as per the **Retry Package** command) using this administrator account?

Remove SD Log Entries
Can software distribution log entries be deleted using this administrator account?

Modify License Specifications
Can license specifications be edited using this administrator account?

Remove License Reports

Can entries in the reports in the License Monitoring Center be deleted using this administrator account?

Remove History Commands

Can entries in the command history be deleted using this administrator account?

Change Command History Options

Can the options for recording a command in the command history (in the command's **Options** dialog) be edited using this administrator account?

Remove Computer Records

Can computer records be deleted from browser windows using this administrator account?

Remove Inventory Data

Can inventory data for computers be deleted using this administrator account?

Change Computer Tracking

Can computer tracking settings be edited from this administrator account?

Enable Computer Tracking Screenshots

Can making screenshots as part of the computer tracking be enabled from this administrator account?

Remote Control

Can remote controlling of administered computers be initiated from this administrator account?

Manage Mobile Devices

Can this administrator change settings for managed mobile devices and send commands to them?

Manage Device Users

Can this administrator import device user records and delete them?

Modify Enrollment Users

Can this administrator specify enrollment users and device owners for mobile devices?

Mobile Remote Control

Can this administrator view and control the screens of compatible managed mobile devices?

Modify Mobile Applications

Can this administrator create and edit mobile application packages?

Modify Mobile Configuration Profiles

Can this administrator create and edit configuration profiles for mobile devices?

Modify Mobile Media

Can this administrator create and edit media files for mobile devices?

Modify Mobile Actions

Can this administrator create and edit actions for assignment to smart policies

Modify Mobile Device Policies

Can this administrator create and edit policies and smart policies for mobile devices?

Change Device Enrollment Program Account

Can this administrator specify and edit account settings for Apple's device enrollment program?

Change VPP Account Settings

Can this administrator specify and edit account settings for Apple’s volume purchase program?

Modify Bookstore Books

Can this administrator create and edit records for books from the iBooks Store?

Modify Device Enrollment Profiles

Can this administrator create, edit, and assign device enrollment profiles?

Modify VPP License Management

Can this administrator assign and revoke VPP app and book licenses?

Classroom Management

Can this administrator use the **Classroom Management** window and associated functions for managing classroom settings?

Modify Samsung KNOX Accounts

Can this administrator enter and modify information about Samsung KNOX accounts?

Remove Mobile Device Records

Can this administrator remove records for mobile devices from the LANrev database?

Remove Mobile Device History Commands

Can this administrator remove entries in the mobile device command history?

View Mobile Device Tracking Data

Can this administrator see the geolocation information of managed mobile devices?

Change Mobile Device Tracking

Can this administrator enable and disable mobile device tracking?

Change Agent General Settings

Can settings in the **General** pane of the **Agent Settings** dialog be edited from this administrator account?

Change Agent Server Settings

Can settings in the **Servers** pane of the **Agent Settings** dialog be edited from this administrator account?

Change Agent Client Info Settings

Can settings in the **Client Information** pane of the **Agent Settings** dialog be edited from this administrator account?

Change Agent Custom Field Settings

Can settings in the **Custom Fields** pane of the **Agent Settings** dialog be edited from this administrator account?

Is AD User

Is this an Active Directory user account? (As opposed to a user account that has been created in LANrev.)

Appointments

The **Appointments** category contains information about appointment groups. They can be used only in the **Server Center** window.

Appointment Group Name

The name of this appointment group.

Active Directory Users

The **Active Directory Users** category contains information about Active Directory accounts that are being made available for use as LANrev administrator accounts. These information items can be used only in the **Server Center** window.

AD Display Name
The displayed account name of this Active Directory account.

AD Account Name
The internal account name of this Active Directory account.

AD Login Name
The name with which users can log into this Active Directory account.

AD Account Disabled
Is this account currently disabled in Active Directory?

Actions

Information items in the **Actions** category contain information on the administrators assigned to computers. There are three subcategories:

Desktop Action Type
The type of the action, for example, send message or gather inventory.

Desktop Action Description
The description of the action that was specified when the action was created.

Desktop Action Name
The name of the action that was specified when the action was created.

Desktop Action Supported Platforms
The operating system platforms to which this action applies.

Desktop Action Unique Identifier
The unique identifier that LANrev has given this action.

Desktop Action Assignment Initial Delay
The delay specified in the action’s execution options before it is executed on any target devices.

Desktop Action Assignment Repeat Count
The number of times that the action is executed on each target device, as specified in the action’s execution options.

Desktop Action Assignment Repeat Interval
The amount of time between repeat executions of the action on the same target device, as specified in the action’s execution options.

Desktop Action Execution Error Info
The error information, if any, returned from the last execution of the action.

Desktop Action Execution Time
The time when the action was last executed.

Desktop Action Execution Status
The current execution status of the action.

Software Distribution

Information items in the **Software Distribution** category contain information on the elements of the software distribution system. There are six subcategories:

- **Packages** (page 878)
- **Payloads** (page 882)
- **Configuration Profiles** (page 882)
- **Distribution Points** (page 883)
- **Disk Images** (page 884)
- **Installation Status** (page 884)
- **Configuration Profile Installation Status** (page 885)
- **Mac App Store Applications** (page 885)

Packages

The **Packages** category contains information about software packages and metapackages. They can be used only in the **Server Center** window, for smart groups displaying software packages.

Package Name

The name of the software package.

Package Unique ID

The unique ID of the software package.

Package Type

The kind of software contained in the software package, whether a regular package (created manually in LANrev) or one of several kinds of patch packages (created by the automated patch process).

Executable Payload

The name of the payload in the package that has been specified as being executable.

Is Metapackage

Is this package a metapackage?

Executable Size

The size of the installer specified in the package.

Executable Options

The command-line options to use for the specified installer.

Target Installation Volume

The name of the volume, if any, of the target computers on which the software is to be installed.

Continue Installation After Failure

Whether the installation of this metapackage is to continue even if there is a failure installing one of the contained packages. (This information item applies only to metapackages, not standard packages.)

Package Description

The description of the software package that has been entered in the **Software Package** dialog.

Availability Date

The earliest time when this package can be used for installations, as specified in the package.

Install At

The general occasion on which this package is to be installed – at any time, after the next restart, or after the next login.

Install When User Is Logged In

Is this package to be installed when a user is logged in at install time?

Install When No User Is Logged In

Is this package to be installed when no user is logged in at install time?

Install Time Start

If the package may be installed only during a certain time of the day, this is the beginning of the specified interval.

NOTE The content of this information item is disregarded when any Install Time Option other than “Between” has been chosen.

Install Time End

If the package may be installed only during a certain time of the day, this is the end of the specified interval.

NOTE The content of this information item is disregarded when any Install Time Option other than “Between” has been chosen.

Priority

The installation priority of the package.

Distribution Point Selection

Which distribution point may be used for installing this software package – any, preferably servers from the target computer’s local zone, or exclusively servers from the local zone?

Installation Context

The user context in which this package is to be installed.

Installation Context User

The user account which is to be the context in which this package is to be installed. This information item is relevant only when the installation context is “Other user”.

Requires Admin Privileges

Does the installation of this software package require administrator privileges on the target computer?

Keep Package File After Installation

Will leave LANrev Agent the downloaded installation files on the target computer’s hard disk instead of deleting it?

Allow On-Demand Installation

Is the package available for pull-installation by the user (instead of the standard push-installation?

Don’t Install on Slow Network

Is this software package set to install only when there is at least a 100 Mbit/s connection to the target computer?

Payload Download Time

When LANrev is to download the payload to the client computers, before or after displaying any user dialogs.

Target OS Platform

The operating system family – macOS or Windows – for which this software package is intended.

Minimum OS

The earliest version of the operating system that supports the software package.

Maximum OS

The latest version of the operating system that supports the software package.

Platform Architecture

The processor architecture (processor type and bit width) required by the installed software as specified in the software package’s specification.

User Interaction

The type of involvement by the local users of target computers allowed by the package.

Auto Start Installation

The number of minutes after which the installation from the package is started automatically on a client if the notification dialog has not been answered by the user.

Allow to Defer For

The number of minutes for which the local user of a target computer can defer this installation.

NOTE If the interval is specified in the package in a unit other than minutes, it is converted to minutes in this information item.

Installation Deadline

The latest date by which the installation of the package must start.

Display Installation Progress

Whether LANrev Agent is to display the progress of this package’s installation.

Action after Installation

Which action, if any, is the agent to take after completing the installation?

Close Install Notification After

The time in minutes after LANrev Agent automatically closes the notification dialog on the target computer if the local user does not acknowledge it.

Restart Notification

Whether LANrev Agent is to display a notification before it restarts the computer after having installed this package.

Allow to Postpone Restart

Whether the local user of the target computer can postpone the restart after the end of the installation.

Repeat Restart Notification

The interval in which LANrev Agent is to display a restart notification while the local user of the target computer keeps postponing the restart.

Warn About Slow Network

Is the local user of the target computer to be warned before the installation of this software package is the network connection is slower than 100 Mbit/s?

Has Installation Condition

Whether any conditions have been specified for the package that must be met before installation commences.

See “Installation Conditions” on page 708 for details.

Is macOS Software Update

Whether this package is a software update from Apple that has automatically been turned into a software package by the Software Distribution Center.

Is Windows Software Update

Whether this package is a software update from Microsoft that has automatically been turned into a software package by the Software Distribution Center.

Software Patch Version

The version number of this software update. This information applies only to software packages created via the automated patch management.

Software Patch Recommended

macOS and third-party patches only: Whether the producer of the patch recommends installing this software update. (For macOS patches, this is equivalent to the update being checkmarked in the Software Update utility.) This information applies only to software packages created via the automated patch management.

Software Patch Severity

Windows and third-party patches only: The rated severity of this patch. This information is supplied by the source of the patch and may not be present for all patches.

Software Patch Security Bulletin Numbers

Windows patches only: The number of the security bulletin describing the patch. If there are multiple numbers, they are separated by commas.

Supported Operating Systems

The operating system versions or subtypes for which this patch is intended (for example, macOS 10.12 or Windows 8).

Patch Release Date

Windows patches and third-party patches only: The date when this patch was released by the software vendor.

Patch Install Deadline

Windows only: The date recommended by Microsoft by which this patch should be installed.

Patch Is Mandatory

Windows only: Whether Microsoft has marked this patch as mandatory.

Patch Action

Windows only: Whether this patch includes an install or an uninstall action.

Patch Is Beta

Windows only: Is this patch marked as beta-level software?

Patch Can Be Uninstalled

Windows only: Whether this patch can be uninstalled using the **Add/ Remove Software** control panel.

Superseded by Package

Windows only: Whether a later patch is available that supersedes this patch.

Patch Language

Windows only: The operating system language for which this patch is intended.

Requires Exclusive Install

Windows only: Whether this patch must be installed by itself, that is, not in one installation process together with other patches.

NOTE LANrev automatically handles such needs for exclusiveness; you do not need to do anything about it.

Requires Exclusive Uninstall

Windows only: Whether this patch must be uninstalled by itself, that is, not in one uninstallation process together with other patches.

Payloads

The **Payloads** category contains information about payloads. They can be used only in the **Server Center** window, for smart groups displaying payloads.

Payload Name

The name of the payload, as specified in the Payload dialog.

Executable Name

The name of the file contained in the payload.

Payload Size

The download size of the payload contents.

Upload Status

The current status of the process of uploading the payload to the distribution point.

Is Executable

Whether the payload has been marked as being executable in the Payload dialog.

Transfer All Files in Folder

Whether the software package is set to transfer all files from the specified installer’s folder for installations.

Executable Source

The path on your disk of the file contained in the payload.

Payload Unique ID

An ID for identifying the payload. The ID is guaranteed to be unique in this installation of LANrev.

Payload Notes

The notes that have been entered for this payload.

Configuration Profiles

The **Configuration Profiles** category contains information about configuration profiles for desktop computers. They can be used only in the **Server Center** window, for displaying configuration profiles.

Profile Name

The name of the configuration profile.

Profile Type

The type of the configuration profile, for example, “macOS Configuration Profile”.

Profile Description

The description of the configuration profile.

Profile Organization

The organization which has issued the configuration profile.

Profile Identifier

The unique identifier of the configuration profile, as entered by the creator of the profile.

Profile UUID

The automatically created globally unique ID of the configuration profile.

Profile Scope

Whether the profile sets user or device options.

Profile Allow Removal

Whether the profile may be removed from the computer by the user. Possible values include, “Never”, “Always”, and “With authentication”.

Distribution Points

The **Distribution Points** category contains information about distribution points. They can be used only in the **Server Center** window, for smart groups displaying distribution points.

Distribution Point Name

The name of the distribution point, as specified in the Server Center.

Address

The network address of the distribution point.

Port

The network port used by the LANrev agent on this distribution point.

Distribution Point Unique ID

The unique ID of the distribution point, which stays constant even if tis renamed.

Distribution Point Certificate Fingerprint

The fingerprint of the certificate validating the identity of the distribution point.

IP Range Start

If the distribution point is set to provide software packages only to a specific range of IP addresses, this is the lower limit of that range.

IP Range End

If the distribution point is set to provide software packages only to a specific range of IP addresses, this is the upper limit of that range.

Only Use Distribution Point When Assigned

Is this distribution point set to serve only client computers to which it has explicitly assigned (by way of computer groups or IP ranges)?

Max. Downloads

The maximum number of concurrent downloads that this distribution point is to support.

Current Load

The number of concurrent downloads currently in progress on this distribution point.

Allow More than Max. Downloads

Is this distribution point to support more than the specified maximum number of concurrent downloads if no other distribution points with free capacity are available?

Is Master Distribution Point

Is this distribution point set to be the master distribution point?

Distribution Point OS Platform

The operating system platform installed on the computer on the distribution point is running.

Packages Root Path

The path to the folder containing the software installers on this distribution point.

Distribution Bandwidth

The limit to the bandwidth for providing downloads to the clients that has been specified for this distribution point. If no limit has been set, “n/a” is displayed.

Mirroring Bandwidth

The limit to the mirroring bandwidth that has been specified for this distribution point. If no limit has been set, “n/a” is displayed.

Mirroring From

The start time of the mirroring interval specified for this server. If no mirroring time limit has been specified, “n/a” is displayed.

Mirroring Until

The end time of the mirroring interval specified for this server. If no mirroring time limit has been specified, “n/a” is displayed.

Disk Images

The **Disk Images** category contains information about disk image specifications. They can be used only in the **Server Center** window, for smart groups displaying disk images.

Disk Image Name

The name of the disk image specification.

Disk Image Size

The size of the selected disk image file.

Disk Image Upload Status

Whether the disk image file is available on the distribution points.

Disk Image File

The path of the selected disk image file.

Disk Image Distribution Point

The setting of the **Distribution point** option in the disk image specification (which specifies from which distribution points the image may be downloaded).

Installation Status

The **Installation Status** category contains information about the status of software installation processes initiated by the software distribution system.

Installation Status

The current status of the software installation.

Deferred Until

If the software installation is deferred, the time when the next installation attempt will be made.

Installation Result Error

The result of a completed installation.

Add. Status Information Additional status information that is available for some errors.

Installation Log Date The date and time when the log entry was made.

Configuration Profile Installation Status

The **Configuration Profile Installation Status** category contains information about the status of installation processes for computer configuration profiles initiated by the software distribution system.

Profile Installation Status The current status of the profile installation.

Profile Installation Result Error The result of a completed profile installation.

Profile Add. Status Information Additional status information that is available for some errors.

Profile Installation Log Date The date and time when the log entry was made.

Mac App Store Applications

The **Mac App Store Application** category contains information about software packages that have been created for Mac App Store applications.

Mac App Store Application Name The name of the application, as specified in the package.

Mac App Store Application Category The category of the application, as specified in the package.

Mac App Store Application Min OS Version The minimum version of macOS required to run the application, as specified in the package.

Mac App Store Application Short Description The short description of the application contained in the package.

Mac App Store Application Long Description The long description of the application contained in the package.

Mac App Store Application URL The URL of the application’s page in the Mac App Store.

Mac App Store Application Size The size of the application on disk.

Mac App Store Application Release Date The date when this version of the application became available in the Mac App Store.

Mac App Store Application Vendor

The company or programmer selling the application.

Mac App Store Application Vendor Web Page

The URL of the vendor’s web page for the applications, as specified on the application’s page in the Mac App Store.

Mac App Store Application ID

The ID that the application has in the Mac App Store.

Mac App Store Application Bundle Identifier

The string that uniquely identifies the application’s bundle.

Mac App Store Application Licenses Assigned

The total number of managed licenses (purchased through the App Store volume purchase program) for this app that have been assigned to users.

Mac App Store Application Licenses Purchased

The total number of managed licenses that have been purchased for this application through the App Store volume purchase program.

Mac App Store Application Licenses Remaining

The total number of managed licenses (purchased through the App Store volume purchase program) for this app that have not yet been assigned to users.

Mac App Store Application VPP Accounts

The names of all your accounts for the Apple volume purchase program that contain licenses for this application.

License Monitoring

Information items in the **License Monitoring** category contain information on the elements of the license monitoring system. There are five subcategories:

- **License Specification** (page 886)
- **Purchase Tracking** (page 887)
- **License Status** (page 888)
- **License History** (page 888)
- **License History Summary** (page 889)
- **License Status per Agent** (page 889)

License Specification

The **License Specification** category contains information items related to license specifications. They can be used only in the **Server Center** window.

License Specification Name

The name of the license specification.

Software Identified By

How the software to which the license applies is to be identified.

Licenses Owned

The number of available licenses for this software.

License Type

The type of license – by installation, by concurrent use, or prohibited software.

Scan All Volumes

Whether all volumes of a target computer are to be scanned for the licensed software (Yes) or just the boot volume (No).

Meter App Usage

Whether, in addition to the installed software, the running processes are to be checked as well for the licensed software.

Terminate App If License Exceeded

Whether LANrev agents are to terminate local copies of the software specified by this license if the number of floating licenses is exceeded.

Terminate Prohibited Apps

Whether LANrev agents are to forcefully terminate local copies of the software specified by this license.

Delete Prohibited Apps

Whether LANrev agents are to delete local copies of the software specified by this license.

Track as Missing Software

Whether the specified software is to be listed as missing when it is not found on a computer.

Purchase Tracking

The **Purchase Tracking** category contains information items related to purchase tracking data. They can be used only in the **Server Center** window; most of them correspond to items in the **Purchase Tracking** tab of the **License Specification** dialog.

Purchase Type

The kind of purchase.

Purchase Date

The date when the purchase happened.

Purchase Count

The number of licenses purchased.

Purchase Price

The price of the license purchase.

Purchase Software Version

The version of the software that was purchased.

Purchase Order Number

The order number of the purchase.

Purchase License Owner

The person or department who owns the purchased licenses.

Purchase Vendor Name

The vendor of the licenses.

Purchase Vendor Reference

A reference number for the purchase from the vendor’s company.

Purchase Vendor Contact

The contact person for the purchase at the vendor’s company.

Purchase Vendor Support

Contact information for technical support related to this purchase.

Purchase Maintenance Available

Has maintenance been purchased with these licenses?

Purchase Maintenance Begin

The start date of the purchased maintenance period, if any.

Purchase Maintenance End

The end date of the purchased maintenance period, if any.

Purchase Maintenance Price

The price of the maintenance purchase.

Purchase Maintenance Reference

The contract number or similar identification reference for the maintenance agreement, if any.

Purchase Notes

Any additional notes that have been entered for the purchase record.

License Status

The **License Status** category contains information items related to the status of licenses. They can be used only in the **Server Center** window.

Total Install Count

The number of client computers on which the licensed software is installed.

Total Running Count

The number of client computers on which the licensed software is currently running.

Total Usage Time

The overall time, in minutes, that the licensed software has been used on administered computers.

Total Launches

The total number of times that the licensed software has been started on administered computers.

Last Launch Date

The last date and time that the licensed software has been started on an administered computer.

License Status

The current status of this license – whether the use is within legal limits or exceeds them.

License Status Log Date

The timestamp for the license status – the exact date and time when the status was registered.

License History

The **License History** category contains information items related to historical license monitoring data. They can be used only in the **Server Center** window.

Total Install Count

The number of client computers on which the licensed software was installed when this license metering was taken.

Total Running Count

The number of client computers on which the licensed software was running when this license metering was taken.

Historic License Status

The status of this license – whether the use was within legal limits or exceeded them – at the time specified by the **Status Timestamp** information item.

Status Timestamp

The date and time when this license metering was taken.

License History Summary

The **License History Summary** category contains information items that provide statistical information about the license history. They can be used only in the **Server Center** window.

Min. Install Count

The smallest number of client computers with the licensed software installed that has been encountered in the license history.

Avg. Install Count

The average number of client computers with the licensed software installed throughout the license history.

Max. Install Count

The largest number of client computers with the licensed software installed that has been encountered in the license history.

Min. Running Count

The smallest number of client computers running the licensed software that has been encountered in the license history.

Avg. Running Count

The average number of client computers running the licensed software throughout the license history.

Max. Running Count

The largest number of client computers running the licensed software that has been encountered in the license history.

First Status Timestamp

The date and time when this licensed software was first found.

Latest Status Timestamp

The date and time when this licensed software was most recently found.

License Status per Agent

The **License Status perAgent** category contains information items related to the license status of individual computers.

Install Count

The number of times the licensed software is currently installed on this computer.

Running Count

The number of times the licensed software is currently running on this computer.

Usage Time

The overall time, in minutes, that the licensed software has been used on this computer.

Number of Launches

The total number of times that the licensed software has been started on this computer.

Last Launch Date

The last date and time that the licensed software has been started on an administered computer.

Report Date

The date and time when the status of this license specification on this client computer was reported.

Computer Groups

The **Computer Groups** category contains an information item related to the computer groups defined in the **Server Center** window.

You can use this information item in the **Server Center** window when the **Computer Groups** category is selected and in any browser window displaying computer information.

Computer Group

The name of a computer group. If used in a browser window listing computers, the information item displays the name of a computer group to which the computer belongs.

Agent Deployment Center

Information items in the **Agent Deployment Center** section contain information on devices in the network, on LANrev agents installed on them, and on LANrev Agent installation or update processes. These information items can be used only in the **Agent Deployment Center** window.

Computer Name

The name or IP address of a found network device, depending on the type of zone.

Connection Status

The status of an installation in progress, if any. If no installation is in progress, the status is “idle”.

IP Address

The IP address of a found network device.

DNS Name

The DNS name of a found network device as specified on the local DNS server.

Agent Port

The port on which an installed LANrev agent is set to communicate.

Agent Status

The status of the detected device with regard to the LANrev agent installed on it – whether it is up to date, outdated, or missing. Devices on which no agent can be installed display “n/a”.

Installed Agent Version

The version number of the LANrev agent installed on the computer.

Installed Agent Build Number The build number of the LANrev agent installed on the computer.

Inventory Server The inventory server that an installed LANrev agent is set to use. If several inventory servers are specified, only the first is listed.

SSH Port The port that the SSH service on the device uses.

Access Status The possibility of accessing the computer using SSH.

Protocol The way in which the network device has been detected.

Deployment Result The result of the last installation or update of LANrev agent on this device from the Agent Deployment Center.

Deployment Result Message Additional information that is available for some errors.

Installed Software Statistics

The **Installed Software Statistics** category contains summary information on installed software that has been found by the **Gather Installed Software** command.

NOTE For information on individual installed software items on client computers, see “Installed Software” on page 863.

Inst. Software Stat Name The name of the installed software being summarized.

Inst. Software Stat Count The number of computers on which the installed software has been found.

Inst. Software Stat Company Windows only: The name of the company that produced the software.

Inst. Software Stat Size The size of the installed software on the disk.

Inst. Software Stat Info macOS only: Additional information from the software’s version information file.

Inst. Software Stat Uninstallable Windows only: Is there an uninstallation entry for the software on the client computer?

Inst. Software Stat Is Hotfix Windows only: Is this software marked as a hotfix?

Inst. Software Stat Identification Type The method by which LANrev has found this software?

Inst. Software Stat Installer Receipt ID The identifier of the installer receipt by which the software was identified. This information is available only for software that has been found through its installer receipt.

Missing Patch Statistics

The **Missing Patch Statistics** category contains summary information on which patches are missing on how many applicable computers. This information is collected by the **Gather Installed Software** command.

These information items can be used in the statistics categories of the **Missing Patches** window.

Missing Patch Stat Name The name of the missing patch being summarized.

Missing Patch Stat Version The version number of the missing patch being summarized.

Missing Patch Stat Count The number of computers on which the patch has been found to be missing.

Missing Patch Stat Release Date Windows only: The date when the patch being summarized was released by Microsoft.

Missing Patch Stat Install Deadline Windows only: The date by which the patch being summarized should be installed, according to Microsoft's recommendation.

Missing Patch Stat Superseded by Package Windows only: Is a later patch available that supersedes the patch being summarized?

Missing Patch Stat Language Windows only: The language for which the patch being summarized is intended.

Missing Patch Stat Is OS Patch Is the patch being summarized an operating system patch? Patches that are not operating system patches are third-party patches.

Missing Patch Stat Severity Windows and third-party patches only: The rated severity of the patch being summarized. This information is supplied by the source of the patch and may not be present for all patches.

Compliance Reports

The **Compliance Reports** category contains information from the compliance reports that LANrev has gathered on administered computers. This information is collected by the **Gather Compliance Report** command.

These information items can be used in the **Compliance Reports** window.

There are four subcategories:

- **Reports** (page 893)
- **Computer Summary** (page 893)
- **Item Summary** (page 893)
- **Score Items** (page 894)

Reports

The **Reports** category contains information on the report parameters.

Profile Name

The name of the profile on which the report is based.

Compliance Check Start Date

The date and time when LANrev began gathering the report.

Compliance Check Finish Date

The date and time when LANrev completed gathering the report.

Benchmark File

The report definition file chosen as the basis for this report.

Report Description

The description of the report from the chosen report definition file.

Computer Summary

The **Computer Summary** category contains information on the overall results of the tested computer.

Compliant

Whether the computer was found to be compliant, according to the rules in the report.

Compliance Score

The compliance score the computer achieved in the report.

Compliance Report Date

The date when the report was last changed in LANrev Admin. This may be later than the date when the report was created.

Compliance Report Logged-In User

The name of the user account that was active on the administered computer when the report was compiled.

Item Summary

The **Item Summary** category contains summary information on the score items included in the report.

Max. Achieved Score

The maximum score that any of the tested computers achieved for this item.

Average Achieved Score

The average score achieved by all tested computers for this item.

Min. Achieved Score

The minimum score that any of the tested computers achieved for this item.

Max. Item Score

The maximum score that can be achieved for this item.

Compliance Count The number of computers that met the compliance criteria for this item.

Error Count The number of computers for which the compliance testing for this item returned an error.

Failure Count The number of computers that were found to not meet the compliance criteria of this item.

Scored Computer Count The number of computers that were scored using this report.

Scoring States A list of all individual scoring states that the tested computers achieved for this item.

Score Items

The **Score Items** category contains information on the individual score item results of each computer.

Score Item Title The name of the individual score item from the report.

Score The score the computer achieved in this score item.

Score State The pass or fail state of the report item for this computer.

Max. Score The maximum possible score to be achieved in this score item.

Score Item Index Path The path of the individual score item in the report.

Score Item Weight The weight of the individual score item within the report.

Score Item Description The description of the individual score item, as noted in the report file.

XCCDF Item Identifier The unique identifier of this score item.

Mobile Device Information

The **Mobile Device Information** category contains information about mobile devices managed by LANrev through an MDM server.

This information is collected automatically for managed mobile devices on which LANrev Apps is installed (first upon enrollment and then at each regular contact specified by the iOS contact interval setting of the MDM server). It can be manually updated through the **Update Device Information** command.

There are a number of subcategories:

- **Device Information** (page 895)
- **Device User Information** (page 907)
- **Installed Applications** (page 909)
- **Installed Configuration Profiles** (page 911)

- **Installed Provisioning Profiles** (page 911)
- **Installed Certificates** (page 912)
- **Installed Media Files** (page 913)
- **Installed Application Statistics** (page 913)
- **Installed Configuration Profile Statistics** (page 914)
- **Installed Provisioning Profile Statistics** (page 914)
- **Installed Certificate Statistics** (page 915)
- **Installed Media File Statistics** (page 915)
- **Device Tracking** (page 916)
- **Custom Fields** (page 917)
- **Mobile Application Packages** (page 918)
- **Application Packages** (page 919)
- **App Store Volume Purchase Program** (page 922)
- **Mobile Configuration Profile Definitions** (page 922)
- **iOS Provisioning Profile Definitions** (page 923)
- **Mobile Media** (page 924)
- **Mobile Actions** (page 925)
- **Mobile Device Policies** (page 926)
- **Mobile Device Enrollment Profiles** (page 926)
- **Device Commands** (page 928)
- **EAS Policies** (page 929)

Device Information

The **Device Information** category contains information on the managed mobile devices themselves.

Mobile Device Name

The name of the connected mobile device.

For iOS devices, this is the name that was given to the device in iTunes or the device settings. For Android devices, the name is assigned by LANrev and can be changed as described in “Naming mobile devices” on page 254.

Mobile Device Model

The type of the connected mobile device.

Mobile Device Model Identifier

iOS devices only: Apple’s internal identifier for the device.

Mobile Device Model Number

iOS and Android devices only: The model number the device vendor uses to identify the mobile device in its ordering system.

Mobile Device OS Version

The version number of the operating system installed on the mobile device.

Mobile Device OS Build Number

The build number of the operating system version installed on the mobile device.

Mobile Device OS Platform

The operating system family used on this device.

Mobile Device OS Updates Available

iOS 9 and up only: Whether an OS update for this device is available on Apple’s servers.

Mobile Device Serial Number

iOS and Android devices only: The serial number of the mobile device.

Mobile Device Phone Number

The telephone number currently assigned to the mobile device, if any.

Mobile Device Last Contact

The time when the last communication from the mobile device was received by the MDM server.

Mobile Device Ownership

The kind of owner the device has – the company, the user, or a guest. (This information can be changed with the **Set Device Ownership** context menu command.)

Mobile Device Is Supervised

Devices running iOS 7 and up only: Whether the device is configured to be in supervised mode.

Mobile Device Is Shared

Devices running iOS 9.3 and up only: Whether the device is configured to be shared among multiple users.

Mobile Device Maximum Resident Users

Devices running iOS 9.3 and up only: The maximum number of users whose data is kept on this shared device (space permitting).

Mobile Device Logged-in User Apple ID

Devices running iOS 9.3 and up only: The Apple ID of the user who is currently logged into this shared device.

Mobile Device Attention Mode Enabled

Whether the device has been put into attention mode (where a message is displayed on-screen and no interaction with the device is possible).

Mobile Device IMEI

The IMEI (GSM telephone identification number) of the connected mobile device, if any.

Mobile Device MEID

The MEID (CDMA telephone identification number) of the connected mobile device, if any.

Mobile Device Identifier (UDID)

The target identifier (a unique internal ID) of the connected mobile device.

Mobile Device Capacity

iOS and Android devices only: The storage capacity of the mobile device, excluding space required by the operating system. This capacity is usually a few gigabytes below the nominal capacity. (For example, a 32 GB iPhone may have a capacity of a little over 29 GB.) For iOS devices, this number is the same as the capacity displayed in iTunes.

Mobile Device Available Capacity

iOS and Android devices only: The free storage on the mobile device. For iOS devices, this number is the same as the free space displayed in iTunes.

Mobile Device Bluetooth MAC Address

iOS and Android devices only: The MAC address of the mobile device's Bluetooth connection.

Mobile Device WiFi MAC Address

iOS and Android devices only: The MAC address of the mobile device’s WiFi connection.

Mobile Device Ethernet MAC Address

Devices running iOS 7 and up only: The MAC address of the mobile device’s Ethernet connection.

Note that this information is available only on devices with an Ethernet port (such as an Apple TV) that are enrolled in the MDM.

Mobile Device GPS Capable

iOS and Android devices only: Whether the mobile device can locate itself by GPS signals.

Note that devices which are not GPS capable may still be able to locate themselves by other means, such as known locations of cell towers or WiFi networks in range. However, these location methods are usually less accurate than GPS location.

Mobile Device iTunes Store Account Configured

Devices running iOS 7 and up only: Whether an iTunes account is configured in the system settings on this device.

Mobile Device iTunes Store Account Is Part of VPP

Devices running iOS 8 and up only: Whether the device is currently using an App Store account that is registered for the device user in your VPP program.

Mobile Device App Store Disabled

Devices running iOS 8 and up only: Whether access to the app store is currently disabled on the device.

Mobile Device Is MDM Lost Mode Enabled

Devices running iOS 9.3 and up only: Whether the Lost mode is enabled on this device.

The Lost mode prevents the device from being used until it is unlocked again. It also causes the device location to be tracked.

Mobile Device Find My Device Enabled

Devices running iOS 7 and up only: Whether the “Find My iPhone” function is activated on this device.

Mobile Device Activation Lock Enabled

Devices running iOS 7 and up only: Whether the activation lock function is activated on this device.

Mobile Device Activation Lock Removed

Devices running iOS 7 and up only: Whether an engaged activation lock on the device has been removed.

Mobile Device Has Activation Lock Bypass Code

Devices running iOS 7 and up only: Whether there is a bypass code for the activation lock of this device.

Mobile Device Activation Lock Removal Date

Devices running iOS 7 and up only: The latest date on which an engaged activation lock was removed on the device.

Mobile Device Send App Analytics

Devices running iOS 9.3.2 and up only: Whether this device sends information about app crashes and usage to Apple.

Mobile Device Send Diagnostic & Usage Data

Devices running iOS 9.3.2 and up only: Whether this device sends daily diagnostic and usage information to Apple.

Mobile Device Do Not Disturb Enabled

Devices running iOS 7 and up only: Whether the "Do not disturb" setting is currently active on this device.

Mobile Device Personal Hotspot Enabled

Devices running iOS 7 and up only: Whether this device currently functions as a personal hotspot.

Mobile Device Is Cloud Backup Enabled

Devices running iOS 7.1 and up only: Whether this device is configured to be backed up to iCloud.

Mobile Device Last Cloud Backup

Devices running iOS 7.1 and up only: The date and time when this device was last backed up to iCloud.

Mobile Device Has Home Screen Layout Installed

Supervised devices running iOS 9.3 and up only: Whether the home screen layout is controlled by an installed configuration profile.

Mobile Device Production Date

iOS devices only: The date when the mobile device was manufactured.

NOTE The content of this information item, same as with the next four information items listed below, is downloaded from an Apple server, based on the device's serial number and cached on the LANrev server. The information is updated once every ten days, provided the managed device has an Internet connection.

Mobile Device Purchase Date

iOS devices only: The date when the iOS device was purchased, according to Apple's files.

NOTE See the note for Mobile Device Production Date, above.

Mobile Device Age

iOS devices only: The age of the mobile device, that is, the time that has elapsed since its production.

NOTE See the note for Mobile Device Production Date, above.

Mobile Device Warranty Info

iOS devices only: The iOS device's current warranty status.

NOTE See the note for Mobile Device Production Date, above.

Mobile Device Warranty End

iOS devices only: The date when the warranty for the iOS device will end. A value of “n/a” indicates either that no information is available or that the warranty has expired.

NOTE See the note for Mobile Device Production Date, above.

Mobile Device Organization Name

Devices running iOS 7 and up only: The organization name entered for the device via the **Set Organization Information** command.

Mobile Device Organization Address

Devices running iOS 7 and up only: The organization address entered for the device via the **Set Organization Information** command.

Mobile Device Organization E-Mail

Devices running iOS 7 and up only: The organization e-mail address entered for the device via the **Set Organization Information** command.

Mobile Device Organization Phone

Devices running iOS 7 and up only: The organization phone number entered for the device via the **Set Organization Information** command.

Mobile Device Organization Custom

Devices running iOS 7 and up only: The organization-related custom information entered for the device via the **Set Organization Information** command.

Mobile Device Public IP Address

iOS and Android devices only: The public IPv4 address over which the mobile device was communicating with LANrev at the time of its last contact.

This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet. If the device connects to the MDM server over a proxy server, the proxy server’s address is reported.

Mobile Device Public IP Address (v6)

iOS and Android devices only: The public IPv6 address over which the mobile device was communicating with LANrev at the time of its last contact.

This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet. If the device connects to the MDM server via a proxy, the proxy’s address is reported.

Mobile Device Cell IP Address

iOS and Android devices only: The IP address of the mobile device in the mobile (cellular) network it is currently using (if any).

Mobile Device WiFi IP Address

iOS and Android devices only: The IPv4 address of the mobile device in the WiFi network it was using at the time of its last contact (if any).

Mobile Device WiFi IP Address (v6)

iOS and Android devices only: The IPv4 address of the mobile device in the WiFi network it was using at the time of its last contact (if any).

Mobile Device WiFi Network

iOS and Android devices only: The name of the WiFi network (if any) to which the mobile device was connected at the time of its last contact.

Mobile Device Is Tablet

iOS and Android devices only: Whether the mobile device is a tablet or not.

Mobile Device Display Resolution

iOS and Android devices only: The screen size of the mobile device, measured in pixels.

Mobile Device Status

The management status of the device:

- Unmanaged: This device is not part of the MDM.
- Managed and offline: The device is part of the MDM system but has not responded to the last contact request.
- Managed and online: The device is part of the MDM system and has responded to the last contact request.

Mobile Device Battery Level

iOS and Android devices only: The remaining charge level of the mobile device’s battery, expressed as a percentage.

Mobile Device Managed

Whether the device is managed: The information item contains “true” if the device is managed and online or managed and offline; it contains “false” if the device is unmanaged (see above).

Mobile Device Jailbroken

iOS and Android devices only: Whether the device has been jailbroken, that is, whether it contains modified firmware.

Mobile Device Supports Persistence

Android devices only: Whether the device supports persistence, that is, lets the LANrev client software remain on the device even after removal attempts and factory resets.

Mobile Device Modem Firmware Version

iOS and Android devices only: The version number of the modem firmware in the mobile device, if any.

Mobile Device Hardware Encryption

iOS and Android devices only: The kind of hardware encryption (block level or file level) available on the device.

Mobile Device Passcode Compliant

iOS and Android devices only: The passcode on the device complies with all applicable requirements, including those of Exchange when applicable.

Mobile Device Passcode Compliant with Profiles

iOS and Android devices only: The passcode on the device complies with all active profiles.

Mobile Device Passcode Present

iOS and Android devices only: A passcode (PIN to wake up the device) is set on the mobile device.

Mobile Device Passcode Lock Grace Period

iOS devices only: The user preference setting for the amount of time after the device locks (the screen is turned off after a period of inactivity) before unlocking the device requires entering the device passcode.

Mobile Device Passcode Lock Grace Period Enforced

iOS devices only: The actually enforced amount of time after the device locks (the screen is turned off after a period of inactivity) before unlocking the device requires entering the device passcode.

Mobile Device Is Roaming

iOS and Android devices only: Whether the mobile device is currently roaming (connected to a mobile network other than that of the standard provider).

Mobile Device Data Roaming Enabled

iOS and Android devices only: Whether the mobile device is set to allow data roaming (exchanging data over mobile networks other than that of the standard provider).

Mobile Device Voice Roaming Enabled

iOS devices only: Whether the mobile device is set to allow voice roaming (initiating or receiving voice calls over mobile networks other than that of the standard provider).

Mobile Device Home Network

iOS and Android devices only: The standard mobile network of the mobile device.

Mobile Device Cellular Technology

iOS and Android devices only: The basic cellular technology that the mobile device is currently using to communicate, such as GSM or CDMA.

Mobile Device Current Carrier Network

The mobile network into which the mobile device was booked at the time of the last contact.

Mobile Device Carrier Settings Version

iOS and Android devices only: The version number of the carrier settings in the iOS device. Carrier settings include the name of the various available networks and other information. They are provided by Apple and can be updated independently of the iOS software.

Mobile Device Home Mobile Country Code

iOS and Android devices only: The mobile country code of the standard mobile network of the mobile device.

Mobile Device Home Mobile Network Code

iOS and Android devices only: The mobile network code of the standard mobile network of the mobile device.

Mobile Device Current Mobile Country Code

iOS and Android devices only: The mobile country code of the mobile network into which the iOS device was booked at the time of the last contact.

Mobile Device Current Mobile Network Code

iOS and Android devices only: The mobile network code of the mobile network into which the iOS device was booked at the time of the last contact.

Mobile Device SIM ICC Identifier

iOS and Android devices only: The mobile country code of the SIM installed in the mobile device.

Mobile Device EAS Identifier

Devices running iOS 7 and up only: The Exchange Active Sync ID of the device.

Mobile Device Board

iOS and Android devices only: The name or type code of the motherboard of the mobile device.

Many motherboards used in mobile devices do not have an accessible name or type code.

Mobile Device Brand

iOS and Android devices only: The brand name of the mobile device as noted in its firmware.

This brand is not necessarily the manufacturer; see “Mobile Device Manufacturer”, below. (For example, the brand may also be the carrier who sold the phone.)

Mobile Device CPU Name

iOS and Android devices only: The type of the CPU used in the mobile device.

Mobile Device CPU Speed

iOS and Android devices only: The clock rate of the CPU used in the mobile device.

Mobile Device Info

Android devices only: Additional information about the mobile device as provided by its manufacturer.

Mobile Device IMEISV

Android devices only: The revision number of the software installed on the mobile device, as noted in the device’s IMEI.

Mobile Device Internal Storage Available

Android devices only: The amount of internal storage for application data in the mobile device that is currently free.

Note that some devices partition the built-in storage and declare some to be USB storage. In this case, the internal storage shown by this information item is much smaller than the actual built-in storage. (See “Mobile Device SD Card 1 Available”, below.)

Mobile Device Internal Storage Total

Android devices only: The total amount of internal storage for application data available in the mobile device.

Note that some devices partition the built-in storage and declare some to be USB storage. In this case, the internal storage shown by this information item is much smaller than the actual built-in storage. (See “Mobile Device SD Card 1 Total”, below.)

Mobile Device Kernel Version

Android devices only: The version information for the operating system kernel active in the mobile device.

Mobile Device Manufacturer

The company which produced the mobile device.

This is not necessarily the same company under the brand name of which the device was sold; see “Mobile Device Brand”, above.

Mobile Device Network Type

Android devices only: The base technology of the cellular network to which the mobile device is connected. Possible values are “none”, “EDGE”, “GPRS”, or “UMTS”.

Mobile Device Product Name

Android devices only: The product name of the mobile device, as noted in the device’s firmware.

This name is usually not the same as the product name printed on the case.

Mobile Device SD Card 1 Available

Android devices only: The amount of storage that is currently free on the first SD card in the mobile device.

Note that some devices partition the built-in storage and declare some to be USB storage. In this case, some of the internal storage is shown as SD card 1.

Mobile Device SD Card 1 Total

Android devices only: The amount of storage available on the first SD card in the mobile device.

Note that some devices partition the built-in storage and declare some of it to be USB storage. In this case, some of the internal storage is shown as SD card 1.

Mobile Device SD Card 2 Available

Android devices only: The amount of storage that is currently free on the second SD card in the mobile device.

Mobile Device SD Card 2 Total

Android devices only: The amount of storage available on the second SD card in the mobile device.

Mobile Device System Cache Total

Android devices only: The total amount of cache memory on the mobile device.

Mobile Device System Memory Available

Android devices only: The amount of RAM in the mobile device that is currently free.

Mobile Device System Memory Total

Android devices only: The amount of RAM installed in the mobile device.

Mobile Device System Storage Available

Android devices only: The amount of storage memory, excluding SD cards, that is currently free on the mobile device.

Mobile Device System Storage Total

Android devices only: The total amount of storage memory, excluding SD cards, on the mobile device.

Mobile Device LANrev Apps Version

iOS and Android devices only: The version number of the copy of LANrev Apps that is installed on the managed mobile device.

Mobile Device LANrev Apps Build Number

iOS and Android devices only: The build number of the copy of LANrev Apps that is installed on the managed mobile device.

Mobile Device LANrev Apps Vendor Support

iOS and Android devices only: The vendor-specific MDM framework supported by the installed version of LANrev Apps. For the iOS version, this is “iOS”; for the standard Android version, it is “generic”. For other Android, the specific vendor framework is noted, such as “Samsung SAFE”.

Mobile Device LANrev Apps Supports Tracking

iOS and Android devices only: Whether the copy of LANrev Apps installed on the device supports geotracking.

Mobile Device Vendor MDM Version

iOS and Android devices only: The latest version of the vendor-specific MDM framework supported by the installed version of LANrev Apps. (See “Mobile Device LANrev Apps Vendor Support”, above.)

Mobile Device Record Creation Date

The time when the record for this mobile device was created in the server.

Mobile Device Supports KNOX

Whether Samsung KNOX can be installed on this mobile device.

Mobile Device KNOX Status

The current status of Samsung KNOX on the mobile device: active, inactive, in creation, locked, or no workspace.

Mobile Device KNOX Version

The version of Samsung KNOX (if any) that is installed on the mobile device.

Mobile Device MDM Profile Up-to-date

iOS devices only: Whether the MDM access privileges that are set in the MDM profile on the managed device are the same as those currently set on the server.

For information on updating MDM profiles, see “Updating MDM access rights on enrolled iOS devices” on page 89.

Mobile Device OS Language

The language to which the operating system on this mobile device is set.

Mobile Device GUID

The GUID (UUID) of the mobile device.

Mobile Device Identity

The identifier of the mobile device on the Exchange server.

Mobile Device Color

iOS devices only: The case color of the mobile device.

Mobile Device Enable Outbound SMS

Whether the device is set to allow the user to send SMS messages.

Mobile Device Last Policy Update Time

The date and time when the EAS policy of the device was last modified.

Mobile Device Remote Erase Supported

Does this device allow its contents to be remotely erased by an administrator?

Mobile Device Erase Ack Time

The time at which the Exchange server received the acknowledgement for the most recent erase of the mobile device.

Mobile Device Erase Request Time

The time at which the remote erase setting was enabled on the mobile device.

Mobile Device Erase Sent Time

The time at which the Exchange server sent the most recent erase command to the mobile device.

Mobile Device Last Device Erase Requestor

The Exchange user who initiated the most recent remote erase of the mobile device. If the device has since again been paired to the Exchange server, this information may be lost.

Mobile Device Number of Folders Synched

The number of folders on this device that are synchronized to the Exchange server.

Mobile Device Access State

The access status that the device currently has with respect to the Exchange server. The normal status is “Allowed”, which grants normal access. “Quarantined” or “blocked” indicates, respectively, limited or prohibited access. For details, see the Exchange documentation.

Mobile Device Access State Reason

A brief indication of the reason for the current access status. For details, see the Exchange documentation.

Mobile Device Remote Erase Status

The status of the device regarding remote erasing, if any. The normal status for a mobile device with no erases pending or underway is “DeviceOk”.

Mobile Device Remote Erase Status Note

Additional information regarding the Mobile Device Remote Erase Status (see above). Additional information is not always available.

Mobile Device Information Last Change

The most recent time at which the information stored on the server for the mobile device changed.

Note that this is not necessarily the time on which the corresponding property of the device changed, just the time when the mobile client software informed the MDM server of the change.

Certain changes that frequently occur are not considered for this information, such as changes of the battery level, free storage, or roaming status.

Mobile Device Installed Software Last Change

The most recent time at which the information stored on the server for the software installed on the mobile device changed.

Note that this is not necessarily the time on which an app was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Mobile Device Installed Configuration Profiles Last Change

The most recent time at which the information stored on the server for the configuration profiles installed on the mobile device changed.

Note that this is not necessarily the time on which a profile was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Mobile Device Installed Certificates Last Change

The most recent time at which the information stored on the server for the certificates installed on the mobile device changed.

Note that this is not necessarily the time on which a certificate was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Mobile Device Installed Provisioning Profiles Last Change

The most recent time at which the information stored on the server for the provisioning profiles installed on the mobile device changed.

Note that this is not necessarily the time on which a profile was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Mobile Device Available OS Updates Last Change

iOS 9 and up only: The most recent time at which the list on the server changed of which OS updates are available for the mobile device.

Mobile Device Installed Media File Last Change

The most recent time at which the information stored on the server for the media files installed on the mobile device changed.

Note that this is not necessarily the time on which a media file was installed on or deleted from the device, just the time when the mobile client software informed the MDM server of the change.

Mobile Device Installed Application Count

The total number of apps installed on the managed device.

This total includes all apps on the device installed by any means – app store and enterprise apps installed through LANrev as well as any apps installed by the device user independently of LANrev, for example, through her own app store account.

Mobile Device Enrolled via Enrollment Program

Devices running iOS 7 and up only: Whether the device was enrolled in MDM through Apple's device enrollment program.

Mobile Device Enrollment Status

Devices running iOS 7 and up only: Whether and in what way the device is part of Apple's device enrollment program. This information item can have these values:

- **not in enrollment program**: The device has not been entered into any enrollment program.
- **not assigned**: The device is part of an enrollment program, but no enrollment profile is durrently assigned to it.
- **assigned**: An enrollment profile has been assigned to the device but the device has not yet been enrolled in the MDM.
- **installed**: The enrollment profile has been installed on the device; that is, the device has been enrolled in MDM and the profile options have taken effect.

Mobile Device Enrollment Program Registration Date

Devices running iOS 7 and up only: The date when the device was registered in the enrollment program.

Mobile Device Enrollment Profile Assignment Date

Devices running iOS 7 and up only: The date when the current enrollment profile was assigned to the device.

Mobile Device Enrollment Profile Installation Date

Devices running iOS 7 and up only: The date when the current enrollment profile was installed on the device.

Mobile Device Enrollment Profile UUID

Devices running iOS 7 and up only: The unique identifier of the enrollment profile currently assigned to the device.

Device User Information

The **Device User Information** category contains Active Directory or Open Directory information on the on the current user of a managed device.

You can use these information items as substitution variables in configuration profiles, as described in “Using variables in configuration profiles” on page 185.

Device User Display Name The user’s display name as stored in Active Directory or Open Directory.

Device User First Name The user’s first name as stored in Active Directory or Open Directory.

Device User Last Name The user’s last name as stored in Active Directory or Open Directory.

Device User Log-on Name The account name with which the user can log into Active Directory or Open Directory.

Device User E-Mail The user’s e-mail address as stored in Active Directory or Open Directory.

Device User Phone Number The user’s phone number as stored in Active Director or Open Directory.

Device User Mobile Phone Number The user’s mobile phone number as stored in Active Director or Open Directory. Note that this number is not necessarily the number of the managed device.

Device User Department The user’s department as stored in Active Directory or Open Directory.

Device User Department Number The number of the user’s department as stored in Active Directory or Open Directory.

Device User Company The name of the user’s company as stored in Active Directory or Open Directory.

Device User Street The user’s street address as stored in Active Directory or Open Directory.

Device User City The user’s city as stored in Active Directory or Open Directory.

Device User State The user’s state as stored in Active Directory or Open Directory.

Device User ZIP Code The user’s postal code as stored in Active Directory or Open Directory.

Device User Country The user’s country as stored in Active Directory or Open Directory.

Device User Office The user’s office as stored in Active Directory or Open Directory.

Device User Job Title The user’s job title as stored in Active Directory.

Device User Managed By
The user’s immediate manager as stored in Active Directory.

Device User Employee ID
The user’s employee ID as stored in Active Directory.

Device User Employee Number
The user’s employee number as stored in Active Directory or Open Directory.

Device User Account Disabled
Is this account currently disabled in Active Directory?

Device User Account Locked
Is this account currently locked in Active Directory?

Device User Account Lockout Time
The time when the user’s Active Directory account was locked.

Device User Account Password Expiration Date
The date when the account’s Active Directory password is scheduled to expire. This information is available only if the Active Directory domain controller is running on Windows Server 2008 or above.

Device User Account Password Expired
Has this account’s Active Directory password expired?

Device User Business Category
The business category in which the user works, as stored in Active Directory.

Device User Organizational Unit Path
The name of the Active Directory or Open Directory organizational unit to which the mobile device’s current user belongs

Device User Organizational Unit
The path of the Active Directory or Open Directory organizational unit to which the mobile device’s current user belongs

Device User Is Member Of
The Active Directory or Open Directory groups to which the mobile device’s current user belongs. Multiple groups are separated by commas.

Device User Enrollment Username
The username that the user entered when enrolling this device into the MDM server.

Device User Enrollment Domain
The domain that the user entered when enrolling this device into the MDM server.

Device User Active VPP Accounts
A list of VPP accounts of the organization which are available to the user, together with the status of the user in respect to each account. The status can be “invited” (an invitation message has been sent) or “associated” (the user has entered the Apple ID).

This is the same as Device User VPP Accounts, below, except that accounts from which the user has been retired are excluded.

Device User VPP Accounts

A list of VPP accounts of the organization with which the user is associated, together with the status of the user in respect to each account. The status can be "invited" (an invitation message has been sent), "associated" (the user has entered the Apple ID), and "retired" (the membership in the account has been revoked).

This is the same as Device User Active VPP Accounts, above, except that accounts from which the user has been retired are also listed.

Device User VPP Invite URL

The URL on Apple's servers which this user must access to complete the registration with a VPP account.

Device User Extension Attribute 1

The content of the extension attribute 1 field for this user in Active Directory.

Additional information items exist for the extension attribute 2 through 15 fields (Device User Extension Attribute 2, etc.).

Managed Device User Information

The **Managed Device User Information** category contains information about local users on shared mobile devices.

The information items in this category apply only to shared iOS devices.

Mobile Device User Apple ID

The Apple ID with which the user logs is identified on the device.

Mobile Device User Data Quota

The amount of data that the user is allowed to store on the device.

Mobile Device User Data Used

The amount of data that the user is currently storing on the device.

Mobile Device User Has Data to Sync

Whether the data of the mobile user currently requires synchronizing.

When data requires synchronizing, it is present on the device, but not yet in iCloud.

Mobile Device User Is Logged In

Whether the mobile user currently logged into the mobile device.

Installed Applications

The **Installed Applications** category contains information on the applications that are installed on a mobile device.

The information items in this category apply only to iOS and Android devices.

NOTE Applications that are included with the device firmware, such as Camera or Mail on iOS devices, are not listed.

Mobile Device Installed App Name

The name of the application.

Mobile Device Installed App Version

The short version number of the application.

Mobile Device Installed App Build Number

The build number of the application.

NOTE Not all applications have build numbers.

Mobile Device Installed App Version String

The version string of the application.

Mobile Device Installed App Bundle Identifier

The string that uniquely identifies the application’s bundle.

Mobile Device Installed App Size

The amount of storage that the application takes up on the mobile device.

Mobile Device Installed App Data Size

iOS devices only: The amount of storage that the data of the application takes up on the mobile device.

Mobile Device Installed App Data Directory

Android devices only: The directory on the mobile device in which the app stores its data.

Mobile Device Installed App Is KNOX

Android devices only: Whether this mobile application is installed in a KNOX workspace on the device.

Mobile Device Installed App Is Validated

iOS devices running iOS 9.2 and up only: Whether iOS considers this app validated.

This applies only to apps that have been installed with an enterprise certificate. For such apps, iOS verifies every few weeks that the certificate is still valid. If this cannot be verified, the app is considered not validated and can no longer run on the device.

Mobile Device Managed App Status

iOS devices only: The status of this app on the specific managed device (for example, “Managed” or “Needs redemption code”.

This information is not supported for apps on devices running iOS 4.x.

Mobile Device Managed App Prevent Data Backup

iOS devices only: Whether backing up of the apps data (through standard system backups) is prevented on this device.

Mobile Device Managed App Bound to MDM

iOS devices only: Whether the app will be automatically removed from this device once the device is no longer enrolled in an MDM management server.

Mobile Device Managed App Has Configuration Profile

Devices running iOS 7 and up only: Whether a configuration profile has been assigned to this app in LANrev.

Installed Configuration Profiles

The **Installed Configuration Profiles** category contains information about configuration profiles that are installed on administered mobile devices.

These information items can be used in the **Mobile Devices** window.

Mobile Device Installed Profile Name

The name of the configuration profile.

Mobile Device Installed Profile Description

The optional description string of the profile.

Mobile Device Installed Profile Organization

The optional name of the organization which has provided the profile.

Mobile Device Installed Profile Identifier

The identifying string of the profile.

Mobile Device Installed Profile UUID

The unique identifier of the profile.

Mobile Device Installed Profile Version

The version of the profile installed on the mobile device.

Mobile Device Installed Profile Encrypted

Whether the profile is encrypted.

Mobile Device Installed Profile Managed

Whether the profile is managed by the MDM system.

Mobile Device Installed Profile Allow Removal

Whether the profile can be removed remotely.

Mobile Device Installed Profile Type

The type of profile – for example, device profile, user profile, or app profile. Device profiles contain settings for the hardware or operating system, user profiles contain similar settings but are valid only for a specific user of a shared device, and app profiles contain settings for individual apps.

Mobile Device Installed Profile for User

The user of the shared mobile device for whom this profile has been installed. For device profiles, this information items contains “n/a”.

Installed Provisioning Profiles

The **Installed Provisioning Profiles** category contains information about the provisioning profiles that are installed on administered iOS devices.

These information items can be used in the **Mobile Devices** window. They apply only to iOS devices.

iOS Installed Provisioning Profile Name

The name of the provisioning profile.

iOS Installed Provisioning Profile Expiry Date

The date until which the provisioning profile is valid.

iOS Installed Provisioning Profile UUID

The unique identifier of the provisioning profile.

Installed Certificates

The **Installed Certificates** category contains information on the certificates which are installed on the administered mobile devices.

These information items can be used in the **Mobile Devices** window. They apply only to iOS devices.

Mobile Device Installed Certificate Name

The name of the certificate.

Mobile Device Installed Certificate Company

The company to which the certificate was issued.

Mobile Device Installed Certificate Country

The country where the owner of the certificate is located.

Mobile Device Installed Certificate Serial Number

The serial number of the certificate‘s issuer.

Mobile Device Installed Certificate Key Usage

The purposes for which the certificate may be used, as noted in the certificate.

Mobile Device Installed Certificate Is Identity

Whether the certificate is the identity certificate of the device.

Mobile Device Installed Certificate Is Root

Whether this certificate is a root certificate.

Mobile Device Installed Certificate Valid Until

The date until which the certificate is valid.

Mobile Device Installed Certificate Valid From

The date from which the certificate is valid.

Installed Media Files

The **Installed Media Files** category contains information on the media files which have been installed on the administered mobile devices using the **Install Media File** command.

These information items can be used in the **Mobile Devices** window.

Installed Media File Title

The name of the installed media file.

Installed Media File Type

The file type of the installed media file.

Installed Media File Version

The version of the installed media file, as specified in the file's record in LANrev.

Installed Media File State

The installation status of the file, such as "Queued for installation" or "Installed by user.

Installed Media File Author

The author of the installed media file, as specified in the file's record in LANrev.

Installed Media File Container

Whether the media file was installed in LANrev Safe or in iBooks on the device.

Installed Media File Download Date

The date when the file was downloaded to the mobile device.

Installed Media File Removal Date

The date when the user removed the file from LANrev Safe.

This information is displayed only for files that the user has removed but that have not yet been deleted from the mobile device. For files that have been removed by other means or that have not been removed at all, this is "n/a".

Installed Media File Bookstore ID

Media downloaded from Apple's bookstore only: The ID of the book in the bookstore.

Installed Application Statistics

The **Installed Application Statistics** category contains summary information on the installed applications found across all managed mobile devices.

NOTE As with the information items in the Installed Applications category, applications that are included in the device firmware are not listed. Also, applications on ignored devices (see "Ignore Devices" on page 631) are not included in the statistics.

These information items can be used in the Installed Software Statistics smart group in the **Mobile Devices** window. They apply only to iOS and Android devices.

Mobile Device Inst. App Name

The name of the application being summarized.

Mobile Device Inst. App Count

The number of copies of the application being summarized that were found across all mobile devices.

Mobile Device Inst. App Bundle Identifier

The string that uniquely identifies the bundle of the application being summarized.

Installed Configuration Profile Statistics

The **Installed Configuration Profile Statistics** category contains summary information on the configuration profiles installed on the managed mobile devices.

These information items can be used in groups in the **Mobile Devices** window that provide configuration profile statistics

Mobile Device Inst. Profile Name

The name of the configuration profile being summarized.

Mobile Device Inst. Profile Count

The number of copies of the configuration profile being summarized that were found across all managed mobile devices.

Mobile Device Inst. Profile Managed Count

The number of found copies of the configuration profile that are managed.

Mobile Device Inst. Profile Description

The description of the configuration profile being summarized.

Mobile Device Inst. Profile Identifier

The (locally) unique identifier of the configuration profile being summarized.

Mobile Device Inst. Profile Organization

The organization which has issued the configuration profile being summarized.

Mobile Device Inst. Profile UUID

The globally unique identifier of the configuration profile being summarized.

Installed Provisioning Profile Statistics

The **Installed Provisioning Profile Statistics** category contains summary information on the provisioning profiles installed on the managed iOS devices.

These information items can be used in groups in the **Mobile Devices** window that provide provisioning profile statistics. They apply only to iOS devices.

iOS Inst. Prov. Profile Name

The name of the provisioning profile being summarized.

iOS Inst. Prov. Profile Count

The number of copies of the provisioning profile being summarized that were found across all managed mobile devices.

iOS Inst. Prov. Profile Max Expiry Date

The latest expiry date found in any of the copies of the provisioning profile being summarized.

iOS Inst. Prov. Profile Min Expiry Date

The earliest expiry date found in any of the copies of the provisioning profile being summarized.

iOS Inst. Prov. Profile UUID

The globally unique identifier of the configuration profile being summarized.

Installed Certificate Statistics

The **Installed Certificate Statistics** category contains summary information on the certificates installed on the managed iOS devices.

These information items can be used in groups in the **Mobile Devices** window that provide certificate statistics. They apply only to iOS devices.

Mobile Device Inst. Certificate Name

The name of the certificate being summarized.

Mobile Device Inst. Certificate Count

The number of copies of the certificate being summarized that were found across all managed mobile devices.

Mobile Device Inst. Certificate Identity Count

The number of copies of the certificate being summarized that are used as identity certificates on managed mobile devices.

Installed Media File Statistics

The **Installed Media File Statistics** category contains information on how often managed media files are installed on managed mobile devices.

These information items can be used in the **Mobile Devices** window.

Inst. Media File Title

The name of the installed media file being counted.

Inst. Media File Count

The number of devices on which the media file being counted is installed.

Inst. Media File Type

The file type of the installed media file being counted.

Inst. Media File Author

The author of the installed media file being counted, as specified in the file's record in LANrev.

Available OS Updates

The **Available OS Updates** category contains information on iOS updates that are available for managed devices. All information items in this category apply only to supervised devices running iOS 9 and up.

The content of these information items is provided by Apple and cannot be configured through LANrev.

These information items can be used in the **Mobile Devices** window.

OS Update Name

iOS 9 and up only: The name of the OS version installed by the update.

OS Update Version
iOS 9 and up only: The version number of the OS version installed by the update.

OS Update Build Number
iOS 9 and up only: The build number of the OS version installed by the update.

OS Update Download Size
iOS 9 and up only: The amount of data downloaded for the update.

OS Update Install Size
iOS 9 and up only: The amount of data that will be installed on the device by this update.

OS Update Required Installation Size
iOS 9 and up only: The amount of free space on the device that the update requires.

OS Update Is Critical
iOS 9 and up only: Whether Apple has flagged this update as critical.

OS Update Is Preview
iOS 9 and up only: Whether this update is beta software or a similar precursor version to a final release.

OS Update Allow to Install Later
iOS 9 and up only: Whether the device user may choose to postpone the update.

OS Update Restart Required
iOS 9 and up only: Whether this update requires the device to be restarted.

Device Tracking

The **Device Tracking** category contains geotracking information on tracked mobile devices.

These information items can be used in groups in the **Mobile Devices** window that list mobile devices. They apply only to iOS and Android devices.

Mobile Device Tracking Enabled
Whether the geolocation of this device is being tracked.

Mobile Device Tracking Interval
The interval in which the geolocation of this device is recorded.

Mobile Device Tracking Accuracy
The tracking accuracy set for this device. Note that the actual accuracy of a particular location record (see the Mobile Device Location Accuracy information item, below) may be lower than this setting when the desired accuracy is not technically possible at the time of recording the location.

Mobile Device Tracking Time
The time when the location of the device was determined.

Mobile Device Location Latitude
The latitude at which the device was located.

Mobile Device Location Longitude
The latitude at which the device was located.

Mobile Device Location Accuracy

The maximum possible distance from the true position with which the device was located.

Mobile Device Location Cell IP Address

The IP address of the mobile device in the mobile (cellular) network it is currently using (if any).

This information is reported only when it changes; otherwise, the information item contains “n/a”.

Mobile Device Location Public IP Address

The public IP address over which the mobile device is communicating with LANrev.

This is either the cell IP address or the public address of the NAT router over which the WiFi network is connected to the Internet.

This information is reported only when it changes; otherwise, the information item contains “n/a”.

Mobile Device Location WiFi IP Address

The IPv4 address of the mobile device in the WiFi network it is currently using (if any).

This information is reported only when it changes; otherwise, the information item contains “n/a”.

Mobile Device Location WiFi IP Address (v6)

The IPv6 address of the mobile device in the WiFi network it is currently using (if any).

This information is reported only when it changes; otherwise, the information item contains “n/a”.

Mobile Device Location Battery Level

The remaining charge level of the mobile device’s battery at the time the location was recorded, expressed as a percentage.

Mobile Device Location Battery State

The state of the mobile device’s battery when the location was recorded:

- On Battery (Discharging): The device is running on battery power.
- On Power (Charging): The device is running on mains power.
- Full: The battery is full

Custom Fields

The **Custom Fields** category contains all custom information fields for mobile devices that have been defined on the currently connected server.

The exact contents of this category and the functions of the individual fields depend entirely on the specific local configuration of the site and cannot be described further here.

NOTE Double-clicking a custom information item in the **Information Items** window lets you edit its specifications.

Mobile Application Packages

The **Mobile Application Packages** category contains information on the mobile application packages which have been created in LANrev.

These information items can be used in the **Mobile Devices** window, in the **Enterprise Applications** group as well as the **Enterprise Applications** groups of policies. They apply only to iOS and Android devices.

Mobile App Name

The name of the application package.

Mobile App Category

The category of the application package, as specified by the administrator.

Mobile App Version

The version number of the application contained in the package.

Mobile App Build Number

The build number of the application contained in the package.

Mobile App OS Platform

The operating system for which the application contained in the package was written.

Mobile App Size

The size the app code requires on the mobile device after installation.

Mobile App Is Universal

iOS devices only: Whether this app runs on all three iOS hardware platforms – iPhone, iPad, and iPod touch.

Mobile App Supported Devices

iOS devices only: A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) on which this app runs.

Mobile App Min OS Version

The minimum version of the mobile operating system that this app requires to run.

Mobile App Bundle Identifier

The unique identifier of the application package.

Mobile App Short Description

The short description of the application package.

Mobile App Long Description

The long description of the application package.

Mobile App Update Description

The update description of the application package.

Mobile App Prevent Data Backup

iOS devices only: The application data of this app is not included in standard device backups via iTunes.

This is always false for Android apps.

Mobile App Remove When MDM Is Removed

iOS devices only: Whether this application will be automatically removed from the device when the device is no longer managed through an MDM system (that is, when the MDM profile is deleted from the device).

This is always false for Android apps.

Mobile App Convert to Managed App

iOS devices only: Whether this application will converted from an unmanaged app to a managed app if a copy is already installed on the device.

This is always false for Android apps.

Mobile App Assignment Rule

Whether the app is installed automatically or on-demand and removed automatically or manually.

Mobile App Assignment Force Into Management

Only devices running iOS 9.0 and up: Whether, if an unmanaged version of this app is already present on a target device, it will be converted to a managed version.

Mobile App Assignment Prevent App Data Backup

iOS devices only: Whether the local data of this app will be excluded from iTunes or iCloud backups of the device.

Mobile App Assignment Remove App When MDM Is Removed

iOS devices only: Whether the app will automatically be deleted from the device when the device is removed from MDM management.

Mobile App Assignment App Configuration

iOS devices only: The configuration assigned to the app, if any.

Mobile App Assignment Per-App VPN Configuration

iOS devices only: The app-specific VPN configuration assigned to the app, if any.

Mobile App Assigned to KNOX Workspace

Android devices only: Whether this mobile app is assigned to be installed in a KNOX workspace. If this information items contains “No”, the app is assigned to be installed on Android devices outside of the KNOX workspace.

Mobile App Is KNOX

Android devices only: Whether this mobile app is a KNOX application. That is, whether this is a version of the app that can run only in a Samsung KNOX workspace.

Application Packages

The **Application Packages** category contains information on the mobile applications that an administrator has specified as recommended apps in LANrev.

These information items can be used in the **Mobile Devices** window, in the **App Store Applications** group and the **Enterprise Applications** groups of policies. They apply only to iOS and Android devices.

App Name

The name of the application package.

App Category

The category of the application package, as specified by the administrator.

App Min OS Version

The minimum version of the operating system required to use the app.

App OS Platform

The mobile operating system on which this app runs.

App Version

The version number of the application.

App Short Description

The short description of the app.

App Long Description

The long description of the app.

App URL

The URL of the app's page in the app store.

App Supported Devices

iOS devices only: A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) on which this app runs.

App Is Universal

iOS devices only: Whether this app runs on all three iOS hardware platforms – iPhone, iPad, and iPod touch.

App Prevent Data Backup

iOS devices only: Whether the data of this app on the device is prevented from being included in system backups.

This is always false for Android apps.

App Remove When MDM Is Removed

iOS devices only: Whether this app will be automatically deleted from devices that are no longer enrolled on an MDM server.

This is always false for Android apps.

App Convert to Managed App

iOS devices only: Whether this application will converted from an unmanaged app to a managed app if a copy is already installed on the device.

This is always false for Android apps.

App Allow Automatic Updates

iOS devices only: Whether LANrev can update this application automatically when it is installed as a managed application.

This information item corresponds to the **Allow automatic updates when installed as managed application** setting described in "Application Info tab" on page 555.

This is always false for Android apps.

App App Store ID

iOS devices only: The ID of this app in the App Store.

App Bundle Identifier

iOS devices only: The unique identifier of the application package.

App Store VPP Licenses Purchased

iOS apps only: The total number of App Store volume purchase program managed licenses that have been purchased for this app.

App Store VPP Licenses Assigned

iOS apps only: The total number of App Store volume purchase program managed licenses for this app that have been assigned to users.

App Store VPP Licenses Remaining

iOS apps only: The total number of App Store volume purchase program managed licenses for this app that remain available for assignment.

App Store VPP Accounts

The names of all your accounts for the Apple volume purchase program that contain licenses for the app in this package.

App Store VPP Codes Purchased

iOS apps only: The total number of App Store volume purchase program codes that have been imported for this app.

App Store VPP Codes Redeemed

iOS apps only: The number of App Store volume purchase program codes that have already been used to install a copy of this app on an administered mobile device.

App Store VPP Codes Remaining

iOS apps only: The remaining number of App Store volume purchase program codes that are available for installing this app on an administered mobile device.

App Store VPP Order Number

iOS apps only: The order number under which the App Store volume purchase program codes were bought.

App Store VPP Purchaser

iOS apps only: The App Store user through whose account the App Store volume purchase program codes were bought.

App Assignment Rule

Whether the app is installed automatically or on-demand and removed automatically or manually.

App Assignment Use Device License

iOS only: Whether the license for this app will be assigned to a device. Licenses that are not assigned to devices are assigned to device users. If the device does not run iOS 9 or up, the license will be assigned to the user, regardless of this setting.

App Assignment Force Into Management

Only devices running iOS 9.0 and up: Whether, if an unmanaged version of this app is already present on a target device, it will be converted to a managed version.

App Assignment Prevent App Data Backup

iOS devices only: Whether the local data of this app will be excluded from iTunes or iCloud backups of the device.

App Assignment Remove App When MDM Is Removed

iOS devices only: Whether the app will automatically be deleted from the device when the device is removed from MDM management.

App Assignment VPP Account for Device Assignments

iOS devices only: The VPP account used when this app is assigned to a device.

App Assignment App Configuration

iOS devices only: The configuration assigned to the app, if any.

App Assignment Per-App VPN Configuration

iOS devices only: The app-specific VPN configuration assigned to the app, if any.

App Assignment Perform Automatic Updates

iOS devices only: Whether auto-updating has been enabled for this application when it was assigned to a policy.

This setting applies only to apps that are part of the “Auto-install” or “Auto-install, Auto-remove” groups of policies.

This is always false for Android apps.

App License Is Irrevocable

Whether the license for this app can be revoked from one user and assigned to another user. This applies only to licenses managed through a volume purchase program.

App Store Volume Purchase Program

The **App Store Volume Purchase Program** category contains information about individual purchase codes and licenses from the App Store volume purchase program.

These information items can be used in the **Mobile Devices** window, in the **App Store Applications** group, and the **Enterprise Applications** groups of policies.

ASVPP Redemption Code

The actual purchase code that must be entered.

ASVPP Code Redeemed

Whether the code has already been redeemed.

ASVPP Redemption Date

The date when the code has been redeemed. If the code has not yet been redeemed, this information item contains “n/a”.

ASVPP License Status

Whether this license is currently assigned to an enrolled user or revoked. If the license has not yet been assigned to any user, this information item contains “n/a”.

ASVPP License Is Assigned to Device

Whether this license is currently assigned to a device (as opposed to a user).

ASVPP License Is Device-Assignable

Whether this license is can be assigned to a device (as opposed to a user).

ASVPP License Product Name

The name of the product covered by this license. This is the same name that the product has in the app store or book store.

ASVPP License Product Type

The type of the product covered by this license (application or book).

Mobile Configuration Profile Definitions

The **Mobile Configuration Profile Definitions** category contains information on the configuration profiles with have been imported into LANrev.

These information items can be used in the **Mobile Devices** window, in the **Assignable Items** > **Configuration Profiles** group.

Mobile Profile Name

The name of the configuration profile.

Mobile Platform Type

The mobile OS platform to which this configuration profile applies.

Mobile Profile Type

The type of profile – for example, device profile or app profile. Device profiles contain settings for the hardware or operating system, app profiles contain settings for individual apps.

Mobile Profile Description

The description of the configuration profile.

Mobile Profile Organization

The organization which has issued the configuration profile.

Mobile Profile Identifier

The unique identifier of the configuration profile, as entered by the creator of the profile.

Mobile Profile UUID

The automatically created globally unique ID of the configuration profile.

Mobile Profile Allow Removal

Whether the profile may be removed from the iOS device by the user. Possible values include, “Never“, “Always“, and “With authentication“.

Mobile Profile Variables Used

A comma-separated list of variables that are used in this configuration profile.

See “Using variables in configuration profiles” on page 185 for more information on variables in configuration profiles.

Mobile Profile App Bundle Identifier

The unique identifier of the application package to which this configuration profile applies.

Assigned Mobile Profile Availability

Whether the profile is always available on the devices to which it was assigned or only at certain times.

Assigned Mobile Profile Availability Start Time

The time when the profile becomes available on the devices to which it was assigned.

Assigned Mobile Profile Availability End Time

The time when the profile stops being available on the devices to which it was assigned.

Assigned Mobile Profile Assignment Rule

Whether the profile is installed automatically or on-demand and removed automatically or manually.

iOS Provisioning Profile Definitions

The **iOS Provisioning Profile Definitions** category contains information on the provisioning profiles with have been found on administered iOS devices.

These information items can be used in the **Mobile Devices** window, in the **Assignable Items** > **Provisioning Profiles** group.

iOS Provisioning Profile Name

The name of the provisioning profile.

iOS Provisioning Profile Expiry Date

The date until which the provisioning profile is valid.

iOS Provisioning Profile UUID

The automatically created globally unique ID of the provisioning profile.

Mobile Media

The **Mobile Media** category contains information on mobile media files that are managed by LANrev.

These information items can be used in the **Mobile Devices** window, in the **Assignable Items** > **Media** group.

Media Name

The name of the mobile media file, as specified in the **Mobile Media File** dialog. (See also "Media File Name", below.)

Media Description

The description of the mobile media file, as entered in the **Mobile Media File** dialog.

Media File Size

The size (in bytes) of the mobile media file on disk.

Media Type

The file type of the mobile media file.

Media Category

The content category to which the mobile media file has been assigned in the **Mobile Media File** dialog.

Media File Can Leave LANrev Safe

Whether the mobile users are permitted to take this file out of LANrev Safe, either to view or edit it in another app or to forward it to other devices.

Media File Can Be E-Mailed

Whether the mobile media file can be sent from within LANrev Safe to the system mail program for e-mailing to another device.

Media File Can Be Printed

Whether the mobile media file can be printed from within LANrev Safe.

Media File Is WiFi-Only

Whether the mobile media file is downloaded only when the device is connected over WiFi.

Media File Last Modified

The date when the mobile media file object (as opposed to the file that it specifies) was last edited.

Media File Name

The name of the file specified in the mobile media file object. (See also Media Name, above.)

Media File Author

The author of the file, as specified in the **New Media File** dialog.

Media File Version

The version of the file, as specified in the **New Media File** dialog.

Media Unique Identifier

The unique internal modifier of the mobile media file within LANrev.

Assigned Media Availability

Whether the media file is always available on the devices to which it was assigned or only at certain times.

Assigned Media Availability Start Time

The time when the media file becomes available on the devices to which it was assigned.

Assigned Media Availability End Time

The time when the media file stops being available on the devices to which it was assigned.

Assigned Media Assignment Rule

Whether the media file is installed automatically or on-demand and removed automatically or manually.

Mobile Actions

The **Mobile Actions** category contains information on the actions which have been defined for assignment to smart policies.

These information items can be used in the **Mobile Devices** window, in views where actions are displayed.

Mobile Action Name

The name of the action.

Mobile Action Description

The description of the action, as entered by the administrator.

Mobile Action Type

The type of the action, for example, send message or freeze device.

Mobile Action Supported Platforms

The mobile operating systems on which this action can be performed.

Mobile Action Unique Identifier

The unique identifier of the action.

Mobile Action Device Execution Time

The last time the action was executed on this device.

This information item can only be used in views displaying the actions that have been performed on a particular device.

Mobile Action Policy Initial Delay

The delay between a device entering this policy and the first execution of the action on that device.

This information item can only be used in views displaying the actions assigned to a particular policy.

Mobile Action Policy Repeat Count

The number of times that the action is specified to be executed on devices belonging to this smart policy.

This information item can only be used in views displaying the actions assigned to a particular policy.

Mobile Action Policy Repeat Interval

The interval between repeated executions of the action on devices belonging to this smart policy.

This information item can only be used in views displaying the actions assigned to a particular policy.

Mobile Device Policies

The **Mobile Device Policies** category contains information on the mobile device policies which have been created in LANrev.

These information items can be used in the **Mobile Devices** window, in the **Policies** section.

Policy Name

The name of the policy.

Is Smart Policy

Whether this policy is a smart policy, that is, a policy in which mobile devices are included automatically according to rules set in the policy.s

Mobile Device Enrollment Profiles

The **Mobile Device Enrollment Profiles** category contains information on device enrollment profiles which have been created in LANrev.

These information items can be used in the **Mobile Devices** window, in the **Device Enrollment Profiles** section.

Enrollment Profile Name

The name of the enrollment profile.

Enrollment Profile UUID

The unique identifier of the enrollment profile.

Enrollment Profile Is Mandatory

Whether the profile prohibits the user from skipping the MDM enrollment during the device setup.

Enrollment Profile Is MDM Profile Removable

Whether the profile allows users to delete the MDM profiles from their devices.

Enrollment Profile Company Support Phone

The IT support phone number that has been specified in the profile.

Enrollment Profile Company Support E-Mail

The IT support e-mail address that has been specified in the profile.

Enrollment Profile Department

The department that has been specified in the profile.

Enrollment Profile Skip Location Services Setup

Whether the profile causes the device to skip the location services setup screen during setup.

Enrollment Profile Skip Restore from Backup

Whether the profile causes the device to skip during setup the screen where the user is given the option to restore the device from a backup.

Enrollment Profile Skip Apple ID Setup

Whether the profile causes the device to skip the Apple ID setup screen during setup.

Enrollment Profile Skip Terms and Conditions

Whether the profile causes the device to skip the terms and conditions screen during setup.

Enrollment Profile Skip App Analytics Setup

Whether the profile causes the device to skip the app analytics setup screen during setup.

Enrollment Profile Skip Move from Android

Whether the profile causes the device to skip the screen for importing data from Android devices during setup.

Enrollment Profile Skip Touch ID Setup

Whether the profile causes the device to skip the Touch ID setup screen during setup.

Enrollment Profile Skip Passcode Lock Setup

Whether the profile causes the device to skip the passcode lock setup screen during setup.

Enrollment Profile Skip Apple Pay Setup

Whether the profile causes the device to skip the Apple Pay setup screen during setup.

Enrollment Profile Skip True Tone Display Setup

Whether the profile causes the device to skip the True Tone display setup screen during setup.

Enrollment Profile Skip Home Button Setup

Whether the profile causes the device to skip the Home button setup screen during setup.

Enrollment Profile Skip Siri Setup

Whether the profile causes the device to skip the Siri setup screen during setup.

Enrollment Profile Skip Display Zoom Setup

Whether the profile causes the device to skip the display zoom screen during setup. The screen let's users of certain iOS devices decide whether text and controls on their devices should be displayed in standard or enlarged sizes.

Enrollment Profile Skip Registration

Whether the profile causes the device to skip the registration screen during setup.

Enrollment Profile Skip FileVault Setup

Whether the profile causes the device to skip the FileVault screen during setup.

Enrollment Profile Skip Local Account Setup

Whether the profile causes the device to skip the setup of a local user account.

Enrollment Profile Create Primary Account

Whether the profile causes the creation of an additional administrator account on the device.

Enrollment Profile Supervise Device

Whether the profile sets the device to be supervised.

Enrollment Profile Perform Queued Commands During Setup

Whether the profile makes the device ask for any queued MDM commands and execute them during the setup process.

Enrollment Profile Require Authentication

Whether the profile requires the user of the device to enter valid Active Directory credentials during setup.

Enrollment Profile Allow Computers to Connect

Whether the profile allows the managed devices to be configured from computers to which they are connected via USB.

Device Enrollment Account Expiry

The expiration date of the device enrollment program account to which this device or profile belongs.

This information item can also be used in tables displaying devices (in addition to tables displaying enrollment profiles).

Device Enrollment Account Name

The name of the device enrollment program account to which this device or profile belongs.

This information item can also be used in tables displaying devices (in addition to tables displaying enrollment profiles).

Device Enrollment Account Identifier

The unique identifier of the device enrollment program account to which this device or profile belongs.

While the name of the account (see above) may be changed by you, the identifier is guaranteed to remain unchanged for the life of the account. It is therefore a more robust way to specify accounts, for example, in smart groups.

This information item can also be used in tables displaying devices (in addition to tables displaying enrollment profiles).

Device Commands

The **Device Commands** category contains information on commands issued to managed mobile devices.

These information items can be used in the **Mobile Devices** window, in the **Commands** section.

Mobile Device Command Type

The command that was sent to the mobile device.

Mobile Device Command Status

The current status of the command.

Mobile Device Command Time Issued

The date and time when the command was sent by LANrev Admin to LANrev Server.

Note that this time is not necessarily the time when the mobile device received the command, as commands are forwarded to the device only when it contacts the push notification server. This can take some time, even days, if the device is, for example, switched off or overseas with roaming disabled.

Mobile Device Command Error

The error, if any, of the command execution that was returned.

Mobile Device Command Details

Additional information about the issued command, for example, the installed item or the scope of the command.

Some commands have no detail information.

Mobile Device Command Error Info

A verbose explanation of the returned error.

Mobile Device Command Finish Time

The time when the execution of the command finished on the mobile device.

Mobile Device Command User

The Apple ID of the user of a shared device when a command sent from LANrev is intended only for that user. This is “n/a” for commands sent to the device.

EAS Policies

The **EAS Policies** category contains information on the Exchange ActiveSync policy settings which are active on administered Windows Phone devices.

These information items can be used in the **Mobile Devices** window.

All information items in this category apply only to Windows Phone devices.

EAS Allow Bluetooth

Whether and to which degree the EAS policy active on this device allow Bluetooth to be used on it:

- Allow: The user can access all Bluetooth capabilities.
- HandsFreeOnly: The user can use Bluetooth headsets, but all other devices are blocked.
- Disable: The user cannot access any Bluetooth functions of this device.

EAS Allow Browser

Whether the EAS policy active on this device allows Microsoft Pocket Internet Explorer to be used on it. Note that this setting does not affect third-party browsers.

EAS Allow Camera

Whether the EAS policy active on this device allows the camera (if any) of it to be used.

EAS Allow Consumer E-Mail

Whether the EAS policy active on this device allows the user of it to configure a personal e-mail account.

EAS Allow Desktop Sync

Whether the EAS policy active on this device allows it to be synchronized with a desktop computer via direct cable connection.

EAS Allow External Device Management

Whether the EAS policy active on this device allows it to access the Exchange server even if it is being managed by an external device management program. Note that LANrev is not considered “external” for purposes of this setting, because it works through the Exchange server.

EAS Allow HTML E-Mail

Whether the EAS policy active on this device allows HTML e-mails on it.

EAS Allow Internet Sharing

Whether the EAS policy active on this device allows it to be used as an internet modem for other devices (tethering).

EAS Allow IrDA

Whether the EAS policy active on this device allows it to accept infrared connections.

EAS Allow Mobile OTA Update

Whether the EAS policy active on this device allows it to see certain available updates. Not all Windows Phone devices may support this restriction.

EAS Allow Non-Provisionable Devices

Whether the EAS policy active on this device allows non-provisionable devices to synchronize with the Exchange server.

Non-provisionable devices are devices that cannot enforce all of the restrictions specified in the EAS policy.

EAS Allow POP/IMAP E-Mail

Whether the EAS policy active on this device allows the user to configure a POP or IMAP e-mail account on it.

EAS Allow Remote Desktop

Whether the EAS policy active on this device allows it to view the screens of other devices using a remote desktop connection.

EAS Allow Simple Device Password

Whether the EAS policy active on this device allows the user to set a device password with a recognizable pattern (for example, 1111 or 1234) on it.

EAS Allow S/MIME Encryption Algorithm Negotiation

Whether the EAS policy active on this device allows the messaging application to negotiate a different encryption algorithm in cases where a receiver does not support the specified algorithm.

EAS Allow S/MIME Software Certificates

Whether the EAS policy active on this device allows S/MIME software certificates.

EAS Allow Storage Card

Whether the EAS policy active on this device allows access to information on storage cards in the device.

EAS Allow Text Messaging

Whether the EAS policy active on this device allows its user to send text messages.

EAS Allow Unsigned Applications

Whether the EAS policy active on this device allows unsigned applications to be installed on it.

EAS Allow Unsigned Installation Packages

Whether the EAS policy active on this device allows unsigned installation packages to be run on it.

EAS Allow WiFi

Whether the EAS policy active on this device allows wireless Internet access on it.

EAS Alphanumeric Device Password Required

Whether the EAS policy active on this device requires the device password to be alphanumeric.

EAS Allowed Applications

A list of applications that are marked as approved for this device by the EAS policy active on it.

EAS Attachments Enabled

Whether the EAS policy active on this device allows to user to download e-mail attachments.

EAS Policy Creation Date

The date when the EAS policy active on this device was created.

EAS Device Encryption Enabled

Whether the EAS policy active on this device enables the encryption of the device.

EAS Device Password Enabled

Whether the EAS policy active on this device requires the user to set a password for the device.

EAS Device Password Expiration

The maximum time the EAS policy active on the device allows the same password to be used before it must be changed. The time has the format dd.hh.mm:ss, for example, “04.17.30:00”. If no maximum time is specified, “unlimited” is displayed.

EAS Device Password History

How many previously used password the EAS policy active on this device requires the device to store. The device will not let the user specify a new password that is the same as one of the stored passwords.

EAS Device Policy Refresh Interval

The interval in which the Exchange server sends the EAS policy to this mobile device, as specified in the EAS policy active on the device. The interval has the format dd.hh.mm:ss, for example, “04.17.30:00”. If no interval is specified, “unlimited” is displayed.

EAS IRM Enabled

Whether the EAS policy active on this device enables information rights management.

EAS Is Default Policy

Whether the EAS policy active on this device is the default mailbox policy.

EAS Maximum Attachment Size

The maximum size of e-mail attachments in kilobytes that the EAS policy active on this device allows to be downloaded.

EAS Maximum Calendar Age Filter

The maximum range of calendar entries that the EAS policy active on this device specifies to be synchronized.

EAS Maximum Device Password Failed Attempts

The maximum number of incorrect password entries that the EAS policy active on this device allows before refusing additional attempts.

EAS Maximum E-Mail Age Filter

The maximum age of e-mails that are synchronized to this device by the EAS policy active on it. E-mails that are older than the specified time are not synchronized.

EAS Maximum E-Mail Body Truncation Size	The maximum size in kilobytes of plain-text e-mail bodies (that is, not counting attachments or headers) that the EAS policy active on this device synchronizes in their entirety. E-mails bodies larger than this size are truncated.
EAS Maximum E-Mail HTML Body Truncation Size	The maximum size in kilobytes of HTML e-mail bodies (that is, not counting attachments or headers) that the EAS policy active on this device synchronizes in their entirety. E-mails bodies larger than this size are truncated.
EAS Maximum Inactivity Before Device Lock	The interval of inactivity before this device locks itself that the EAS policy active on it specifies. The interval has the format hh.mm:ss, for example, “06.20:00”. If no interval is specified, “unlimited” is displayed.
EAS Minimum Device Password Complex Characters	The minimum number of non-letter characters that the EAS policy active on the device requires the device password to include.
EAS Minimum Device Password Length	The minimum number of characters that the EAS policy active on the device requires the device password to include in total.
EAS Mobile OTA Update Mode	The kinds of updates that the EAS policy active on the device allows the device to see. Not all Windows Phone devices may support this restriction.
EAS Policy Modification Date	The date when the EAS policy active on this device was last modified.
EAS Policy Name	The name of the EAS policy active on this device.
EAS Password Recovery Enabled	Whether the EAS policy active on this device allows the recovery password to be stored on an Exchange server.
EAS Require Device Encryption	Whether the EAS policy active on this device requires the device to be encrypted.
EAS Require Encrypted S/MIME Messages	Whether the EAS policy active on this device requires S/MIME messages to be encrypted.
EAS Require Encryption S/MIME Algorithm	The algorithm that the EAS policy active on this device specifies for encrypting an S/MIME message.
EAS Require Manual Sync When Roaming	Whether the EAS policy active on this device disables automatic synchronization with the Exchange server while the device is roaming.
EAS Require Signed S/MIME Algorithm	The algorithm that the EAS policy active on this device specifies for signing an S/MIME message.
EAS Require Signed S/MIME Messages	Whether the EAS policy active on this device requires S/MIME messages to be signed.

EAS Require Storage Card Encryption
Whether the EAS policy active on this device requires any storage card used in the device to be encrypted.

EAS Blocked Applications
A list of applications on the mobile device that are prevented from running by the EAS policy active on the device.

EAS UNC Access Enabled
Whether the EAS policy active on this device allows it to access Windows file shares.

EAS WSS Access Enabled
Whether the EAS policy active on this device allows it to access SharePoint services.

iBooks Books

The **iBooks Books** category contains summary information on entries for books from the iBooks Store that have been added to LANrev.

These information items can be used in the Bookstore Books category of the **Mobile Devices** window.

Book Title
The title of the book, as specified in the LANrev entry.

Book Category
The genre of the book, as specified in the LANrev entry.

Book Short Description
The short description of the book, as specified in the LANrev entry.

Book Long Description
The long description of the book, as specified in the LANrev entry.

Book URL
The URL of the book in the iTunes store.

Book Bookstore ID
The ID of the book in the iTunes store.

Book Assignment Rule
Whether the book is installed automatically or on-demand and removed automatically or manually.

Book VPP Licenses Purchased
The total number of iBooks Store volume purchase program managed licenses that have been purchased for this book.

Book VPP Licenses Assigned
The total number of iBooks Store volume purchase program managed licenses for this book that have been assigned to users.

Book VPP Licenses Remaining
The total number of iBooks Store volume purchase program managed licenses for this book that remain available for assignment.

Book VPP Accounts
The names of all your accounts for the Apple volume purchase program that contain licenses for this book.

Windows Reinstallation Tasks

The **Windows Reinstallation Tasks** category contains information on reinstallation processes for Windows computers that have been dispatched to the LANrev PXE server or to a FOG server.

These information items can be used in the **Window Reinstallation Tasks** window.

There are two subcategories:

- **FOG Reinstallation Tasks** (page 934)
- **LANrev Reinstallation Tasks** (page 935)

FOG Reinstallation Tasks

The **FOG Reinstallation Tasks** category contains information on reinstallation tasks handled by a FOG server.

These information items can be used in the **Window Reinstallation Tasks** window, in the **FOG Reinstallation Tasks** section.

FOG Host Name

The name of the computer that is being reinstalled.

FOG Image Name

The name of the image on the FOG server that is being used for the reinstallation.

FOG Image Size

The size of the image on the FOG server that is being used for the reinstallation.

FOG Image Creation Date

The date when the image on the FOG server that is being used for the reinstallation was created.

FOG Image Created By

The username of the administrator who created the image on the FOG server that is being used for the reinstallation.

FOG Task Name

The name that has been set for the FOG task.

LANrev does not set task names, so this information item always displays “n/a”, but FOG tasks entered from other sources, for example, through the web interface, may have names.

FOG Task State

The current processing state of the reinstallation task, for example, “in progress”. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

FOG Task Type

The type of the FOG task displayed. Tasks initiated by LANrev always have the type “Push image” but tasks from other sources, for example, FOG’s web interface, may have different types.

FOG Task Creation Date

The date and time when the FOG server received the command to execute the task.

FOG Task Data Copied

The amount of data that has been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

FOG Task Data Total

The total amount of data that needs to be copied to the target computer.

FOG Task Percent Complete

The ratio of the total data that has already been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

FOG Task Time Elapsed

The length of time that the reinstallation process has been taken so far. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

For completed reinstallations, the total amount of time they have taken is displayed.

LANrev Reinstallation Tasks

The **LANrev Reinstallation Tasks** category contains information on reinstallation tasks handled by a LANrev server with the support of a LANrev PXE server.

These information items can be used in the **Window Reinstallation Tasks** window, in the **LANrev Reinstallation Tasks** section.

Reinstallation Task State

The current processing state of the reinstallation task, for example, “In progress.

Reinstallation Task Percent Complete

The ratio of the total data that has already been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

Reinstallation Task Info

Diagnostic info on the reinstallation task, if any.

Reinstallation Task Data Total

The total amount of data that needs to be copied to the target computer.

Reinstallation Task Data Copied

The amount of data that has so far been copied to the target computer. Note that this information is updated only periodically. You can refresh the information by right-clicking and choosing **Synchronize Records** from the context menu.

Reinstallation Task Last Update

The last time that information about this task was received from the updater process.

In effect, this is the record modification date for the reinstallation task description and the date at which all variable fields (like Reinstallation Task Data Copied) were updated.

Reinstallation Task Join AD Domain

Whether the computer being reinstalled will automatically join an Active Directory domain afterwards.

This information item corresponds to the **Join domain after imaging task** option in the **Reinstall Windows Computer** dialog.

Reinstallation Task Domain to Join

The name of the Active Directory domain (if any) that the computer being reinstalled will join after the reinstallation is complete.

This information item corresponds to the **Domain to join** field in the **Reinstall Windows Computer** dialog.

Reinstallation Task Hostname Action

What will done about the hostname of the reinstalled computer.

This information item corresponds to the **Computer name** option in the **Reinstall Windows Computer** dialog.

Reinstallation Task Hostname to Set

The new hostname of the reinstalled computer (if it is not set to keep the previous hostname).

This information item corresponds to the **Use name** field in the **Reinstall Windows Computer** dialog.

Classroom Management

The **Classroom Management** category contains information on persons and objects used in managing classrooms.

These information items can be used in the appropriate sections of the **Classroom Management** window. (For example, class-related items can be used in table views that displays class information.)

Classroom Class Name

The name of a class that has been defined.

Classroom Room

The name or number of the room that is assigned to the class.

Classroom Class Source

The source of the class information, such as manual entry or a kind of database system connected to Apple School Manager.

Classroom Class Source System Identifier

The identifier that the record for this class was given in the source system.

Classroom Class Unique Identifier

The unique identifier of the class.

Classroom Class Data Origin

The way this class information was entered into LANrev – from Apple School Manager, by locally importing a data file, or by manual entry.

Classroom Location Name

The name of a location where classes are held.

Classroom Location Source

The source of the location information, such as manual entry or a kind of database system connected to Apple School Manager.

Classroom Location Source System Identifier

The identifier that the record for this location was given in the source system.

Classroom Location Unique Identifier

The unique identifier of the location.

Classroom Location Data Origin

The way this location information was entered into LANrev – from Apple School Manager, by locally importing a data file, or by manual entry.

Classroom Course Name

The name of a course that has been defined.

Classroom Course Source

The source of the course information, such as manual entry or a kind of database system connected to Apple School Manager.

Classroom Course Source System Identifier

The identifier that the record for this course was given in the source system.

Classroom Course Unique Identifier

The unique identifier of the course.

Classroom Course Data Origin

The way this course information was entered into LANrev – from Apple School Manager, by locally importing a data file, or by manual entry.

Classroom Person Name

The full name of a person set up in classroom management, such as a teacher or student.

Classroom Person First Name

The first name of a person set up in classroom management, such as a teacher or student.

Classroom Person Middle Names

The middle names or initials of a person set up in classroom management, such as a teacher or student.

Classroom Person Last Name

The first name of a person set up in classroom management, such as a teacher or student.

Classroom Person Managed Apple ID

The Apple ID which the person uses in the classroom.

Classroom Person Grade

The grade to which the person belongs. Not all persons have a grade assigned.

Classroom Person Name

The role which the person plays in the classroom. The available roles are defined in Apple School Manager.

Classroom Person Role

The role which the person plays in the classroom. The available roles are defined in Apple School Manager.

Classroom Person Password Prompt

The type of password prompt that a shared classroom device displays for this person. If no prompt type is specified, the default prompt from the operating system is displayed.

Classroom Person Source

The source of the person information, such as manual entry or a kind of database system connected to Apple School Manager.

Classroom Person Source System Identifier

The identifier that the record for this person was given in the source system.

Classroom Person Unique Identifier

The unique identifier of the person.

Classroom Person Data Origin

The way this person information was entered into LANrev – from Apple School Manager, by locally importing a data file, or by manual entry.

Classroom Person Custom Info 1

The information for this person in the Custom Info 1 field.

Classroom Person Custom Info 2

The information for this person in the Custom Info 2 field.

Chapter 28 LANrev Remote

LANrev Remote is a VNC viewer application that is part of LANrev. It is compatible with any VNC-compliant host software on remote computers.

LANrev Remote is automatically installed with LANrev and usually launched from within it with the **Remote Control** context menu command.

The menus and commands of LANrev Remote as well as its menu bar indicator are described in these sections:

- "LANrev Remote" on page 939
- "Connection" on page 941
- "Edit" on page 942
- "View" on page 943
- "Session" on page 945
- "Command" on page 947
- "Window" on page 947
- "Help" on page 948
- "Menu bar indicator" on page 948

For the mobile LANrev Remote app, see "LANrev Remote" on page 957.

LANrev Remote

The **LANrev Remote** menu contains the **About**, **Preferences**, and **Quit** commands. The rest of the menu is under control of the operating system.

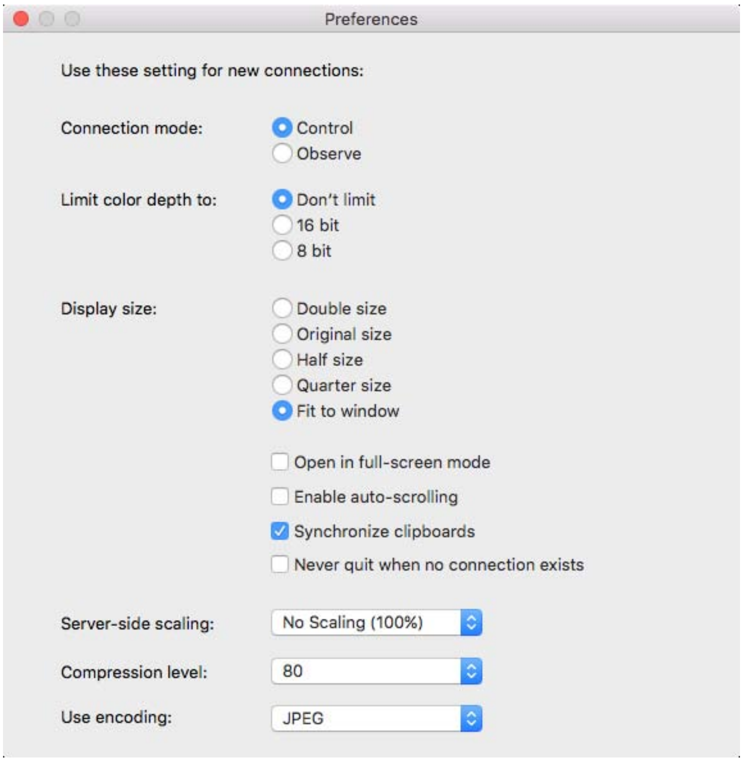
- **About LANrev Remote** (page 939)
- **Preferences** (page 940)
- **Quit LANrev Remote** (page 941)

About LANrev Remote

The **About LANrev Remote** command opens the application's About dialog. The dialog contains the application version and copyright information.

Preferences

The **Preferences** command opens the **Preferences** dialog that lets you specify settings for the application:



Preferences

Use these setting for new connections:

Connection mode: ● Control ○ Observe

Limit color depth to: ● Don't limit ○ 16 bit ○ 8 bit

Display size: ○ Double size ○ Original size ○ Half size ○ Quarter size ● Fit to window

□ Open in full-screen mode

□ Enable auto-scrolling

☑ Synchronize clipboards

□ Never quit when no connection exists

Server-side scaling: No Scaling (100%)

Compression level: 80

Use encoding: JPEG

The dialog contains settings for specifying the defaults for a new connection:

- **Connection mode**: Choose how a new connection accesses remote computers:
    - **Control**: You can see the screen, use the mouse, and input text.
    - **Observe**: You can just see the screen but not control the computer through the remote link.
- **Limit color depth to**: The maximum color depth that the representation of the remote screen on your computer may have. If you specify **Don't limit**, the full screen depth of the remote **computer is used.**
- **Display size**: The initial enlargement or reduction used to display the remote computer screen. If you choose **Fit to window**, the maximum size is used that fully fits in the LANrev Remote window. Resizing that window changes the display enlargement factor.
- **Open in full-screen mode**: If this option is checked, the window for a new connection takes up your whole screen.
- **Enable auto-scrolling**: If this option is checked, the display of the remote screen in the LANrev Remote window automatically scrolls when the mouse pointer nears the edge of the window.
- **Synchronize clipboards**: If this option is checked, the clipboard of the remote computer and your clipboard are automatically synchronized in a new connection.

- **Never quit when no connection exists**: By default, LANrev Remote quits when it is not connected to a remote device. If this option is checked, it stays open even when it does not display any remote screens.
- **Server-side scaling**: Any scaling that the remote connection server on the viewed computer performs before transmitting the screen image.
  Scaling the image on the server reduces the amount of data to transmit and may improve the display speed but reduces the size and therefore the quality of the displayed image.
- **Compression level**: The amount of compression to apply to the image before transmitting it. Higher compression rates (lower numbers) accelerate the transmission but reduce the image quality.
- **Use encoding**: Which type of image compression to use for transmitting the screen content of the remote computer.

Quit LANrev Remote

The **Quit LANrev Remote** command quits LANrev Remote. If there are open connections, they are closed.

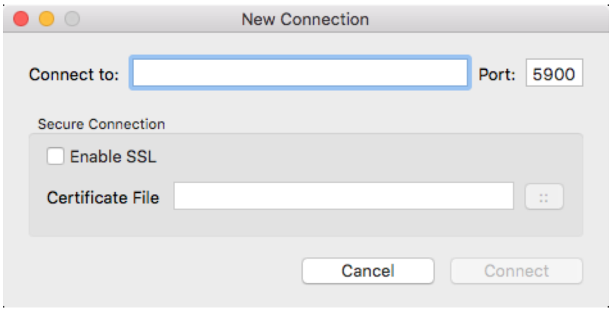
Connection

The **Connection** menu contains commands for opening and closing connections:

- **New** (page 941)
- **Open** (page 942)
- **Recent Connections** (page 942)
- **Close** (page 942)
- **Save As** (page 942)

New

The **New** command opens the **New Connection** dialog:


New Connection

Connect to:

Port: 5900

Secure Connection

□ Enable SSL

Certificate File

The dialog contains these elements:

- **Connect to**: The DNS name or IP address of the computer to which you want to connect.
- **Port**: The port of the remote computer to which you want to connect. This is usually 5900.
- Additional elements in the dialog are intended for future expansion and cannot yet be used.

Open

The **Open** command opens a standard Open dialog in which you can choose a saved connection document.

Clicking **Open** causes LANrev Remote to connect to the remote computer specified in the connection document with the saved settings.

Recent Connections

The **Recent Connections** submenu contains the most recent connections that you have established in LANrev Remote.

Choosing a connection from the submenu opens it with the same settings it had when you closed it.

Choosing **Clear Menu** removes all recent connections from the submenu.

Close

The **Close** command closes the frontmost window and the connection to the computer displayed in it.

Save As

The **Save As** command opens a standard Save dialog in which you can save the current connection to disk as a document.

Clicking **Save** saves the address of the target computer and the current connection settings in a connection document.

Edit

The **Edit** menu contains the usual clipboard-related commands as well as commands for manually transferring the clipboard content to or from the remote computer and a command for accessing special characters.

- **Cut** (page 942)
- **Copy** (page 942)
- **Paste** (page 942)
- **Delete** (page 943)
- **Select All** (page 943)
- **Send Clipboard** (page 943)
- **Get Clipboard** (page 943)
- **Start Dictation** (page 943)
- **Emoji & Symbols** (page 943)

Cut

The **Cut** command has no function in LANrev Remote.

Copy

The **Copy** command has no function in LANrev Remote.

Paste

The **Paste** command has no function in LANrev Remote.

Delete

The **Delete** command has no function in LANrev Remote.

Select All

The **Select All** command has no function in LANrev Remote.

Send Clipboard

The **Send Clipboard** command transfers the content of your clipboard to the clipboard of the remote computer displayed in the frontmost window.

Get Clipboard

The **Get Clipboard** command transfers the content of the clipboard of the remote computer displayed in the frontmost window to your clipboard.

Start Dictation

The **Start Dictation** command allows you to enter text by spoken voice.

This command is provided by the operating system; see the macOS documentation for details.

Emoji & Symbols

The **Emoji & Symbols** command opens the **Characters** Palette of macOS that lets you enter characters that are not available on the keyboard.

This palette is provided by the operating system; see the macOS documentation for details.

View

The **View** menu contains commands for setting the size of the remote display and displaying and customizing the toolbar:

- **Show Tab Bar** (page 943)
- **Full-Screen Mode** (page 944)
- **Auto-Scrolling** (page 944)
- **Double Size** (page 944)
- **Original Size** (page 944)
- **Half Size** (page 944)
- **Quarter Size** (page 944)
- **Fit to Window** (page 944)
- **Show Toolbar** (page 944)
- **Hide Toolbar** (page 944)
- **Customize Toolbar** (page 944)

Show Tab Bar

The **Show Tab Bar** command displays or hides the tab bar in the frontmost window.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Full-Screen Mode

The **Full-Screen Mode** command expands the frontmost window to fill the entire screen.

To return the display to windowed mode, move the mouse to the middle of the upper screen border and click the Window icon on the tab that appears.

Auto-Scrolling

The **Auto-Scrolling** command toggles the auto-scrolling mode of the frontmost window.

In auto-scrolling mode, the display scrolls automatically when the mouse pointer nears the edge of the window. This setting has no effect when the entire remote screen is visible in the window.

Double Size

The **Double Size** command enlarges the display in the frontmost window to 200%. (Each remote pixel is displayed as two by two local pixels.)

Original Size

The **Original Size** command zooms the display in the frontmost window to 100%. (Each remote pixel is displayed as one local pixel.)

Half Size

The **Half Size** command reduces the display in the frontmost window to 50%. (Two by two remote pixels are displayed as one local pixel.)

Quarter Size

The **Quarter Size** command reduces the display in the frontmost window to 25%. (Four by four remote pixels are displayed as one local pixel.)

Fit to Window

The **Fit to Window** command enlarges or reduces the display in the frontmost window to the maximum size that still fits in the window.

If the window is subsequently resized, the zooming of the remote screen is automatically adapted.

Show Toolbar

The **Show Toolbar** command displays the toolbar of the frontmost window. It is available only if the toolbar of the frontmost window is currently hidden.

Hide Toolbar

The **Hide Toolbar** command hides the toolbar of the frontmost window. It is available only if the toolbar of the frontmost window is currently visible.

Customize Toolbar

The **Customize Toolbar** command lets you customize the contents of the toolbar of the frontmost window.

Choosing the command displays a customization dialog that contains these elements:

- **Full Screen**: Clicking this button sets the window to full-screen mode. This is the same as choosing the **Full-Screen Mode** command.
- **Color Depth**: You can choose the color depth from this pop-up menu. This is the same as choosing the corresponding option from the **Session** menu.
- **Toggle Auto-Scrolling**: Clicking this button switches auto-scrolling on (if it is currently off) or off (if it is currently on). This is the same as choosing the **Auto-Scrolling** command.
- **Zoom**: You can choose the zoom factor from this pop-up menu. This is the same as choosing the corresponding option from the **View** menu.
- **Get Clipboard**: Clicking this button copies the content of the remote clipboard to your clipboard. This is the same as choosing the **Get Clipboard** command.
- **Send Clipboard**: Clicking this button copies the content of your clipboard to the remote clipboard. This is the same as choosing the **Send Clipboard** command.
- **Toggle Clipboard Sync**: Clicking this button switches clipboard synchronization on (if it is currently off) or off (if it is currently on). This is the same as choosing the **Automatic Clipboard Transfer** command.
- **Toggle Observe/Control**: Clicking this button switches between the Control and Observe modes. This is the same as choosing the **Observe Remote Computer** and **Control Remote Computer** commands.
- Key press button: Clicking this button sends a keyboard combination to the remote device. Which command is sent varies according to the controlled device and is noted below the button.
- **Compression Level**: The amount of compression to apply to the image before transmitting it. Higher compression rates (lower numbers) accelerate the transmission but reduce the image quality.
- **Server-side scaling**: Any scaling that the remote connection server on the viewed computer performs before transmitting the screen image.
  Scaling the image on the server reduces the amount of data to transmit and may improve the display speed but reduces the size and therefore the quality of the displayed image.

The other elements in the dialog are standard elements found in all toolbar customization dialogs.

Session

The **Session** menu contains commands for configuring the running session:

- **Automatic Clipboard Transfer** (page 946)
- **Don’t Limit Color Depth** (page 946)

- **Limit Color to 16 Bit** (page 946)
- **Limit Color to 8 Bit** (page 946)
- **No Server-Side Scaling (100%)** (page 946)
- **Three Quarters Server-Side Scaling (75%)** (page 946)
- **Half Server-Side Scaling (50%)** (page 946)
- **Quarter Server-Side Scaling (25%)** (page 946)
- **Observe Remote Computer** (page 947)
- **Control Remote Computer** (page 947)

Automatic Clipboard Transfer

The **Automatic Clipboard Transfer** command toggles the synchronization of the local clipboard and the clipboard of the computer displayed in the frontmost window.

If the clipboards are synchronized, each change to one of them is automatically applied to the other as well. If they are not synchronized, they normally have different content (which can be transferred between them manually with the **Send Clipboard** and **Get Clipboard** commands).

Don’t Limit Color Depth

The **Don’t Limit Color Depth** command sets the frontmost window to display the same color depth as the remote computer does locally.

Limit Color to 16 Bit

The **Limit Color to 16 Bit** command sets the frontmost window to a color depth of 16 bit per pixel or the same color depth as the remote computer uses locally, whichever is lower.

Limit Color to 8 Bit

The **Limit Color to 8 Bit** command sets the frontmost window to a color depth of 8 bit per pixel or the same color depth as the remote computer uses locally, whichever is lower.

No Server-Side Scaling (100%)

The **No Server-Side Scaling (100%)** command instructs the remote computer to not scale the screen image before transmitting it.

Three Quarters Server-Side Scaling (75%)

The **Three-Quarters Server-Side Scaling (75%)** command instructs the remote computer to scale the screen image to 75% of its original size before transmitting it.

Half Server-Side Scaling (50%)

The **Half Server-Side Scaling (50%)** command instructs the remote computer to scale the screen image to 50% of its original size before transmitting it.

Quarter Server-Side Scaling (25%)

The **Quarter Server-Side Scaling (25%)** command instructs the remote computer to scale the screen image to 25% of its original size before transmitting it.

Observe Remote Computer

The **Observe Remote Computer** command sets the mode of the session displayed in the frontmost window to Observe. You can only see the remote screen but not perform any actions on it.

Control Remote Computer

The **Control Remote Computer** command sets the mode of the session displayed in the frontmost window to Control. You can both see the remote screen and perform any actions on it by controlling the remote mouse and the keyboard input.

Command

The **Command** menu contains commands for sending keyboard combinations to remote computers.

Choosing any of the commands from this menu is the same as pressing the corresponding keys locally on the remote computer that is displayed in the frontmost window.

Window

The **Window** menu contains window management commands and a list of open windows:

- **Minimize** (page 947)
- **Zoom** (page 947)
- **Show Previous Tab** (page 947)
- **Show Next Tab** (page 947)
- **Move Tab to New Window** (page 948)
- **Merge All Windows** (page 948)
- **Bring All to Front** (page 948)

Minimize

The **Minimize** command reduces the frontmost window to an icon and puts it in the dock.

Zoom

The **Zoom** command toggles the frontmost window between its normal size and full-screen size.

Show Previous Tab

The **Show Previous Tab** command displays the previous tab in the front-most window, if that window contains multiple tabs.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Show Next Tab

The **Show Next Tab** command displays the next tab in the front-most window, if that window contains multiple tabs.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Move Tab to New Window

The **Move Tab to New Window** command displays the front-most tab in a window of its own.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Merge All Windows

The **Merge All Windows** command moves all open LANrev Remote windows as tabs into a single window.

The command is provided by macOS 10.12 (Sierra) and above; it is not available in older versions. See the macOS documentation for details.

Bring All to Front

The **Bring All to Front** command puts all windows of LANrev Remote in front of the windows of all other applications.

Help

The **Help** menu contains the system-wide help search and the online help.

- **LANrev Remote Help** (page 948)

LANrev Remote Help

The **LANrev Remote Help** command opens the application’s online help.

Menu bar indicator

LANrev Remote provides an indicator icon in the menu bar, which lets a user view basic information about incoming connections and disconnect them when desired.

The indicator provides access to these menu commands:

- **Disconnect <user>** (page 948)
- **Disconnect All** (page 949)
- **About This Connection** (page 949)

Disconnect <user>

The **Disconnect <user>** command lets you disconnect individual users who currently have an active remote connection to your computer.

There is one **Disconnect** command for each active incoming remote control connection.

Disconnect All

The **Disconnect All** command lets you disconnect all users who currently have an active remote connection to your computer. The command is available only when there is more than one active connection.

About This Connection

The **About This Connection** command opens a message window that displays some basic information about active incoming remote control connections and explains for what they are used.

Chapter 29 Mobile Apps

LANrev comes with three mobile apps, LANrev Apps, LANrev Find, and LANrev Safe, that let users of managed mobile devices access distributed software and apps, and that provide reporting, messaging, and other functions to administrators.

The apps are described in these sections:

- "LANrev Apps" on page 950
  - "LANrev Apps for iOS" on page 950
  - "LANrev Apps for Android" on page 952
- "LANrev Find" on page 954
- "LANrev Remote" on page 957
- "LANrev Safe" on page 957
  - "LANrev Safe for iOS" on page 957
  - "LANrev Safe for Android" on page 964

LANrev Apps

LANrev Apps is the client app for mobile devices that ties them into LANrev:

- It enables administrators to provide software and configuration profiles to mobile device users.
- It reports on the state and properties of the mobile device.
- It provides a channel for direct distribution of messages for LANrev administrators to mobile device users.

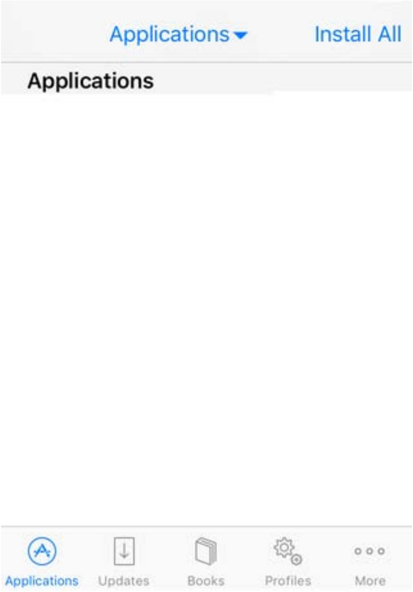
LANrev Apps is available for iOS and Android:

- "LANrev Apps for iOS" on page 950
- "LANrev Apps for Android" on page 952

LANrev Apps for iOS

The installation of LANrev Apps is described in "Preparing iOS devices for software installation" on page 195.

LANrev Apps is structured in multiple sections, which are described below.



Applications

The Applications section lists all applications that have been made available to the mobile device and that are not yet installed on it. (For information on making apps available, see “Installing software on mobile devices” on page 197.)

The **Applications** menu at the top of the screen lets you restrict the display to a particular category of applications.

Tapping one of the listed applications displays details about it. Tapping the **Install** button installs the application on the mobile device.

Tapping **Install All** installs all listed apps on your device.

Updates

The Updates section list all available updates for apps that have been installed on this device via LANrev Apps.

The **Updates** menu at the top of the screen lets you restrict the display to updates for a particular category of applications.

Tapping an update displays details on it. Tapping **Update** installs the update on the mobile device.

Tapping **Update All** in the main Updates section installs all available updates.

Books

The Books section lists all bookstore books that have been made available to the mobile device and that are not yet installed on it. (For information on making books available, see “Distributing iBooks Store books to mobile users” on page 229.)

The **Books** menu at the top of the screen lets you restrict the display to a particular category of books.

Tapping a book displays details on it. Tapping **Install** installs the book on the mobile device.

Profiles

The Profiles section lists all configuration profiles that are available for installation on the iOS device.

The **Profiles** menu at the top of the screen lets you restrict the display to a particular category of profiles.

Tapping one of the listed applications displays details about it. Tapping **Install** installs the profile on the mobile device.

Messages

The Messages section contains all messages that have been sent from LANrev to this mobile device.

Tapping the **Clear** button removes all messages.

More

The **More** button opens a screen where additional sections are listed.

Tapping the **Edit** button lets you configure which sections are listed on the main screen. To add a section to the main screen, drag it to the desired position in the button bar at the bottom of the edit screen. Tap **Done** to return to the More screen.

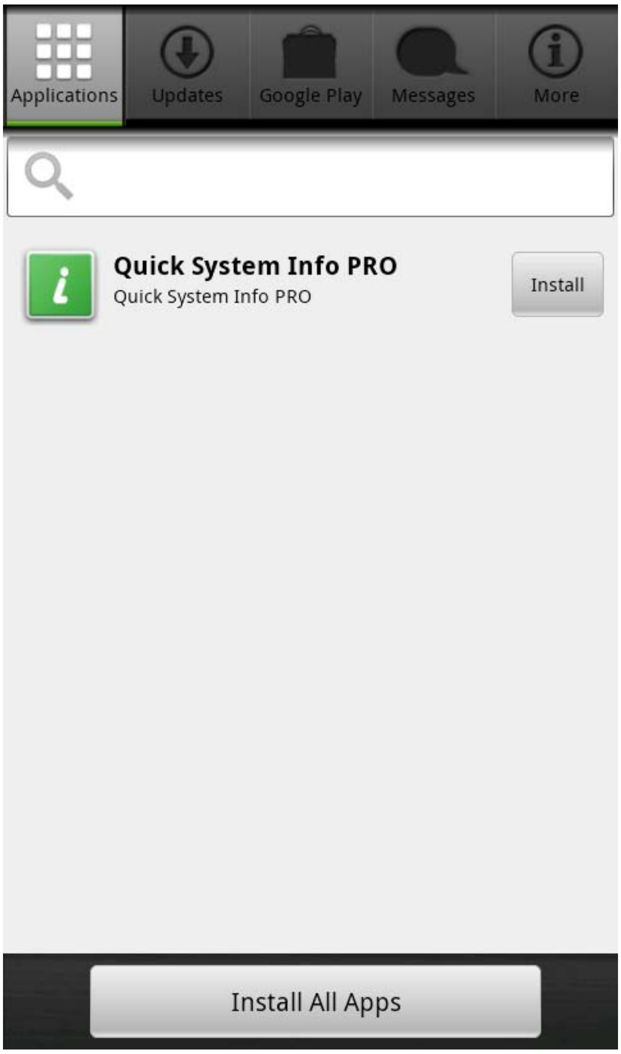
About

The About section displays version and copyright information for LANrev Apps.

LANrev Apps for Android

The installation of LANrev Apps for Android is described in “Enrolling mobile devices” on page 50.

LANrev Apps is divided into multiple sections, which are described below.



Quick System Info PRO
Quick System Info PRO

Applications

The Applications section lists all applications that have been made available to the mobile device and that are not yet installed on it. (For information on making apps available, see "Installing software on mobile devices" on page 197.)

Tapping one of the listed applications displays details about it. Tapping the **Install** button installs the application on the mobile device.

Tapping the **Install All Apps** button installs all displayed apps.

The filter field at the top of the applications screen allows you to enter a string to filter the displayed apps: Only apps that contain the specified string in their names are displayed.

Updates

The Updates section list all available updates for apps that have been installed on this device

Tapping an update displays details on it. Tapping the **Update** button installs the update on the mobile device.

Tapping the **Update All Apps** button in the main Updates section installs all available updates.

Google Play

The Google Play section is similar to the Applications section but, instead of enterprise applications, it lists apps from Google Play that you have made available.

Messages

The Messages section contains all messages that have been sent from LANrev to this mobile device.

Tapping the **Clear Selected** button removes the selected messages; tapping **Clear All** removes all messages.

Profiles

The Profiles section contains two tabs:

- The Installed tab lists all configuration profiles that are installed on the device.
  Tapping a profile lists its details and shows a **Remove** button. Tapping that button deletes the profile from the device.
- The Available tab lists all profiles that have been made available for optional installation on this device but aren’t yet installed. Clicking the **Install** button beside a profile installs it.

About

The About section displays version and copyright information for LANrev Apps.

LANrev Find

LANrev Find is an app that lets you display the location of geotracked devices on an iPad and send messages to tracked devices, lock them, or erase them.

Accessing the app requires an administrator account in LANrev Server with the **View Mobile Device Tracking Data** right, which in turn requires the **Manage Mobile Devices** right. To be able to perform the various available actions, these commands must be enabled for the administrator account:

- Sending messages: **Send Message to Mobile Device**
- Locking devices: **Issue Mobile Device Lock**
- Erasing devices: **Issue Mobile Device Remote Erase**

See “Administrator accounts” on page 72 for more information on account rights and command authorization.

LANrev Find can be downloaded from Apple’s App Store like any normal app. To make it easier for mobile users, you can specify LANrev Find as a recommended app, as described in “Distributing App Store or Google Play apps to mobile users” on page 206.

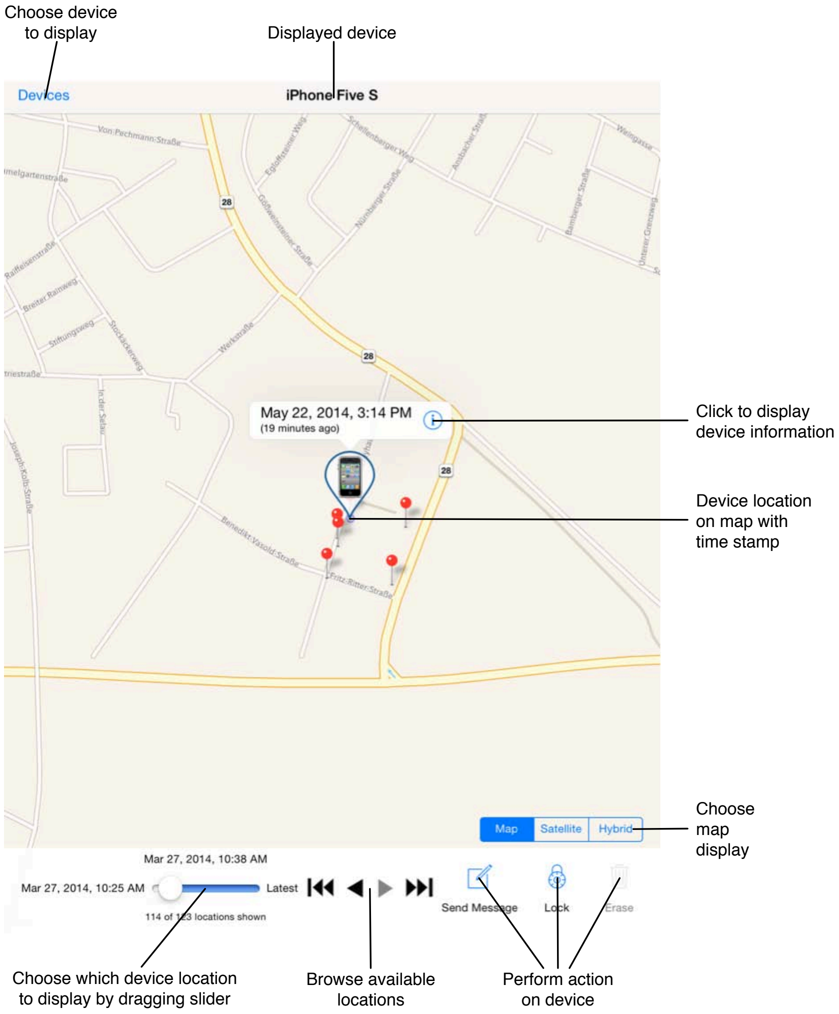
Start screen

The start screen requires you to log into your account on the LANrev server before you can use the app:

- **Address**: The public DNS name or IP address of the MDM server.
- **Port**: The port for external connections on the MDM server.
- **Name**: Your administrator account name on the LANrev server.
- **Password**. The password for your administrator account.

On subsequent launches, you need only specify your account name and password. (For information on changing the server address, see “Preferences” on page 956.)

Home screen



Choose device to display

Displayed device

Click to display device information

Device location on map with time stamp

Choose map display

Choose which device location to display by dragging slider

Browse available locations

Perform action on device

The home screen displays a map with the most recently selected device location. It allows you to:

- Select the device to display.
- Choose the location of the current device to display.
- Perform actions on the device.
- Display device information.
- Set map options.

You can zoom and pan the map as usual.

Preferences

The LANrev Find preferences are set in the Settings app:

- **Address**: The public DNS name or IP address of the MDM server.
- **Port**: The port for external connections on the MDM server.
- **Locations Per Device**: How many locations to download for a displayed device.

- **Logout After**: The interval of inactivity before you are automatically logged out of LANrev Find.
- **Log Out When Closed**: Whether LANrev Find requires you to log in when you leave the app and return to it.

LANrev Remote

LANrev Remote is an app that allows LANrev Admin to remotely view and control the screen of the mobile device.

LANrev Remote is a faceless background app that offers no user interface on the phone, except a dialog that is displayed when a connection request is made and in which you can accept or decline the request.

LANrev Remote requires Samsung SAFE to be available on the mobile device.

For the LANrev Remote application for desktop devices, see “LANrev Remote” on page 939.

LANrev Safe

LANrev Safe is the client app for mobile devices that lets administrators distribute media to mobile users:

- Media can be distributed selectively based on policies.
- Access to media can be restricted to specific periods of time.
- Media can be displayed in the app. For each document, administrators can allow or prohibit transfer to other apps on the mobile device.
- The app supports text, images, video, and audio documents.

LANrev Safe is available for iOS and Android:

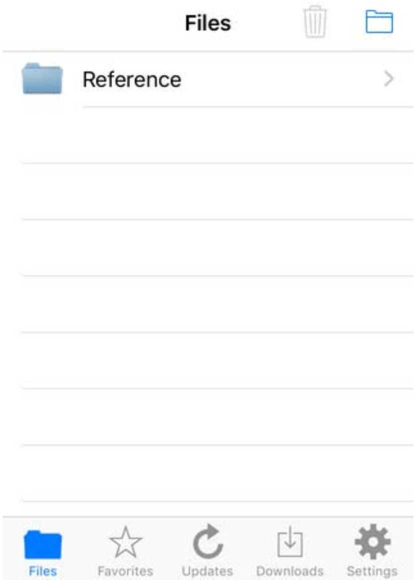
- “LANrev Safe for iOS” on page 957
- “LANrev Safe for Android” on page 964

LANrev Safe for iOS

LANrev Safe for iOS can be downloaded from Apple’s App Store like any normal app. To make it easier for mobile users, you can specify LANrev Safe as a recommended app, as described in “Distributing App Store or Google Play apps to mobile users” on page 206.

For the file types that LANrev Safe can display, see “Distributing media to mobile devices” on page 221.

Home screen

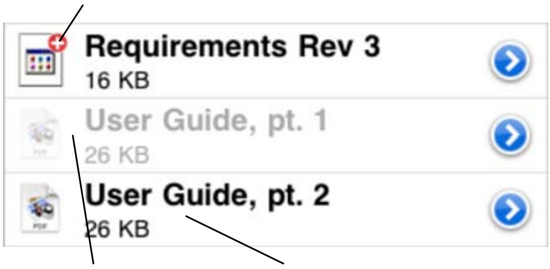


The home screen lists the available media, automatically sorted in folders according to the categories specified for the media files. Connected SharePoint libraries, if any, are indicated by a small SharePoint logo on the folder icon.

Tapping the trash can button lets you delete individual files. Tapping the download folder button downloads all files in the current folder and its subfolders that have not been downloaded yet.

Tapping a folder displays the files it contains; tapping a file displays it. See “Media display screen”, below, for details.

In the folders, files that you have already downloaded are displayed with solid icons; files that have not yet been downloaded have translucent icons. Files that have been downloaded but for which a newer version is available have a small plus sign overlaid over their icons:



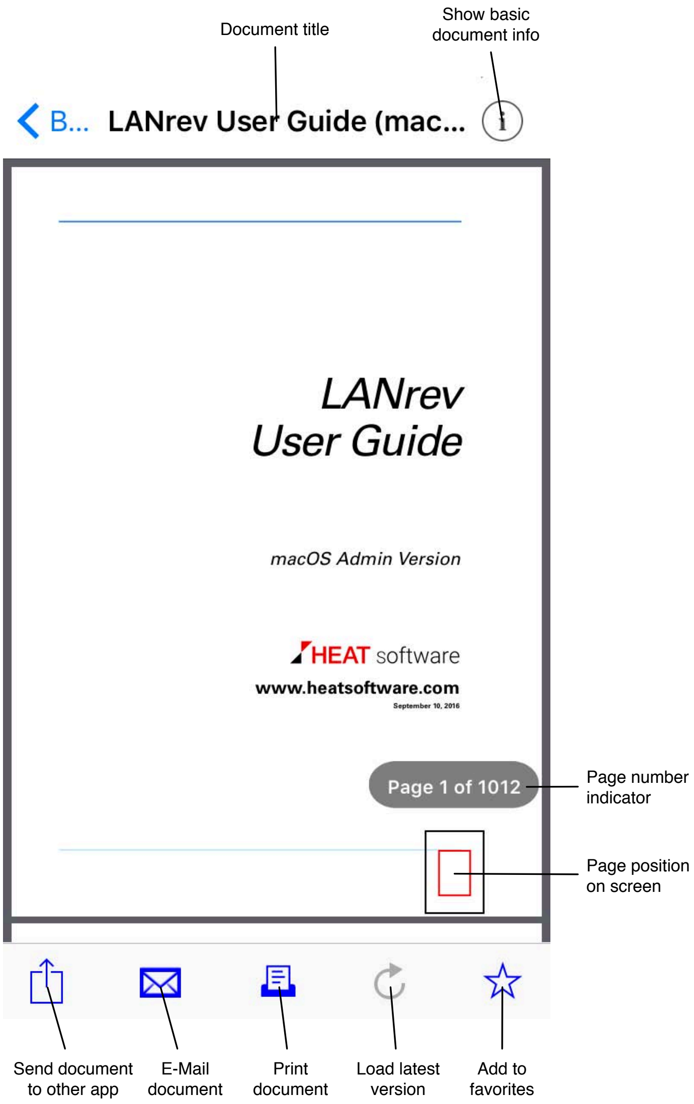
A newer version of this document is available.

This document has not been loaded yet.

This document has already been loaded.

The search field at the top of the home screen lets you enter part of the name of a file you are looking for. If a string is entered in this field, all files containing the string as part of their names are listed.

Media display screen



The media display screen shows the content of supported file types. For unsupported file types, only the basic document information is shown.

You can click the main area to hide or show the controls. The controls let you:

- Show the basic document information, such as type and size, as well as the description entered by the administrator.
- Send the document to another app that supports this document type. This button is available only if the document may leave LANrev Safe.
- E-mail the document using Mail. This button is available only if e-mailing was enabled for the document by the administrator.
- Print the document to a compatible printer. This button is available only if printing was enabled for the document by the administrator.

- Update the document to the latest version made available by the administrator. This button is available only if a newer version of the document is available.
- Show the document full-screen (only on iPads), hiding all controls.
- Mark the document as a favorite. If the star is hollow, the document is not yet a favorite and tapping the star makes it one. If the star is filled, the document is a favorite, and tapping the star removes that status.

Favorites screen

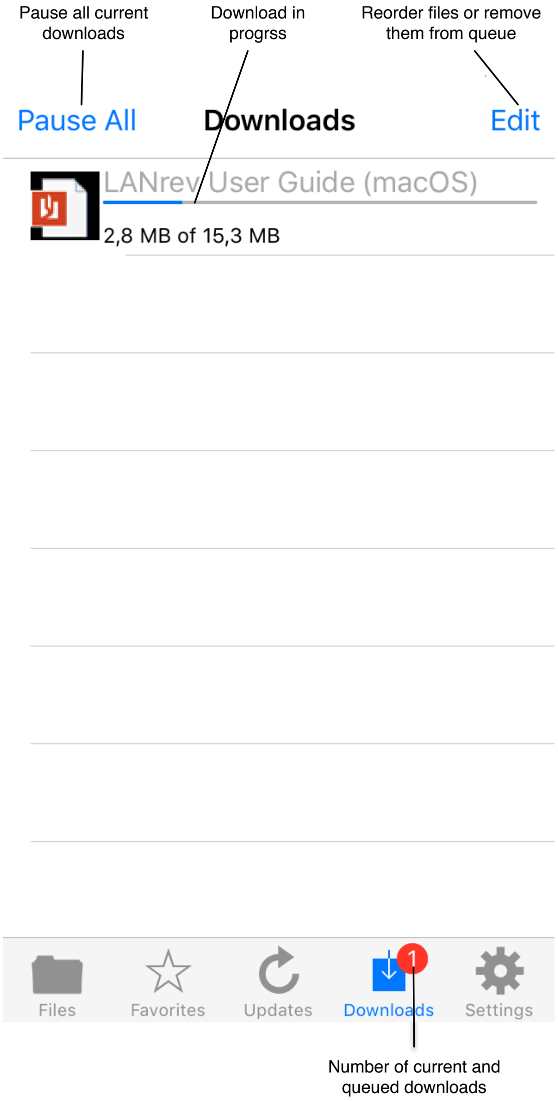
The **Favorites** screen lists all files you have marked as a favorite (see "Media display screen" above). It is otherwise like the home screen.

Updates screen

The **Updates** screen lists all files for which newer versions are available for download. The available buttons are similar to the **Files** screen.

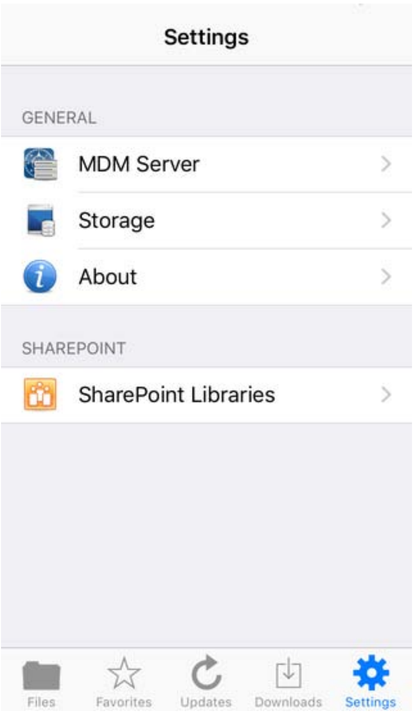
Downloads screen

The **Downloads** screen lists all downloads in progress:


Pause all current downloads
Download in progrss
Reorder files or remove them from queue
Pause All
Downloads
Edit
LANrev User Guide (macOS)
2,8 MB of 15,3 MB
1
Files
Favorites
Updates
Downloads
Settings
Number of current and queued downloads

Clicking the **Edit** button lets you reorder the downloads and remove individual ones.

Settings screen



Settings

GENERAL

MDM Server

Storage

About

SHAREPOINT

SharePoint Libraries

The **Settings** screen has several sections:

- Tapping **MDM Server** displays the MDM server to which you are connected.
  Tapping **Change** in this section lets you connect to a different MDM server.
- Tapping **Storage** displays the amount of storage used by LANrev Safe.
  Tapping **Remove Downloaded Files** in this section deletes all downloaded files from your device. You can, however, redownload all files as desired.
- Tapping **About** displays version and copyright information
- Tapping **SharePoint Libraries** displays the SharePoint Libraries to which this device is connected.
  Tapping **Add Library** displays a dialog through which you can connect to a new SharePoint library. It contains these fields:
  - **Name**: The name under which the library will appear on your device. You can choose this name as desired.
  - **Server URL**: The URL of the SharePoint library you want to access.
  - **Domain**: The domain of the SharePoint server.
  - **User**: Your username on the SharePoint server.
  - **Password**: Your password on the SharePoint server.

  Tapping an existing library opens a similar screen on which you can change the library’s settings or delete the library from LANrev Safe. Deleting a library removes from LANrev Safe all documents that have been downloaded from that library but does not affect documents that have been forwarded to other apps or the documents on the server.

LANrev Safe for Android

LANrev Safe for Android can be downloaded from the LANrev support website. To distribute it to your users, use LANrev, as described in "Installing software on mobile devices" on page 197.

For the file types that LANrev Safe can display, see "Distributing media to mobile devices" on page 221.

LANrev Safe has a toolbar, menu, and four screens:

- The toolbar is context-sensitive and let's you perform important actions in each context. For details, see "Toolbar" on page 964.
- The menu contains commands related to the current document as well as setting for the entire app. For details, see "Menu" on page 965; for details on the settings, see "Settings screen" on page 969.
- The Files screen is the central location for managing the documents in LANrev Safe, both downloaded to the mobile device and available for download on the server. For details, see "Files screen" on page 966.
- The Favorites screen is similar to the Files screen, but lists only favorites. (For information on marking favorites, see the description of the Favorites button in "Toolbar" on page 964.)
- The Update screen lists all updates that are available for files downloaded in LANrev Safe.
- The Download screen provides an overview of the downloads in progress. For details, see "Downloads screen" on page 967.

Toolbar

The toolbar is available in all screens; the available buttons vary between screens:

🔍	Displays the search field, in which you can enter part of the name of a file you are looking for. If a string is entered in this field, all files containing the string as part of their names are listed.
⬇	Download all documents in the current folder.
⏸	Pause all downloads that are in progress. While downloads are paused, no automatic downloads are started.
▶	Resume downloading.
⤢	Displays the current document in full-screen view. Tap the Back button to return to the normal view.

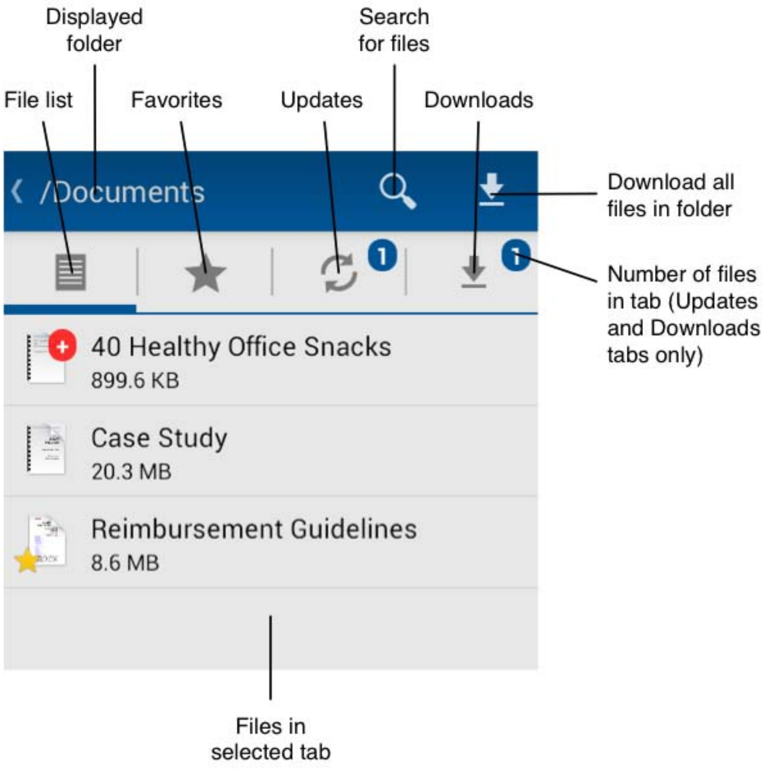
🔄	Download the update for this document.
ⓘ	Displays document metadata.
👁	Displays document content.
☆	Toggles the “favorites” status of the selected document. If the star is hollow, the document is not yet a favorite and tapping the star makes it one. If the star is filled, the document is a favorite, and tapping the star removes that status.

Menu

Tapping the menu button opens the app’s menu:

- **Open with**: Send the document to another app that supports this document type. This button is available only if the document may leave LANrev Safe.
- **Share**: Open Android’s share sheet. This button is available only if e-mailing was enabled for the document by the administrator.
- **Delete**: Delete the document from LANrev Safe. You can redownload deleted documents.
- **Settings**: Go to the Settings screen. For details, see “Settings screen” on page 969.

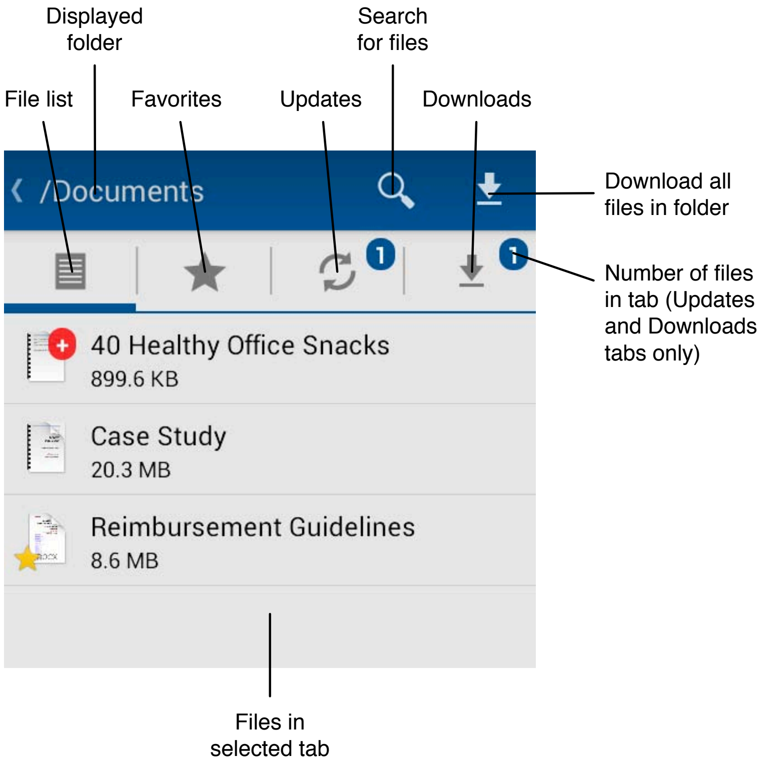
Files screen



40 Healthy Office Snacks
899.6 KB

Case Study
20.3 MB

Reimbursement Guidelines
8.6 MB



40 Healthy Office Snacks
899.6 KB

Case Study
20.3 MB

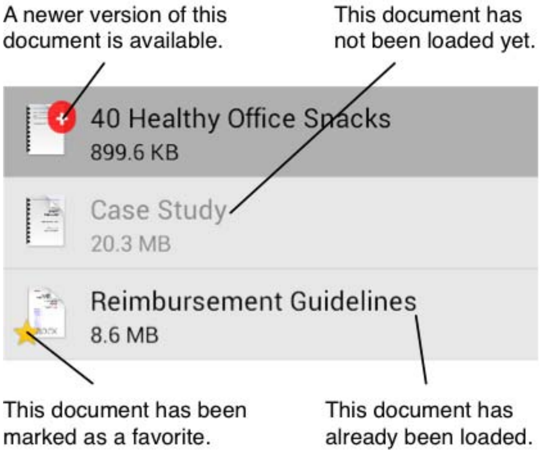
Reimbursement Guidelines
8.6 MB

The Files screen lists the available media, automatically sorted into folders according to the categories specified for the media files.

Connected SharePoint libraries, if any, are indicated by a small SharePoint logo on the folder icon.

Tapping a folder displays the files it contains; tapping a file displays it.

In the folders, files that you have already downloaded are displayed with solid icons; files that have not yet been downloaded have translucent icons and gray text. Files that have been downloaded but for which a newer version is available have a small plus sign overlaid over their icons:



40 Healthy Office Snacks
899.6 KB

Case Study
20.3 MB

Reimbursement Guidelines
8.6 MB

A newer version of this document is available.

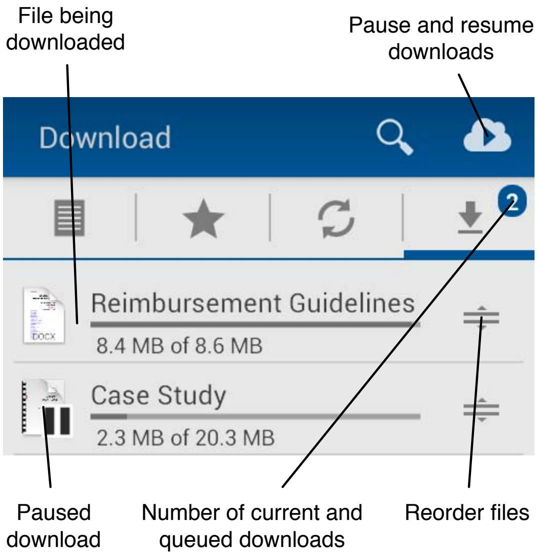
This document has not been loaded yet.

This document has been marked as a favorite.

This document has already been loaded.

Downloads screen

The **Downloads** screen lists all downloads in progress:



Download

Reimbursement Guidelines
8.4 MB of 8.6 MB

Case Study
2.3 MB of 20.3 MB

File being downloaded

Pause and resume downloads

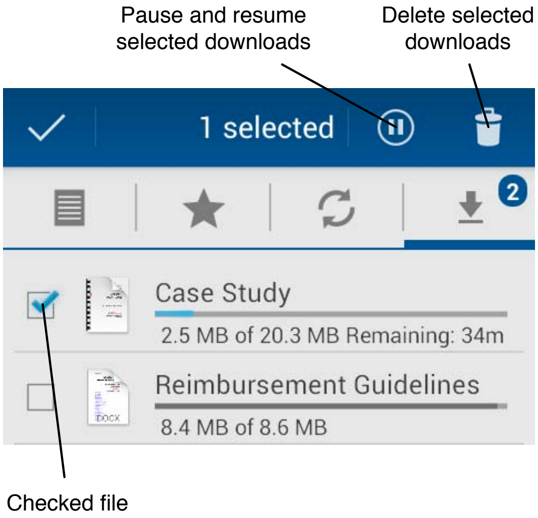
Paused download

Number of current and queued downloads

Reorder files

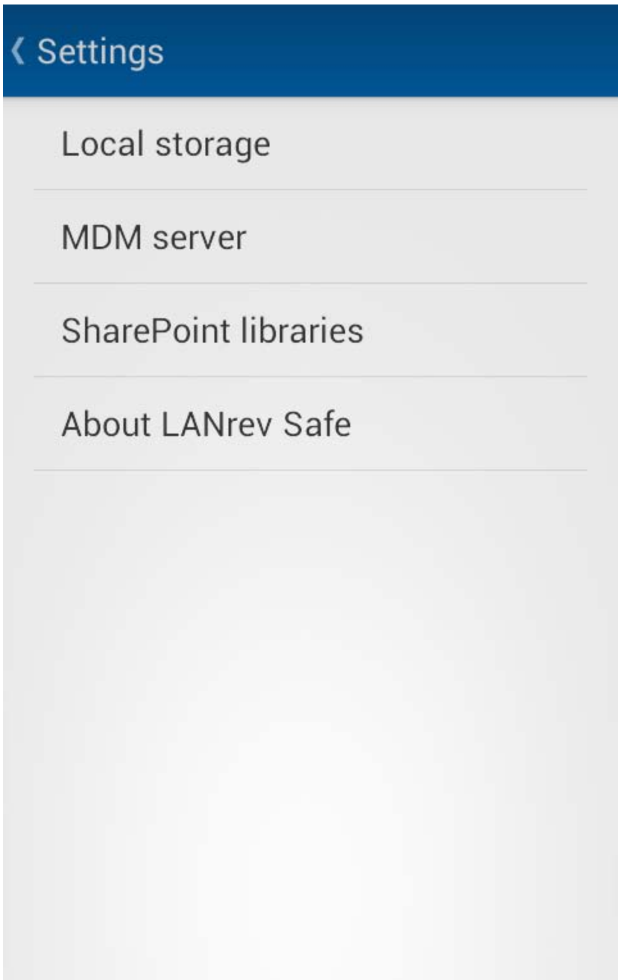
If there are multiple downloads, you can reorder them by dragging on the reorder icons at the right.

Long-pressing a file being downloaded displays checkboxes and additional controls:


Pause and resume selected downloads
Delete selected downloads
1 selected
2
Case Study
2.5 MB of 20.3 MB Remaining: 34m
Reimbursement Guidelines
DOCX
8.4 MB of 8.6 MB
Checked file

Settings screen

The Settings screen is available on the app menu, which is opened via the menu button.



The **Settings** screen lets you access:

- **Local storage**: This screen displays how much storage the media downloaded in LANrev Safe requires on the device and lets the user free up space.
- **MDM server**: Displays the MDM server to which the device is connected and lets the user specify a different server.
- **SharePoint libraries**: Lists the libraries to which the device is connected and lets the user connect to additional libraries.
- **About LANrev Safe**: Displays version and copyright information.

Chapter 30 LANrev Agent

LANrev Agent is the client software of LANrev that is installed on every administered computer. It works mostly behind the scenes, acting on instructions received from the LANrev server, but has some user-accessible elements.

LANrev Agent control panel

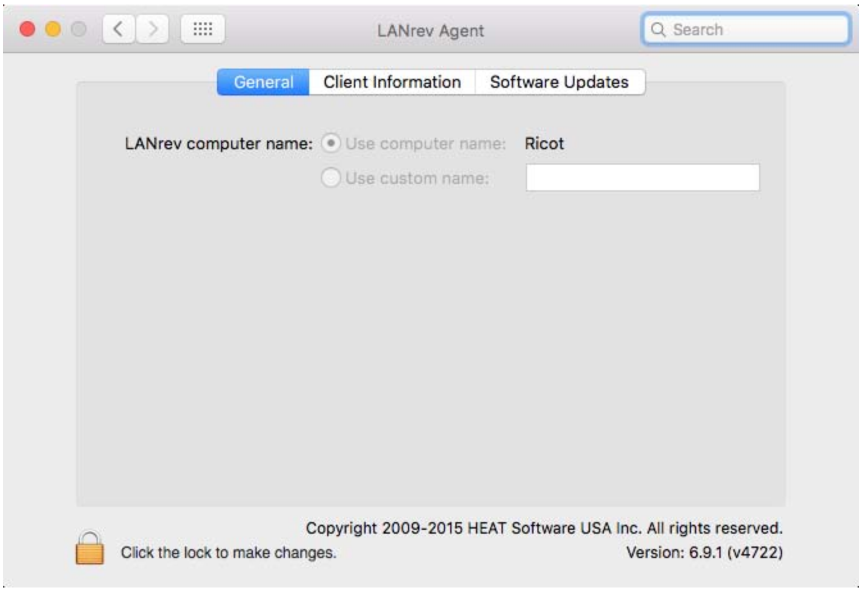
The LANrev Agent control panel is located in the **System Preferences** on macOS clients and the **Control Panel** on Windows systems.

It has three panes:

- **General**
- **Client Information**
- **Software Updates**

General

The General pane lets local users set the name under which their computer appears in LANrev:



LANrev computer name: ● Use computer name: Ricot

○ Use custom name:

Copyright 2009-2015 HEAT Software USA Inc. All rights reserved.

Click the lock to make changes.

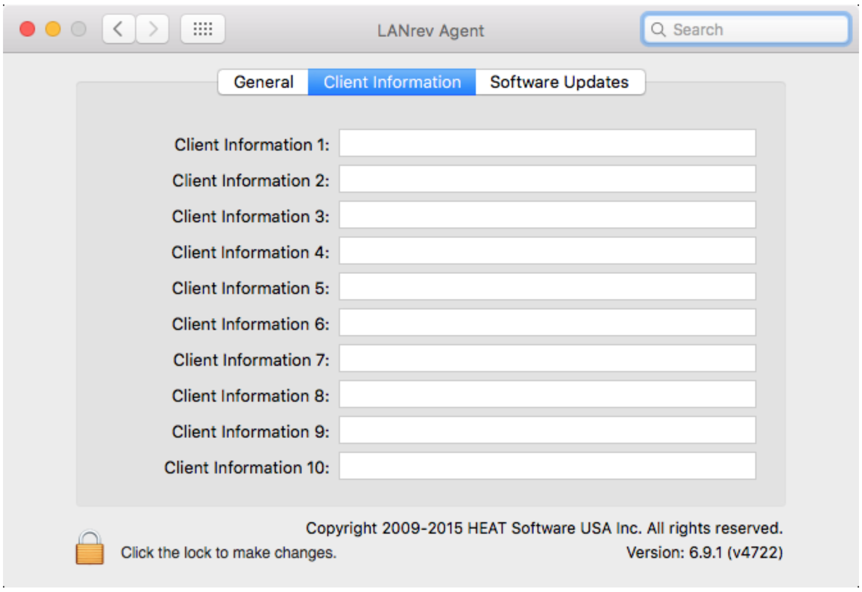
Version: 6.9.1 (v4722)

The pane contains this element:

- **LANrev Computer Name**: The name that is displayed for the computer in the LANrev system. You can choose to use the name specified for the computer in the local operating system or you can specify a custom name that is only used by LANrev. *Note: This setting is available to administrators in the* **Agent Settings** *dialog's* **General** *pane.*

Client Information

The **Client Information** pane lets local users specify information in up to ten fields:



Client Information 1:
Client Information 2:
Client Information 3:
Client Information 4:
Client Information 5:
Client Information 6:
Client Information 7:
Client Information 8:
Client Information 9:
Client Information 10:

Copyright 2009-2015 HEAT Software USA Inc. All rights reserved.

Click the lock to make changes.

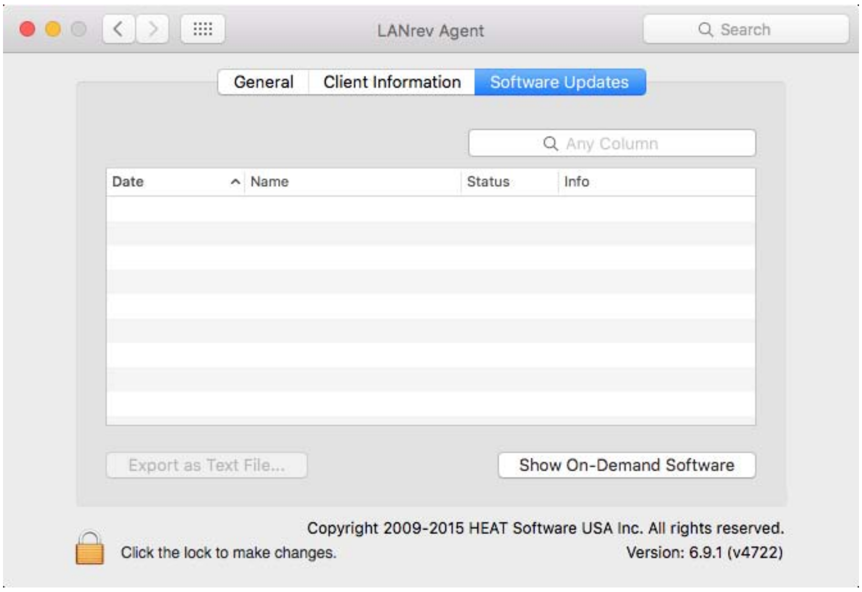
Version: 6.9.1 (v4722)

The pane contains these elements:

- **Client Information n**: All ten fields can contain custom text information that the user by default can freely edit.
  The names of the fields may be set on the server through the **Client Info Titles** pane of LANrev Admin's **Server Settings** dialog. If a field is renamed, its label in the LANrev Agent control panel changes accordingly.
  The fields can be locked against changes by local users in the **Agent Settings** dialog's **Client Information** pane. In that pane, administrators can also edit the fields' contents.

Software Updates

The **Software Updates** pane lists all software updates that have been installed on the computer using LANrev's software distribution and patch management systems and allows local users to check for new updates:



Copyright 2009-2015 HEAT Software USA Inc. All rights reserved.

Click the lock to make changes.

Version: 6.9.1 (v4722)

The pane contains these elements:

- Filter field: When text is entered into this field, the display is restricted to only those software installations whose descriptions contain that string.
  Optionally, the filtering can be restricted to a single column, in which case only software installations containing the string in the specified column are displayed.
- Table: The table lists all software installations that have been made on this computer by means of LANrev’s software distribution and patch management systems.
  In addition to successful software package or patch installations, the table also lists failed and refused installations as well as deferred installations and installations in progress.
  Columns can be rearranged by dragging their titles. Clicking a title sorts the table by that column; if the title of the current sorting column is clicked, the sort order is reversed.
- **Export as Text File**: Clicking this button allows the local user to export the table’s currently displayed contents as a tab-delimited text file.
- **Show On-Demand Software**: Clicking this button causes the Agent to contact its designated software distribution server for any new software packages that are marked as on-demand downloads. It displays all found packages in the **LANrev Software Distribution** window.
- **Get New Software**: If you hold down the Option key, the **Show On-Demand Software** button changes to **Get New Software**.
  Clicking this button causes the Agent to contact its designated software distribution server for new software packages,

downloading any found packages according to the packages' settings.

Note: This is the same kind of check as that invoked by the **Run Software Distribution Check** *command.*

Index