
Getting Started with LANrev MDM

Windows Version

 **HEAT** software

www.heatsoftware.com

October 23, 2016

Getting Started with LANrev MDM 7.0 - Documentation Release 5

This document, as well as the software described in it, is confidential and contains proprietary information protected by non-disclosure and license agreements. No part of this document may be reproduced in any form or disclosed to any party without the express written consent of HEAT Software USA Inc.

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.

© 2009–2016 FrontRange Solutions Inc. All rights reserved.

This product is protected by US patents 7 818 557, 8 234 359, 9 009 857, and 9 081 639. Additional patents are pending.

Getting Started with LANrev MDM

Introduction

Thank you for choosing LANrev! The LANrev suite is a uniquely seamless, multiplatform client management solution for managing all of your iOS and Android devices in a single unified console on a Windows or macOS computer, combining sophisticated profile management with inventory and tracking functions. You'll find that there are often multiple ways to accomplish the same task within LANrev so it's up to you to decide which one fits into your workflows and works best in your computing environment.

This guide is by no means comprehensive but is meant to help you quickly get up and running with LANrev in the shortest possible amount of time. It does not explain nor show you how to use some of the more advanced and subtle features of the suite. For more information or help with LANrev, the following resources are available:

- The built-in context sensitive help. This is accessible via the **Help** menu.
- The complete LANrev user guides. The macOS user guide PDF can be found at the root level of the distribution DMG disk image. The Windows user guide can be accessed from the LANrev program group in the Windows Start menu.
- The LANrev support forums at community.heatsoftware.com/community/products/heat-unified-endpoint-management.
- The LANrev tech notes at <http://support.heatsoftware.com>.
- LANrev technical support at www.heatsoftware.com/support.

Minimum system requirements

Server:

- macOS 10.6 or up
- Windows Vista or Server 2003 or above
On Windows Server 2016, PowerShell 2.0 or above is required.

Admin:

- macOS 10.10 or up
- Windows Vista or Server 2003 or above

Mobile client:

- iOS 4.0 and up
- Android 2.2 and up

Preparing for MDM support

1. Get an SSL/TLS certificate for the computer on which you will install the MDM server. It must either be a wildcard certificate for the domain or a certificate specifically for the computer.

If the certificate is not signed by a root certification authority (CA), you also need the signer certificate of the CA which has signed your certificate.

2. Set up your firewall to allow connections from the MDM server to:
 - gateway.push.apple.com on port 2195 (if you want to manage iOS devices)
 - android.apis.google.com on port 443 (if you want to manage Android devices)

Installing LANrev Server

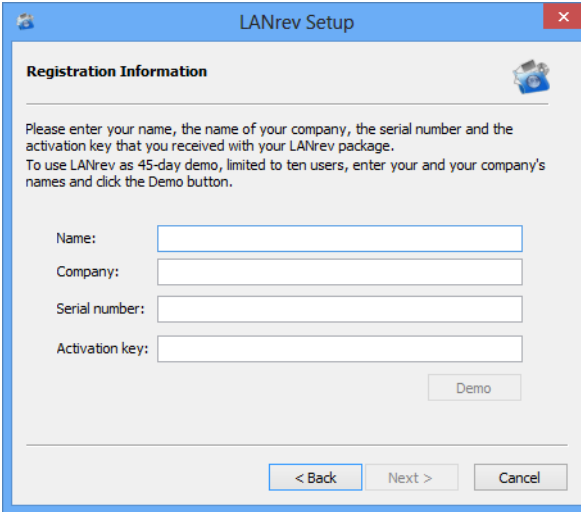
Installing LANrev Server is a very simple process. On a Mac, open LANrev Server.pkg; on a PC, open setup.exe for LANrev Server, accept the license agreement, and click **Next** or **Continue** through the rest of the prompts to complete the installation.

Installing the LANrev admin console and activating LANrev

Upon first launch of the LANrev admin console you will be required to register your LANrev installation and create a default superadministrator account. Store this information in a safe place. You should create a separate admin account for everyday use instead of using the default superadministrator account.

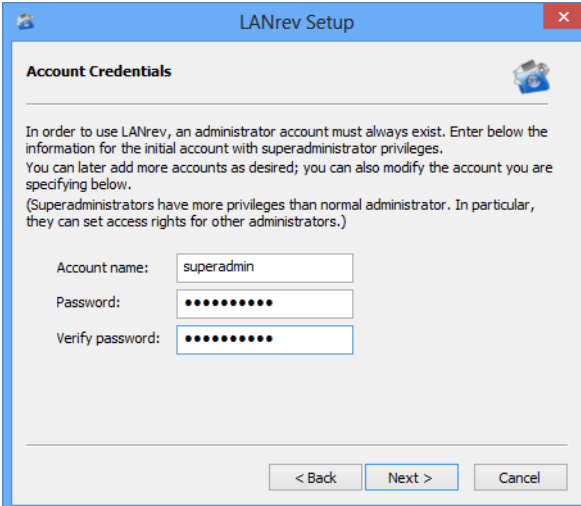
1. Launch the LANrev Admin Setup.exe file and click **Next** through the rest of the prompts to complete the installation.
2. Launch the admin console. When prompted, enter the IP address or DNS name of your LANrev server (do not enter "localhost", "127.0.0.1", or ":::1", even if the admin console is installed on the same computer as the server), leave the **Name** and **Password** fields blank, and click **Login**.

3. Click **Next** or **Continue** through the rest of the prompts until you reach the registration screen.



The screenshot shows a dialog box titled "LANrev Setup" with a "Registration Information" section. The text inside reads: "Please enter your name, the name of your company, the serial number and the activation key that you received with your LANrev package. To use LANrev as 45-day demo, limited to ten users, enter your and your company's names and click the Demo button." There are four input fields: "Name:", "Company:", "Serial number:", and "Activation key:". A "Demo" button is located below the "Activation key" field. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

4. At the registration dialog, enter your registration information. If you do not have any, complete the **Name** and **Company** fields and click the **Demo** button for a 45-day 10-seat evaluation. Then click **Next** or **Continue** until you reach the administrator setup screen.



The screenshot shows a dialog box titled "LANrev Setup" with an "Account Credentials" section. The text inside reads: "In order to use LANrev, an administrator account must always exist. Enter below the information for the initial account with superadministrator privileges. You can later add more accounts as desired; you can also modify the account you are specifying below. (Superadministrators have more privileges than normal administrator. In particular, they can set access rights for other administrators.)" There are three input fields: "Account name:" with the text "superadmin", "Password:" with masked characters, and "Verify password:" with masked characters. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

5. Enter the username and password you want to use for the default superadministrator account. Click **Continue** and then **Setup**.

Logging into the admin console for the first time

Launch the LANrev Admin application. At the authentication dialog, enter the IP address or DNS name of your server and the credentials for the default superadministrator account you created previously.

Exporting an SSL certificate for the server

Setting up a LANrev installation requires you to specify an SSL certificate in several places to allow the system to authenticate the server. Export this certificate now:

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

The **Server Center** window is displayed.

2. In the sidebar at the left of the window, click **Server > Server Settings**.

The server settings are displayed in the main part of the window.

3. Click the **Save Certificate** button at the bottom right of the window.

A standard Save dialog is displayed.

4. Save the certificate in a convenient location.

You can name it as desired, as long as you keep the “.pem” filename extension.

Installing the MDM server

1. Run the MDM server installer package on the computer where you want to install it. (This may be the computer on which LANrev Server is installed or a different one.)

When you are prompted for the website SSL certificate, specify the one you got from the CA (see “Installing the LANrev admin console and activating LANrev” on page 2).

When you are prompted for the LANrev Server certificate, specify the one you exported from the server (see “Exporting an SSL certificate for the server” on page 4).

When you are prompted for a DNS address, make sure to use the fully qualified form, not just the local part (e.g. “mdm.mycompany.com” instead of just “mdm”).

2. On Windows, you are done. On macOS, you are not prompted for the certificates during the installation. Instead, rename the website certificate “lighttpd.pem” and the LANrev Server certificate “TrustedCertificates.pem” and copy both to /etc/lighttpd/certs.
3. If the LANrev Server 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 by executing the command

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

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

4. 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 AMServerHostname key the IP address or DNS name of the LANrev server.
5. On the computer on which the MDM server is installed, start the MDM server by running the Start_MDM_Server.command shell script provided on the LANrev installation disk.

Importing the SSL key into the certificate

If you have received an SSL certificate that does not contain the SSL private key (e.g., 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, e.g., 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 LANrev server preferences

These settings affect the server and are stored on the server itself. Of particular importance are the database maintenance and backup settings for disaster recovery.

1. Choose **Window > Server Center**.
2. Click **Server Setup** in the category bar at the top of the **Server Center** window and click **Server > Server Settings** in the left-hand sidebar.

3. In the **General** tab enable the database maintenance and backup.

The screenshot shows the 'General' tab of the LANrev server preferences. The 'Database backup' section is highlighted with a red box and contains the following settings:

- Backup database every 1 days at 11:45 PM [Run Now]
- keep 14 backups

The 'Database maintenance' section is also highlighted with a red box and contains the following settings:

- Run database maintenance every 1 days at 11:00 PM [Run Now]

Below these sections, there are checkboxes for 'Send e-mail' and 'Send SMS', both of which are checked. The 'Server' section above contains various configuration options like 'Offline threshold', 'Maximum number of entries in license history', and 'Connection timeout'.

Consult the LANrev Disaster Recovery Guide for best practices on configuring these settings. We recommend that you run the database maintenance every day, back up the database every three days, and keep seven backups. These values can be adjusted depending on the amount of free disk space available and the size of your LANrev databases.

4. If you plan on basing your LANrev admin accounts on Active Directory (AD) user accounts, switch to the **Active Directory** tab and enter the name of any user groups from which you want LANrev to be able to pull user accounts for this purpose. Your

LANrev server must be bound for AD for this to work. Click the plus sign and enter just the name of the desired AD user group itself.

The screenshot shows the 'Active Directory' tab in the LANrev server preferences. The window has several tabs: General, Client Info Titles, License Monitoring, ODBC Export, Active Directory (selected), MDM, Notification, FOG, and NAC. The main content area is divided into two sections. The first section is titled 'Active Directory groups to be displayed in the Server Center's Administration section:' and contains a list box with the entry 'Administrators'. Below this list box are three buttons: a plus sign (+), a minus sign (-), and an 'Edit' button. The second section is titled 'Active Directory domain credentials for reading user info:' and contains a table with two columns: 'Domain' and 'Username'. The table is currently empty. Below the table are three buttons: a plus sign (+), a minus sign (-), and an 'Edit' button.

5. In the **MDM** tab, enter:

- A descriptive name for the deployment profile in the **Profile name** field
- A unique identifier for the profile in the **Profile identifier** field
- The name of your organization in the **Organization** field
- A text explaining the profile's purpose to mobile users in the **Description** field

If you want to manage iOS devices, click the upper **Configure** button and create or select an Apple push certificate.

If you want to manage Windows Phone devices, fill in the Microsoft Exchange Server information as well.

The screenshot shows the 'MDM' configuration window with the following fields and sections:

- Profile name [required]:** MDM Server
- Profile identifier [required]:** com.mycompany.mdm
- Organization [optional]:** MyCompany, Inc.
- Description [required]:** Manages your mobile devices
- MDM server [required]:** mdm.mycompany.com, Port: 443
- Microsoft Exchange:** 2010, Exchange: exchange.mycompany.com, Username: PPS\Administrator, Password: *****
- Access rights:** Query devices for (General settings, Security settings, Network settings, Restrictions), 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, Update device information checked
- Apple VPP licensing accounts:** 3 accounts configured
- Apple device enrollment program accounts:** One account configured
- Samsung KNOX accounts:** 3 KNOX accounts configured

The screenshot shows the 'MDM' configuration window with the following fields and sections:

- Profile name (required):** MDM Server
- Profile Identifier (required):** com.mycompany.mdm
- Organization (optional):** MyCompany, Inc.
- Description (required):** Manages your mobile devices
- MDM server (required):** mdm.mycompany.com, Port: 443
- Microsoft Exchange Server:** 2010, Exchange server: exchange.mycompany.com, Username: PPS\Administrator, Password: *****
- Access rights:** Query devices (General settings, Security settings, Network settings, Restrictions), Add and remove (Configuration profiles, Provisioning profiles, Applications), Security (Change device password, Erase device, Change settings)
- Certificates:** MDM (required): Valid until 3/10/2016 9:32:04 PM; LANrev Apps push: Valid until 6/29/2016 12:50:56 PM; LANrev Safe push: Valid until 11/4/2015 9:33:40 PM; MDM profile signing: Not configured
- Device contact interval:** 24 hours, Update device information checked
- Apple VPP licensing accounts:** 3 accounts configured
- Apple device enrollment program accounts:** One account configured
- Samsung KNOX accounts:** 3 KNOX accounts configured

Setting up an admin hierarchy

Sufficient care should be taken in determining who on your IT staff has access to which computers and what they can do on them. LANrev's granular role-based administration model allows you to do just that. The following instructions will show you how to add a regular superadministrator account for yourself for everyday usage.

1. Choose **Window > Server Center**.
2. Click **Administrators** in the category bar at the top of the **Server Center** window and click **Administration > Administrators** in the left-hand sidebar.
3. Right-click **Administrators** and choose **Administrator Setup > New Administrator** from the context menu.
4. Fill in the **Name**, **Password**, and **Verify** fields, enable the **Superadministrator** and **Can manage all computers** options, and click **OK**.
5. To create a LANrev admin account based on an Active Directory account, click **Administration > Active Directory** in the left-hand sidebar and then drag an Active Directory user account from the right-hand pane onto the **Administrators** entry in the left-hand sidebar.
6. Exit the LANrev admin console and log back in using your new credentials.

Enrolling mobile devices

Any mobile devices you want to manage through LANrev must first be enrolled.

NOTE The enrollment process described below requires an Active Directory or (if LANrev Server is installed on macOS) Open Directory server on which the users of all mobile devices that you want to enroll have an account. An alternate process without this requirement is described in the LANrev user guide. Certain Apple devices can also be enrolled through Apple's servers, which is also described in the user guide.

Send an e-mail to all mobile devices that are to be managed. Include in the e-mail the enrollment URL (see below) and instruct the users to click on it to start the enrollment process.

The enrollment URL is:
`https://<server address>/Profile/enrollment.mdm`
where <server address> is the DNS name of your MDM server, e.g.,
`mdm.mycompany.com`.

When users click on the URL, they will need to enter their Active Directory or Open Directory credentials, including the Active Directory domain if applicable.

For iOS and Windows phone users, the rest of the process is automatic. Android users need to manually launch the LANrev Apps.apk file, which is downloaded in the process. Android users also need to allow the installation of content from sources other than the Android Market.

Once a device has been enrolled in this manner, you can manage it through LANrev.

Creating a custom inventory report

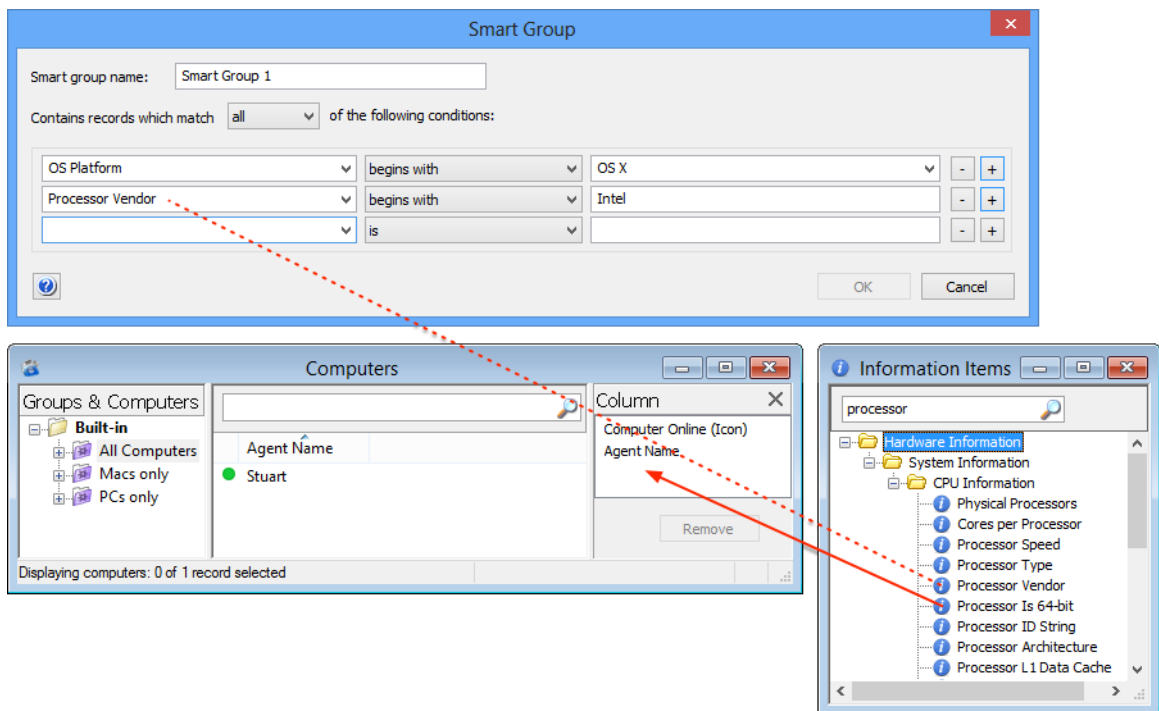
Creating an inventory report involves two basic steps:

1. Narrowing down the field to just the devices you want to include in the report
2. Deciding which inventory items you want to display about them

To create a new standard group in the **Mobile Devices** window select all the devices you want to include, right-click and choose **New Policy with Selected Devices** from the context menu.

To create a smart group, right-click anywhere in the left-hand sidebar of the **Mobile Devices** window and choose **New Smart Group: Mobile Devices** from the context menu. Enter the name of any information items you want to use for selection criteria on the left, choose a comparison operator in the middle, and enter the comparison value on the right. You can get a list of available information items by choosing **Window > Information Items**. You can start typing the name of the desired information item and LANrev will try to autocomplete the name for you. Click the pull-down for the left-hand field before typing to get a complete list of all information items or after entering a few letters to

get a partial list of just information items that begin with those letters. To add more selection criteria, click the plus button.



To change which information items are displayed in the custom inventory report, right-click the column header area and choose **Configure Columns** from the context menu. Information items can be added by copying or dragging them from the **Information Items** window into the columns drawer. To remove information items select them and click the **Remove** button. To search for an information item in the **Information Items** window enter a part of its name in the search field at the top and press the Enter key.