LANrev 7.3.2 Release Notes

Welcome to LANrev!

These release notes contain information on changes from earlier versions of LANrev and late-breaking information that could not be included in the manual.

Updating from earlier versions

Updating from earlier versions of LANrev varies slightly, depending on the version from which you update.

IMPORTANT Never mix different versions of LANrev Server and LANrev Admin; e.g., do not use LANrev Admin 7.3.2 with LANrev Server 7.3.1 or vice versa. Also, make sure that on all computers with LANrev Server, LANrev Agent is updated to the same version as the server.

Updating from LANrev 7.2.1 or earlier

LANrev 7.3 and later versions, standardize on "macOS" as the name of the operating system of Macintosh computers, reflecting the official renaming of the OS by Apple. This also applies to the content reported in some information items, such as "OS Platform".

If you have any smart group definitions that test for the name of the operating system and expect "OS X" to occur in the reported string, you need to update those definitions.

This issue is similar to the change to "OS X" described below in "Updating from Absolute Manage 6.5 or earlier".

Updating from Absolute Manage 6.9.2 or earlier

To improve compatibility with a wider range of mail servers, the default SMTP port has been changed. This change has an effect only when you have left empty the **SMTP server port** field in the **Notification** tab of the server settings.

In earlier releases, port 465 was used for secure connections when the field was left empty. Beginning with LANrev 6.9.3, port 587 is used. If you have not previously specified a port and your SMTP server cannot communicate over port 587, you must manually specify port 465 after updating to LANrev 6.9.3 or up.

Updating from Absolute Manage 6.5 or earlier

Absolute Manage 6.6 and later versions, including LANrev 6.9.2 and up, standardize on "OS X" as the name of the operating system of Macintosh computers. This also applies to the content reported in some information items, such as "OS Platform".

If you have any smart group definitions that test for the name of the operating system and expect "Mac" to occur in the reported string, you need to update those definitions.

Known issues in LANrev 7.3.2

macOS firewall will prompt for confirmation

On each macOS computers on which the built-in firewall is active, upgrading to LANrev Agent, Admin, or Server 7.3 or later will trigger an alert requesting permission for LANrev to accept incoming connections.

Click **Allow** in each such alert. Clicking **Deny** will prevent LANrev from working properly.

This issue does not occur when LANrev is installed on a computer for the first time, but may occur on macOS computers on which LANrev or Absolute Manage had been installed earlier, even if it has been uninstalled in the meantime.

Upgrading LANrev 7.3 to a later version will not trigger this issue.

Reinstalling to boot volumes not possible on macOS 10.11 and up

Because of changes to Apple's security architecture, the **Reinstall macOS Computer** command cannot be applied to boot volumes of client computers running macOS 10.11 and up.

The command can be applied to other volumes on those client computers, as well as to any volumes of client computers running earlier versions of macOS.

Enrollment profiles must not require authentication for OS X 10.9

Enrolling OS X 10.9 (Mavericks) computers into Apple's device enrollment program (ADEP) does not work if the device enrollment profile used specifies that authorization is required.

If you are using LANrev to enroll OS X 10.9 computers, make sure that the **Require authentication as part of the enrollment** option is unchecked in the enrollment profile you assign.

Support for new iOS 8 features

In relation to the support of new features introduced with iOS 8, there are some known issues caused by factors outside our control. We are working closely with the relevant external parties to resolve these issues.

These issues and the progress being made in correcting them are detailed on the support site in article 21047.

Smart policies based on the last contact of mobile devices

Smart policies for mobile devices that select devices based on the "Mobile Device Last Contact" information item do not behave as expected and should not be used.

This issue does not affect smart policies set up with other information items. It also does not affect smart groups that are based on "Mobile Device Last Contact".

Installing OS X and directory services

Reinstalling some versions of OS X may have limitations regarding directory services:

- On computers that were running Mac OS X 10.6.8 or older before the reinstallation, Open Directory settings are not retained.
  To correct this issue, run the dsconfigldap tool locally on the client computer.
  This issue does not affect computers who were already running Mac OS X 10.7 or higher before the reinstallation.
- Client computers reinstalled with Mac OS X 10.7 (irrespective of which operating system they were running before the reinstallation) will be unable to automatically connect to Active Directory.
  To correct this issue, run the dsconfigad tool locally on the client computer.

You can automate running dsconfigldap and dsconfigad, respectively, by executing an appropriate shell script remotely from LANrev Admin using the **Execute Script** command.

Active Directory Support by LANrev Admin for macOS

When LANrev Admin is running on macOS, the **Active Directory** category in the **Deployment Center** window's sidebar displays only the first 1000 computers.

This issue is caused by a limitation in macOS: Apples Active Directory support does not currently include paged LDAP calls.

Until Apple fixes this, we recommend using custom zones for deploying agents from macOS administrator computers if your network contains more than 1000 computers.

NOTE It is not possible to deploy macOS agents from Windows administrator computers.

Changes in LANrev 7.3.2

- LANrev MDM is supported on Windows Server 2016. Note, however, that the HTTP/2 protocol must be disabled on the server.
- The serial numbers of MDM push certificates are displayed in the **Push Services Certificates** dialog.
- LANrev Remote displays the application name in the Windows Task Manager.
- LANrev Remote uses OpenSSL 1.1.0.
- The late 2016 MacBook Pro models are correctly recognized.
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.3.1

- Improvements in classroom management:
  - Single persons can be assigned to classes (in addition to groups of persons).
  - Classroom data can be exported as a JSON file.
  - The new first name, middle initials, and last name fields of the Apple School Manager are supported.
  - Group definitions can be imported and exported.
  - Groups can be copied and pasted, except for built-in groups. (This also applies to groups in other windows.)
- When the installation of a configuration profile fails, more detailed information is now displayed in the **Command History** window.
- The **Schedule OS Update** command has been renamed **Install iOS Update**.
- New information items:
  - **Server Center** > **Administration** > **Administrators** > **Modify Desktop Actions**
  - **Server Center** > **Actions** (new category)
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Home Button Setup**
- A variable for the current user account is available in commands for administered computers.
- LANrev supports Windows Server 2016 (except LANrev MDM Server).
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.3

- LANrev Admin for macOS now requires macOS 10.10 or up.
- Actions are now available for computers.
- The Lost mode on mobile devices can be set through an action.
- Information variables can now be used in commands, actions, and configuration profiles for computers.

- Information variables are supported in additional commands for mobile devices.
- Custom information items for computers can have variable names, which means that they can be used as information variables (see above).
- Enrollment profiles for iOS devices can include skipping the Home button setup screen.
- When importing Apple School Manager data, you can now reassign devices that are assigned to existing users (in addition to assigning devices to new users).
- On iOS 10, apps can be automatically installed on shared iPads when a user is logged in.
- New settings in configuration profiles:
  - Allow user to unlock a Mac with an Apple watch (macOS: Security & Privacy)
  - Firewall settings (macOS device profiles: Security & Privacy)
  - Restrict sharing access to Notes, Reminders, and LinkedIn (macOS: Restrictions)
  - Pulse Secure connection type (macOS: VPN)
  - Disconnect a VPN on idle (for additional VPN connection types; iOS: VPN)
  - Allow Exchange ActiveSync mail drops (iOS and macOS: Exchange ActiveSync)
  - Specify the RSA key size (macOS: AD Certificate)
  - Disable captive network detection (iOS: Wi-Fi)
  - Restrict fast lane QoS marking (macOS: Network (Wi-Fi); iOS: Wi-Fi)
  - Communication service rules (iOS: Contacts, Exchange ActiveSync, Google Account, LDAP)
  - Hide **Install All** button (LANrev Apps)
- iOS home screen layouts can no longer include web clips, because this feature has been dropped from iOS.
- PowerShell scripts executed on client computers using the **Execute Script** command always bypass local execution restrictions.
- New information items:
  - **Server Center** > **Administration** > **Administrators** > **Modify Desktop Actions**
  - **Server Center** > **Actions** (new category)
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Home Button Setup**
- LANrev fully supports macOS 10.12 (Sierra).
- The documentation reflects the name change from “OS X” to “macOS”.
- The following Apple devices are correctly recognized:
  - iPhone 7 and 7 Plus
  - iPhone 6s (32 GB)
  - iPad mini 4 (32 GB)
  - iPad Air 2 (32 GB)
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.2.1

- Additional details are displayed for mobile commands in the command queue and command history in the Mobile Devices window.
- When apps are installed via a policy, the app configuration and app-specific VPN settings can be specified.
- When LANrev removes mobile apps that have been install under a volume license, the license is automatically revoked. (This does not apply when the license was assigned to a person, not a device, because the person might still use the same license on other devices.)
- For shared iOS devices, the transmission of diagnostic information to Apple and the grace period before unlocking the device requires entering the passcode can be configured.
- For devices with a True Tone display, enrollment profiles can specify that the True Tone setup screen is skipped.
- Depending on the circumstances, two different FileVault recovery keys can be generated. When the FileVault key is displayed in LANrev, both keys are always shown.
- The **Set Device Name** and **Enable Attention Mode** commands supports variable substitution.
- There are variables that insert the address, port, or URL of the MDM server.
- KNOX workspaces on Samsung Galaxy S6 devices are now correctly recognized.
- Remote control connections to desktop devices with LANrev Remote use SSL.
- Scheduled OS updates and OS update actions can specify – instead of a specific version of the OS – that the latest available OS version is installed.
- When the MDM server is installed on a system that uses SSLv3 – which has long been known to be no longer secure – the installer now warns of the problem. (LANrev Server always uses a recent implementation of TLS and is therefore not affected by this issue.)
- The file size of log files is limited. When the size is exceeded, the log file is closed and a new one is started.
- New information items:
  - **Agent Information** > **Agent Settings** > **LANrev Remote SSL Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Send App Analytics**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Send Diagnostic & Usage Data**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Has Home Screen Layout Installed**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Passcode Lock Grace Period**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Passcode Lock Grace Period Enforced**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment Force into Management**

  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment Prevent App Data Backup**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment Remove App When MDM Is Removed**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment App Configuration**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment Per-App VPN Configuration**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Force into Management**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Prevent App Data Backup**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Remove App When MDM Is Removed**
  - **Mobile Device Information** > **Application Packages** > **App Assignment VPP Account for Device Assignments**
  - **Mobile Device Information** > **Application Packages** > **App Assignment App Configuration**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Per-App VPN Configuration**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip True Tone Display Setup**
  - **Mobile Device Information** > **Device Commands** > **Mobile Device Command Details**
  - **Mobile Device Information** > **Device Commands** > **Mobile Device Command Type**
- Some inconsistent terminology has been corrected:
  - Apps signed with enterprise certificates are "enterprise apps".
  - Apps downloaded from an app store are "app store apps".
  - Books downloaded from Apple's book store are "iBooks Store books".
- The installer folders on Windows are named more clearly.
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.2

- Enrollment profiles can be edited even when they are already assigned to devices. The devices on which they have been installed are automatically updated for the changes.
- The home screen layout of managed iOS devices can now also be configured in LANrev Admin for Windows (in addition to LANrev Admin for OS X.)
- VPP accounts that are updated automatically for purchased iOS apps are now also updated for books and OS X apps.
- Enterprise apps on iOS devices can be validated through an action (in addition to manually).
- The "Allow modifying diagnostics settings" restriction for iOS devices can be set in configuration profiles.

- When a managed device in a classroom settings is reconfigured, related devices can be reconfigured at the same time.
- The type of password (four- or six-digit or alphanumeric) can be specified for users of shared devices in classroom settings.
- Smart class groups can be filtered by location and by course.
- LANrev displays notifications when the license key is about to expire.
- The MacBook (early 2016) is correctly recognized.
- New information items:
  - **Classroom Management** > **Classroom Person Password Name**
  - **Classroom Management** > **Classroom Person Password Prompt**
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.1

- LANrev adds support for classroom management using Apple Classroom. Classes, teachers, students, and devices are managed in the new **Classroom Management** window. Support for Apple School Manager is included as a preview feature.
- The activation lock of shared and personal devices that are enrolled in an Apple School Manager account can be enabled from LANrev.
- Devices in a classroom setting can be configured by class using a context menu command. It is also possible to configure all devices in one step using a toolbar button or context menu command.
- The new administrator privilege "Modify Enrollment Users" must be enabled on an administrator account to allow an administrator to specify the enrollment user or device owner for a managed mobile device.
- When a device is put into Lost mode, the mode persists across device resets.
- Variables can be used in the Lost mode lock screen message.
- When a new iOS application record is created in LANrev, the application can be searched for by name in the App Store.
- Packages for volume-licensed iOS apps can be automatically created.
- Administrator accounts can be configured to be automatically disabled after a certain number of incorrect passwords were entered.
- A new administrator privilege specifies whether an administrator can change device owners and enrollment users.
- When inventory data is removed, data about OS patches and third-party patches can be removed separately.
- Apple devices introduced in March 2016 are correctly recognized:
  - iPad Pro 9.7"
  - iPhone SE

- New information items:
  - **Server Center** > **Administration** > **Administrators** > **Limit Number of Incorrect Login Attempts**
  - **Server Center** > **Administration** > **Administrators** > **Failed Login Attempts**
  - **Server Center** > **Administration** > **Administrators** > **Maximum Login Attempt Failures**
  - **Server Center** > **Administration** > **Administrators** > **Classroom Management**
  - **Classroom Management** (new section)
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 7.0

- LANrev supports the device Shared iPad feature of iOS 9.3. Supported iPads can be configured as shared during device enrollment, and users can be logged out and their data removed from local device storage. In addition, configuration profiles can be installed for the entire device or only for a specific user.
- LANrev can create configuration profiles that define the home screen layouts of iOS 9.3 devices. These configuration profiles can also be used to prevent the use either of specific apps or of any apps not specified in the profile (blacklisting and whitelisting).
  LANrev Admin for OS X includes a graphical editor for creating these profiles.
- Configuration profiles for iOS 9.3 devices support additional new payloads:
  - Application Restrictions: App-related restrictions for the device, including specifying blacklists or whitelists and restricting access to iTunes Radio.
  - Notification: Notification privileges for apps on the device.
  - Lock Screen Message: Text displayed on a device's lock screen.
  - Google Account: Settings for Google accounts.
  - The Domains payload supports Safari autofill domains.
  - The Restrictions payload supports preventing the modification of notification settings and for allowing remote screen observation.
- The Lost mode of iOS 9.3 devices can be enabled from LANrev. This also tracks the device.
- Apps made available as on-demand installations can be designated as auto-updating.
- When creating in-house app packages, the icon, version number, and category are displayed. The icon and category can be changed.
- LANrev Admin for OS X now requires OS X 10.8 (Mountain Lion) or up.
- The performance of LANrev Remote is greatly improved.

- New information items:
  - **Mobile Device Information** > **Device Information** > **Mobile Device Is Shared**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Maximum Resident Users**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Is MDM Lost Mode Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Logged-in User Apple ID**
  - **Mobile Device Information** > **Managed Device User Information** (new section)
  - **Mobile Device Information** > **Installed Applications** > **Mobile Device Installed App Is Validated**
  - **Mobile Device Information** > **Installed Configuration Profiles** > **Mobile Device Installed Profile for User**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Category**
  - **Mobile Device Information** > **Device Commands** > **Mobile Device Command User**
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in LANrev 6.9.3

- The name of the package and its components changes from "Absolute Manage" to "LANrev".
- MDM-related commands are available for desktop devices even when LANrev is used without an MDM license.
- A new context command allows manually refreshing the Active Directory information for a user.
- MDM enrollment profiles can now be signed, eliminating possible messages about untrusted profiles during the enrollment process.
- Certificates can be removed from the **Push Services Certificates** dialog without requiring them to be replaced by a different certificate.
- Absolute Manage supports migrating VPP app and book licenses from users to devices in batches. (This applies only to licenses that can be assigned to devices.)
- Apps assigned to devices via VPP licenses can be set to update automatically.
- In-house apps using enterprise certificates that have been assigned to devices running iOS 9.2 and up can be validated manually (in addition to standard automatic validation).
- Android device from any vendor can be set to kiosk mode. (Previously, this was only possible for Samsung devices.)
- The default SMTP port for notifications that LANrev sends out (which is configured in the server settings' **Notification** tab) has changed from 465 to 587 for secure connections.
- Third-party patches can now be applied on devices running Windows 10.
- The **Get Device Geolocation** command is now also available while geotracking is enabled for a device.

- Additional applications supported by the third-party patch management:
  - Adobe Acrobat on OS X, Acrobat DC on Windows, Acrobat Reader DC, AIR on OS X
  - Apache OpenOffice on Windows
  - Apple iLife Media Browser on OS X, QuickTime
  - Citrix ICA Win32 Client, Metaframe Server Client, Online Plug-in, Online Plug-in (Web), Presentation Server Client (all on Windows)
  - Evernote on Windows
  - Fetch Softworks Fetch on OS X
  - GIMP on Windows
  - Google Chrome on OS X, Drive on Windows, Earth Pro on Windows
  - Ivo Beltchev's Classic Shell on Windows
  - Microsoft Skype on OS X
  - Novell Client 2 on Windows
  - Opera on Windows
  - Pidgin Team Pidgin on Windows
  - Real Networks RealTimes on Windows
  - Stefan Küng's TortoiseSVN on Windows
  - VMware Horizon View Client on Windows, VMware Server on Windows
  - win.rar WinRAR on Windows
- The iPad Pro is correctly recognized.
- New information items:
  - **Mobile Device Information** > **Application Packages** > **App Version**
  - **Mobile Device Information** > **Application Packages** > **App Allow Automatic Update**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Use Device License**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Perform Automatic Update**
- Various performance improvements and bug fixes. Details are available online in the LANrev knowledge base.

Changes in Absolute Manage 6.9.2

- New Apple devices are correctly recognized:
  - Apple TV (4th generation)
  - iMac (21.5-inch with 4K retina display, October 2015)
  - iMac (27-inch with 5K retina display, October 2015)
  - iPad mini 4
  - iPhone 6s and 6s Plus
- Various performance improvements and bug fixes. Details are available online in the Absolute Manage knowledge base.

Changes in Absolute Manage 6.9.1

Absolute Manage 6.9.1 was not publicly released.

Changes in Absolute Manage 6.9

- Applications from Apple's OS X app store can be installed on managed Macs.
- When a Mac is enrolled into MDM management, the user who receives the notification can be specified. The new **Computer Enrollment MDM User** information item contains the name of the specified user.
- On managed iOS 9 devices, administrators can remotely trigger an operating system update.
- Licenses from Apple's volume purchase program (VPP) can be assigned to devices instead of to users under iOS 9, provided the license allows this.
- When installing applications on mobile devices on iOS 9, administrators can specify that any copy of the application that is already present on a target device is converted to a managed application.
- Management settings for apps installed on mobile devices can also be specified when the app is manually installed and when it is assigned to a policy.
- Enrollment profiles for Apple devices can specify additional setup screens to skip. They can also specify that any pending MDM commands for the device are executed during the setup.
- When information is gathered from a managed mobile device, administrators can specify the categories of information to gather.
- The configuration profile editor supports new options that are available for iOS 9 and OS X 10.11 (El Capitan). New features of Apple Configurator 2.0 are likewise supported.
- The passcode of managed mobile devices can be cleared through an action.
- Administrators can trigger managed devices to contact the MDM server.
- For patches from Microsoft, the security bulletin numbers can be displayed in information items.
- VeraCrypt encryption on managed devices is now detected.
- Renamed information items:
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Diagnostics Setup** has been renamed to **Enrollment Profile Skip App Analytics Setup**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Passcode Setup** has been renamed to **Enrollment Profile Skip Passcode Lock Setup**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Terms of Service** has been renamed to **Enrollment Profile Skip Terms and Conditions**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Zoom Setup** has

been renamed to **Enrollment Profile Skip Display Zoom Setup**

- New information items:
  - **Agent Information** > **General** > **Computer Enrollment MDM User**
  - **Software Information** > **Missing Patches** > **Missing Patch Security Bulletin Numbers**
  - **Server Center** > **Software Distribution** > **Packages** > **Software Patch Security Bulletin Numbers**
  - **Mobile Device Information** > **Device Information** > **Mobile Device OS Update Available**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Available OS Updates Last Change**
  - **Mobile Device Information** > **Available OS Updates** (new section)
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Convert to Managed App**
  - **Mobile Device Information** > **Application Packages** > **App Convert to Managed App**
  - **Mobile Device Information** > **App Store Volume Purchase Program** > **ASVPP License Is Assigned to Device**
  - **Mobile Device Information** > **App Store Volume Purchase Program** > **ASVPP License Product Name**
  - **Mobile Device Information** > **App Store Volume Purchase Program** > **ASVPP License Product Type**
  - **Mobile Device Information** > **App Store Volume Purchase Program** > **ASVPP License Is Device-Assignable**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Move from Android**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip FileVault**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Local Account Setup**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Create Primary Account**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Perform Queued Commands During Setup**
- Various performance improvements and bug fixes. Details are available online in the Absolute Manage knowledge base.

Changes in Absolute Manage 6.8.2

- VPP management has been adapted in preparation for OS X 10.11 (El Capitan) and iOS 9.
- Various performance improvements and bug fixes. Details are available online in the Absolute Manage knowledge base.

Changes in Absolute Manage 6.8.1

- When users are registered with a VPP account, the registration and the sending of an invitation can now be two separate steps.
- VPP operations now run asynchronously in the Admin. Their progress is displayed in the new Activity window.
- Support for payloads in configuration profiles has been improved:
  - iOS:
    - Mail
    - Per-app VPN
    - Restrictions
    - VPN
  - OS X:
    - Mail
    - Network (Ethernet)
    - Network (Wi-Fi)
    - Restrictions
- New Macs are correctly recognized:
  - MacBook (early 2015)
  - iMac (27-inch with 5K retina display, May 2015)
  - MacBook Pro (15-inch with retina display, May 2015)
- The **Mobile Device Model Number** information item is available for Android devices.
- The **Mobile Device Model** information item shows the device model for Samsung devices instead of the model number.
- New information item:
  - **Mobile Device Information** > **Device User Information** > **Device User VPP Invite URL**
- Various performance improvements and bug fixes. Details are available online in the Absolute Manage knowledge base.

Changes in Absolute Manage 6.8

- Patches for a range of third-party productivity and utility applications can now be managed in the same way as operating system patches.
- Devices can no longer be removed from ADEP (disowned) through Absolute Manage. They must now be disowned through Apple's device enrollment portal.
- Recent-model OS X computers with FileVault encryption can now be force-restarted to the desktop without requiring a local user to enter the password, as long as they are MDM-managed and the FileVault recovery key is stored in Absolute Manage.
- Application configuration profiles for third-party applications can now be assigned to policies for automated installation.
- OS X configuration profiles created in Absolute Manage can now specify a list of third-party preference panes that are deactivated (if present) on the configured computer.

- Custom Agent installers can now be imported from the Preferences dialog (in addition to from the Agent Deployment Center).
- When logging in or changing servers, the most recently used servers are now available in a pop-up menu.
- Absolute Manage Administrator for Windows is now available as a 64-bit binary.
- The minimum operating system version for Absolute Manage Agent is now Mac OS X 10.5 (Leopard).
- Correctly detect new Macs:
  - MacBook (early 2015)
  - MacBook Air (11-inch, early 2015)
  - MacBook Air (13-inch, early 2015)
  - MacBook Pro (13-inch with retina display, early 2015)
- Renamed information items:
  - **Agent Information** > **Agent Settings** > **Included in Patch Management** has been renamed to **Included in OS Patch Management**
  - **Software Information** > **Missing OS Patches** has been renamed to **Missing Patches** (renamed category).
  - **Software Information** > **System Information** > **Missing OS Patches Count** has been renamed to **Missing Patches Count**
  - **Missing OS Patches Statistics** has been renamed to **Missing Patch Statistics** (renamed category).

- New information items:
  - **Agent Information** > **Agent Settings** > **Servers** > **Inventory with Fonts**
  - **Agent Information** > **Agent Settings** > **Servers** > **Inventory with Printers**
  - **Agent Information** > **Agent Settings** > **Servers** > **Inventory with Startup Items**
  - **Agent Information** > **Agent Settings** > **Servers** > **Inventory with Windows Services**
  - **Agent Information** > **Agent Settings** > **Servers** > **Scan for Installer Receipts**
  - **Agent Information** > **Agent Settings** > **Servers** > **Scan for Missing OS Patches**
  - **Agent Information** > **Agent Settings** > **Servers** > **Scan for Missing Third-Party Patches**
  - **Agent Information** > **Agent Settings** > **Servers** > **Scan for Applications**
  - **Agent Information** > **Agent Settings** > **Servers** > **Application Scan Options**
  - **Agent Information** > **Agent Settings** > **Included in Third-Party Patch Management**
  - **Software Information** > **System Information** > **FileVault Supported**
  - **Software Information** > **System Information** > **FileVault Enabled**
  - **Software Information** > **System Information** > **FileVault Authentication Restart Supported**
  - **Software Information** > **System Information** > **FileVault Has Personal Recovery Key**
  - **Software Information** > **System Information** > **FileVault Has Institutional Recovery Key**
  - **Software Information** > **System Information** > **FileVault Unlocked Using Recovery Key**
  - **Software Information** > **System Information** > **FileVault Recovery Key Stored on Server**
  - **Software Information** > **Missing Patches** > **Missing Patch Description**
  - **Software Information** > **Missing Patches** > **Missing Patch Severity**
  - **Software Information** > **Missing Patches** > **Missing Patch Is OS Patch**
  - **Server Center** > **Administration** > **Administrators** > **Manage Device Users**
  - **Server Center** > **Software Distribution** > **Packages** > **Package Type**
  - **Server Center** > **Software Distribution** > **Packages** > **Software Patch Severity**
  - **Missing Patch Statistics** > **Missing Patch Stat Is OS Patch**
  - **Missing Patch Statistics** > **Missing Patch Stat Severity**
- Various performance improvements and bug fixes. Details are available online in the Absolute Manage knowledge base.

Changes in Absolute Manage 6.7.1

- User information that is normally read from Active Directory can now be imported manually from a text file for sites where no Active Directory server is available.
  This lets administrators assign VPP licenses to users before they have enrolled a device.
- Mobile devices can now be put into an attention mode from Absolute Manage, directly or through actions. In this mode, a message is displayed on the device's screen, but the device is otherwise completely locked.
- The new "Disable App Store" payload for iOS configuration profiles allows installation of iOS apps through the MDM even when the access to the App Store is blocked on the device.
- The new **Mobile Device iTunes Store Account Is Part of VPP** information item shows whether the active App Store account on a device is registered in the VPP.
- For managed devices running iOS 8.1.3 and above, access to the dictionary, spellchecking, and autocorrection can be disabled through configuration profiles.
- Support for payloads in configuration profiles has been added or improved:
  - iOS:
    - Assessment Restrictions
    - Cellular
  - OS X:
    - Accessibility
    - AD Certificate
    - AirPlay
    - Directory
    - Ethernet
    - Finder
    - Font
    - Login Items
    - Login Window
    - Parental Control
    - Restrictions
    - SCEP
    - Security & Privacy
    - Software Update
    - Time Machine
    - VPN
    - WiFi
    - Xsan
- FileVault can now be configured through a configuration profile, using the Security & Privacy payload.
- The FileVault recovery key for managed OS X devices can be stored and retrieved with Absolute Manage.
- Enrollment profiles for iOS devices can now specify that the devices skip the Touch ID, Apple Pay, and Zoom setup screens.
- Enrollment profiles can now include a support e-mail address.
- Windows operating system patches can now be installed by assigning them to the All PCs group.

- Available App-V applications are detected on administered Windows computers.
- Absolute Manage can now erase and lock devices through Cisco ISE as well as send messages.
- The bandwidth of distribution points can now be limited independently for client downloads and for mirroring with other distribution points.
- Transferring large software distribution payloads over slow connections is more resilient.
- For consistency, all references to "wipe" have been changed to "erase". This concerns:
  - The **Wipe OS X Computer** command (now **Erase OS X Computer**).
  - The **Issue Remote Erase** command (now **Erase Device**).
  - The **Remote wipe** server setting (now **Erase device**).
  - Several information items, as listed below.
- Support for reporting CenterTools DriveLock encryption has been added.
- Renamed information items:
  - **Server Center** > **Software Distribution** > **Distribution Points** > **Download Bandwidth** has been renamed to **Distribution Bandwidth**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Remote Wipe Supported** has been renamed to **Mobile Device Remote Erase Supported**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Ack Time** has been renamed to **Mobile Device Erase Ack Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Request Time** has been renamed to **Mobile Device Erase Request Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Sent Time** has been renamed to **Mobile Device Erase Sent Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Last Device Wipe Requestor** has been renamed to **Mobile Device Last Device Erase Requestor**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Remote Wipe Status** has been renamed to **Mobile Device Remote Erase Status**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Remote Wipe Status Note** has been renamed to **Mobile Device Remote Erase Status Note**
- New information items:
  - **Server Center** > **Software Distribution** > **Distribution Points** > **Mirroring Bandwidth**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Attention Mode Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device iTunes Store Account Is Part of VPP**
  - **Mobile Device Information** > **Device Information** > **Mobile Device App Store Disabled**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Company Support E-Mail**

  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Touch ID Setup**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Apple Pay Setup**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Zoom Setup**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.7

- Apple's device enrollment program (ADEP) is now supported for Macs as well.
- MDM enrollment for Macs is supported.
- On Macs enrolled in MDM that run OS X 10.10 or above, the Agent is automatically installed.
- Macs enrolled in MDM can be remotely locked so that access is only possible by locally entering a special password specified by you. They can also be remotely wiped, deleting any and all information and software on them.
- When Admin lists the media files installed on a managed mobile device, it now includes files installed in AbsoluteSafe.
- Detailed views for Android devices in the Mobile Devices window now include lists with the installed media files and certificates.
- Additional key fields are available for importing mobile device users.
- Absolute Manage InstallEase no longer requires an activation key. It also no longer requires Xcode on the Mac to generate installer packages. The minimum operating system requirement on a Mac is now Mac OS X 10.7 and an Intel processor.
- Added new encryption protocols that are detected on administered computers:
  - PGP 10
  - DESlock
  - BitLocker
  - Kaspersky Lab FDE
- Correctly detect new Apple products:
  - iPad mini 3
  - iPad Air 2
  - iPhone 5c with 8 GB
  - iPhone 6 and iPhone 6 Plus
  - iPod touch. 5th generation 16 GB
  - iMac 21.5" (mid 2014)
  - iMac with Retina 5K display
  - Mac mini (late 2014)
  - MacBook Pro (mid 2014)
- New information items:
  - **Agent Information** > **General** > **Computer Enrollment Date**
  - **Agent Information** > **General** > **Computer Enrolled via Enrollment Program**
  - **Agent Information** > **General** > **Computer Enrollment Registration Date**

  - **Agent Information** > **General** > **Computer Enrollment Profile Assignment Date**
  - **Agent Information** > **General** > **Computer Enrollment Profile Installation Date**
  - **Agent Information** > **General** > **Computer Enrollment Profile UUID**
  - **Agent Information** > **General** > **Computer Enrollment Status**
  - **Agent Information** > **General** > **Computer Device Identifier (UDID)**
  - **Agent Information** > **Agent Settings** > **Servers** > **Is Primary Inventory Server**
  - **Hardware Information** > **System Information** > **Computer Color**
  - **Mobile Device Information** > **Device User Information** > **Device User Depertment Number**
  - **Mobile Device Information** > **Device User Information** > **Device User Employee Number**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Company**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Country Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Serial Number**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Key Usage**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Is Root**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Valid Until**
  - **Mobile Device Information** > **Installed Certificates** > **Mobile Device Installed Certificate Valid From**
  - **Mobile Device Information** > **Installed Media Files** > **Installed Media File Container**
  - **Mobile Device Information** > **Installed Media Files** > **Installed Media File Download Date**
  - **Mobile Device Information** > **Installed Media Files** > **Installed Media File Removal Date**
  - **Mobile Device Information** > **Installed Media Files** > **Installed Media File Bookstore ID**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** > **Enrollment Profile Skip Media Registration**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.6

- Support for managing media files on managed iOS 8 devices has been greatly enhanced:
  - Media files from the iBooks Store are now supported.
  - Compatible media files can be installed in iBooks now. This option is available for PDF, ePub, and iBook files.
  - Installation in iBooks is also available via policies.
  - Statistics for bookstore books are available.

- For items purchased through Apple's volume purchase program, information items are available that list all VPP accounts containing licenses for these items.
- The restrictions password can be removed from managed iOS 8 devices.
- The names of managed iOS 8 devices can be changed. Changing names of managed mobile devices is now also supported as a policy action.
- The contents of custom fields can be set by policy actions.
- New configuration capabilities of configuration profiles for iOS 8 devices are supported:
  - Web content filter plug-ins
  - IKEv2 VPN
  - Additional WiFi options
  - Certificate renewal settings for single sign-on
  - Additional Mail and Exchange options
  - New restrictions
  - Domain settings
- Mac App Store applications that are purchased through Apple's volume purchase program can now be managed and assigned through Absolute Manage.
- Absolute Manage Admin now requires OS X 10.7 or above.
- If an Admin is connected to Absolute Manage Server running on Windows, it displays in the About box whether the server is the 32-bit or 64-bit version.
- Additional disk encryption types are now detected:
  - Wave Cloud 2014
  - SecureDoc 6.4
  - Credant Mobile Guardian 7.3
- New information items:
  - **Agent Information** > **General** > **Computer Enrolled into MDM**
  - **Agent Information** > **General** > **Computer Device Identifier (UDID)**
  - **Hardware Information** > **System Information** > **BIOS Type**
  - **Server Center** > **Software Distribution** > **Mac App Store Applications** (new category)
  - **Mobile Device Information** > **Device Information** > **Mobile Device Last Cloud Backup**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Installed Application Count**
  - **Mobile Device Information** > **Device User Information** > **Device User Mobile Phone Number**
  - **Mobile Device Information** > **Installed Media Files** (new category)
  - **Mobile Device Information** > **Installed Media File Statistics** (new category)
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Accounts**
  - **Mobile Device Information** > **Mobile Media** > **Media File Author**
  - **Mobile Device Information** > **Mobile Media** > **Media File Version**
  - **Bookstore Books** > **Book VPP Accounts**

- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.5

- Windows XP is no longer supported as a platform for Absolute Manage Server and Absolute Manage Admin. We continue to support Absolute Manage Agent on Windows XP, although functionality may be limited.
- Absolute Manage Server and Absolute Manage Admin can no longer be installed on Mac OS X 10.5.
- Absolute Manage is now fully compatible with OS X 10.10 (Yosemite).
- Absolute Manage now supports Cisco ISE and can reply to compliancy inquiries.
- Absolute Manage now supports Samsung KNOX. You can create, remove, lock, and unlock workspaces and install apps into workspaces. Configuration profiles for configuring KNOX on managed devices are also supported.
- A special policy is now available that lists unmanaged mobile devices. The policy is limited to assigning actions to these devices that do require MDM, in particular sending messages.
- Logging of all MDM-related administrator actions can now be enabled through the server settings.
- Device ownership data, enrollment user data, and custom information field contents can now be imported automatically on the server.
- License purchase tracking data can now be imported from a tab-delimited text file.
- For automatic inventory updates from mobile devices, you can now choose between full and basic updates.
- The information items for profile and software installation dates now also include the time.
- Device enrollment profiles can be assigned through policies.
- Bypass codes for activation locks of supervised iOS devices can now be displayed in Absolute Manage.
- Adding and removing users of Apple's volume purchasing program (VPP) can now be added and removed via policy actions.
- The Guided Access module of iOS configuration profiles has been renamed to "Single App Mode".
- The GSM push notification system of Android 4.0 is supported. Gmail accounts are therefore no longer required for Android devices running 4.0 and above.
- Remote viewing and controlling of mobile devices with Samsung SAFE is now supported.
- Configuration profiles for Android devices can now specify web clips – bookmarks for web addresses that appear as an icon on the home screen.
- Desktop computers can now be put under administration through an MDM-like enrollment mechanism instead of push-installations of the agent software.
- Commands for managed computers and devices can now be exported as template files for easy distribution to other administrators.

- Absolute Manage SCCM Integration now supports a wider range of fields for the unique identifier and name of devices that are exported to SCCM or SMS.
- FinallySecure Enterprise Encryption and SecurStar DriveCrypt disk encryption is correctly detected on client computers.
- Correctly detect new Macintosh models:
  - MacBook Pro 15" (late 2013)
  - MacBook Air (early 2014)
- The Server Widget is no longer included with Absolute Manage.
- Renamed information items:
  - **Mobile Device Information** > **Device User Information**: All information items in this category were renamed from **Mobile Device User …** to **Device User …**; for example, from **Mobile Device User Display Name** to **Device User Display Name**.
  - **Mobile Device Information** > **Device Information** > **Mobile Device IMEI/MEID** has been renamed to **Mobile Device IMEI** and no longer displays MEID information.
- New information items:
  - **Agent Information** > **General** > **Computer Enrollment Date**
  - **Agent Information** > **General** > **Computer Ownership**
  - **Hardware Information** > **System Information** > **Computer Boot Duration**
  - **Mobile Device Information** > **Device Information** > **Mobile Device MEID**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Activation Lock Removed**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Has Activation Lock Bypass Code**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Activation Lock Removal Date**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Is Cloud Backup Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Supports KNOX**
  - **Mobile Device Information** > **Device Information** > **Mobile Device KNOX Status**
  - **Mobile Device Information** > **Device Information** > **Mobile Device KNOX Version**
  - **Mobile Device Information** > **Device User Information** > **Device User Job Title**
  - **Mobile Device Information** > **Device User Information** > **Device User Managed By**
  - **Mobile Device Information** > **Device User Information** > **Device User Employee ID**
  - **Mobile Device Information** > **Device User Information** > **Device User Account Disabled**
  - **Mobile Device Information** > **Device User Information** > **Device User Account Locked**
  - **Mobile Device Information** > **Device User Information** > **Device User Account Lockout Time**
  - **Mobile Device Information** > **Device User Information** > **Device User Account Password Expiration Date**

  - **Mobile Device Information** > **Device User Information** > **Device User Password Expired**
  - **Mobile Device Information** > **Device User Information** > **Device User Business Category**
  - **Mobile Device Information** > **Device User Information** > **Device User Extension Attribute 1** through **Device User Extension Attribute 15**
  - **Mobile Device Information** > **Installed Applications** > **Mobile Device Installed App Is KNOX**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assigned to KNOX Workspace**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Is KNOX**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.4.3

- Absolute Manage supports the newly introduced activation lock bypass for supervised devices in iOS 7.1.
  The required bypass code is read from devices automatically during enrollment. It can be displayed with the **Show Activation Lock Bypass Code** context menu command.
  The activation lock can be bypassed with the **Remove Activation Lock** context menu command. It can also be removed when the device is erased remotely.

Changes in Absolute Manage 6.4.2

- Absolute Manage supports Apple's new Device Enrollment Program. You can add devices to the program, set up and assign enrollment profiles, and put devices into supervised mode from Absolute Manage Admin.
- For supervised iOS devices, the automatic connection between "Find My iPhone" and the activation lock can now be configured, either manually or through an action.
- The lock screen and home screen backgrounds on supervised iOS devices can now be set, either manually or through an action.
- Additional information for Apple VPP accounts are displayed.
- Several new administrator privilege settings allow more control over who can access which VPP functions.
- Dynamic SCEP challenges are now supported for iOS configuration profiles that use SCEP.
- Absolute Manage now includes a Linux Agent that supports a limited set of information items and commands.
- Adding information items to browser windows can no longer lead to some devices no longer being shown in the window.
  An additional effect of this change is adding information items that create multiple entries for a device now creates one entry for each combination of entries.
  For example, if an information item for USB devices is added to a browser window displaying computers, one line in the

window displays each device. If a second information item displaying PCI slots is added, the window contains one line for each combination of an USB device and a PCI slot on a computer.

- Dynamic custom field data can now be reset using the **Remove Inventory Data** command.
- The detection of several kinds of disk encryption on administered computers has been added or improved: ATA security, McAfee encryption, SafeBoot, TrendMicro encryption.
- Absolute Manage MDM Server is now available in a 64-bit version for Windows as well (in addition to the 32-bit version).
- The Mac Pro (late 2013) is now correctly recognized.
- New information items:
  - **Agent Information** > **General** > **Last Contacted by Server**
  - **Server Center** > **Administration** > **Administrators** > **Change Device Enrollment Program Account**
  - **Server Center** > **Administration** > **Administrators** > **Change VPP Account Settings**
  - **Server Center** > **Administration** > **Administrators** > **Modify Bookstore Books**
  - **Server Center** > **Administration** > **Administrators** > **Modify Device Enrollment Profiles**
  - **Server Center** > **Administration** > **Administrators** > **Modify VPP License Management**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Model Identifier**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Color**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrolled via Enrollment Program**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrollment Status**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrollment Program Registration Date**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrollment Profile Assignment Date**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrollment Profile Installation Date**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enrollment Profile UUID**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Purchased**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Assigned**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Remaining**
  - **Mobile Device Information** > **Mobile Device Enrollment Profiles** (new category)
  - **Bookstore Books** > **Book VPP Licenses Purchased**
  - **Bookstore Books** > **Book VPP Licenses Assigned**
  - **Bookstore Books** > **Book VPP Licenses Remaining**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.4.1

- Apps purchased through Apple's VPP can now be assigned and removed automatically through policies on managed devices running iOS 7 and up.
  (Removing the app through a policy does not revoke the license; this must be done manually.)
- Licenses for books and apps purchased through Apple's VPP can now be assigned in book, app, or user detail views. App licenses can also be revoked in these views. (Book licenses cannot be revoked because Apple does not permit this.)
- VPP license details have been added to user detail views.
- Licenses for apps purchased through Apple's VPP can be assigned to a user or revoked from the user by selecting a device linked to that user.
- Detail views for apps purchased through Apple's VPP display the number of times the app is currently installed on managed devices.
- VPP invitation can be sent through the MDM system to devices running iOS 7.0.3 and up.
- AbsoluteSafe can now be distributed as an in-house app to iOS 6 and 7 clients in the same way as AbsoluteApps.
- The configuration profile editor now supports Apple's third-party app configuration feature for apps running on iOS 7. It includes modules to create profiles for AbsoluteSafe and to create PList configuration files for arbitrary apps.
- Additional information is displayed in the user detail view for registered MDM users.
- The iPad Air, iPad mini with retina display, iPhone 5C, and iPhone 5S are now correctly recognized, including colors and memory sizes.
- New information items:
  - **Mobile Device Information** > **Device User Information** > **Mobile Device User Active VPP Accounts**
  - **Mobile Device Information** > **Device User Information** > **Mobile Device User VPP Accounts**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Purchased**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Assigned**
  - **Mobile Device Information** > **Application Packages** > **App Store VPP Licenses Remaining**
  - **Bookstore Books** > **VPP Licenses Purchased**
  - **Bookstore Books** > **VPP Licenses Assigned**
  - **Bookstore Books** > **VPP Licenses Remaining**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.4

- Absolute Manage is now fully compatible with iOS 7 and OS X 10.9 Mavericks.

- Absolute Manage Server is now available in a 64-bit version for Windows as well (in addition to the 32-bit versions).
- Apple's upcoming App Store volume purchase program (VPP) is already supported.
- Configuration profiles for third-party mobile apps can now be created in Absolute Manage and assigned to the apps. This requires the app's developers to provide appropriate support in their apps.
- Configuration profiles for OS X devices now support custom settings that lets property list (.plist) files be modified.
- Configuration profiles for iOS 7 devices now support settings for:
  - Per-app VPN
  - Fonts
  - Single sign-on
  - AirPrint
  - AirPlay screen mirroring
  - Web content filtering
- Configuration profiles for iOS 7 devices support expanded settings for:
  - Guided Access
  - Global HTTP proxies
  - WiFi
  - Restrictions
- App-specific VPN settings can now be created as iOS configuration profiles and assigned to iOS 7 apps.
- It is now possible to prevent the activation lock feature from being activated when "Find My iPhone" is switched on.
- AirPlay on iOS 7 devices can be activated and deactivated from Absolute Admin.
- The personal hotspot on iOS 7 devices can be turned on or off from Absolute Admin.
- Basic information on your organization can now be stored on managed mobile devices running iOS 7.
- Books from the iTunes bookstore can now be managed in Absolute Manage.
- In some cases, users may need to bind the iOS versions of AbsoluteApps and AbsoluteSafe to their devices by entering their credentials, and in some cases they may also need to pick their device from a list.
- All iOS apps (AbsoluteApps, AbsoluteFind, AbsoluteSafe) now require iOS 6.0 or newer.
- Apple TV devices registered via MDM are now supported. This requires Apple TV software 6.0 or up.
- Recently introduced Apple devices are now correctly detected:
  - MacBook Pro (mid 2013)
  - MacBook Air (mid 2013)
  - iPhone 5C
  - iPhone 5S
- New information items:
  - **Mobile Device Information** > **Device Information** > **Mobile Device Is Supervised**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Ethernet MAC Address**

  - **Mobile Device Information** > **Device Information** > **Mobile Device iTunes Store Account Active**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Find My Device Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Activation Lock Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Do Not Disturb Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Personal Hotspot Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Organization Name**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Organization Address**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Organization E-Mail**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Organization Phone**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Organization Custom**
  - **Mobile Device Information** > **Device User Information** > **Mobile Device User VPP Status**
  - **Mobile Device Information** > **Installed Applications** > **Mobile Device Managed App Has Configuration File**
  - **Mobile Device Information** > **Application Packages** > **App App Store ID**
  - **Mobile Device Information** > **Application Packages** > **App Bundle Identifier**
  - **Mobile Device Information** > **Application Packages** > **App License Is Irrevocable**
  - **Mobile Device Information** > **App Store Volume Purchase Codes** > **ASVPP License Status**
  - **Mobile Device Information** > **Mobile Configuration Profile Definitions** > **Mobile Profile App Bundle Identifier**
  - **Bookstore Books** (new category)
- Renamed information items:
  - **Hardware Information** > **System Information** > **Apple Purchase Date** has been renamed to **Computer Purchase Date**
  - **Mobile Device Information** > **App Store Volume Purchase Codes**: This category has been renamed to **App Store Volume Purchase Program**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.3.1

- There is now a batch process for setting enrollment users for devices already in use by importing the relevant information from a text file using the **File** > **Import** > **Enrollment Users for Mobile Devices** command or the **Import Enrollment Users** context menu command.
  This process works similarly to importing custom field data.

- For fetching MDM user info automatically from Active Directory, you can now specify a separate Active Directory account in the server settings. This lets Absolute Manage get the information even when your normal account does not have sufficient privileges.
- MDM management of Windows 8 Phone and Windows RT devices is now supported via Exchange ActiveSync.
- Non-managed Android devices are now displayed with grayed-out icons in the **Mobile Devices** window.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.3

- You can now assign configuration profiles and MCX settings files to managed OS X computers.
- Configuration profiles (both for mobile devices and for computers) can now be exported as files to disk.
- Absolute Manage now automatically detects embedded profiles in iOS applications so that a separate preparation step is no longer required.
- The disk encryption recognition for Windows clients now also supports the default encryption of Trend Micro DataArmor 3, OPAL encryption in McAfee Endpoint Encryption, and Credant CMG 7 encryption.
- The following products are correctly detected:
  - MacBook Pro versions with Retina Display released in January 2013
  - iMac 21.5 Inch (early 2013)
- The **Smart Installation Status Group** context menu command has been renamed **Smart Software Installation Status Group**.
- New information items:
  - **Software Information** > **System Information** > **Computrace Agent Last Call Time**
  - **Software Information** > **System Information** > **Computrace Agent Next Call Time**
  - **Software Information** > **Installed Configuration Profiles** (new category)
  - **Hardware Information** > **System Information** > **Computer Identifier**
  - **Server Center** > **Administration** > **Administrators** > **Modify Configuration Profiles**
  - **Server Center** > **Software Distribution** > **Configuration Profiles** (new category)
  - **Server Center** > **Software Distribution** > **Configuration Profile Installation Status** (new category)
  - **Mobile Device Information** > **Device Information** > **Mobile Device AbsoluteApps Vendor Support**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Vendor MDM Version**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.2

- Support for PowerPC processors has been removed from all components of Absolute Manage for OS X (except InstallEase).
- In the Resource Center, an add-on is now available that offers limited MDM functionality over the web. You can:
  - View hardware inventory
  - Send certain commands to manage devices
  - Manage media files for AbsoluteSafe access
- Absolute Manage now has a built-in editor for configuration profiles. It lets you create and edit profiles for all supported mobile platforms (including some vendor-specific extensions such as Samsung SAFE) as well as for the mobile applications that are part of Absolute Manage and the NitroDesk TouchDown client for Microsoft Exchange.
- Configuration profiles can now be duplicated using the **Duplicate Configuration Profile** context menu command.
- Absolute Manage now supports NDES (Microsoft's SCEP implementation) for certificate-based Exchange access of mobile devices.
  SCEP can be enabled by installing a profile on managed mobile devices.
- AbsoluteSafe for iOS now supports displaying media from SharePoint libraries. The handling options and access times for these documents can be controlled through configuration profiles.
- The **Help** menu now includes direct links to Absolute Manage web support pages and forums.
- When dealing with registry keys, Absolute Manage Agent can now create missing parts of the path of a key.
- The remote viewing function now supports VNC 5.
- Disk encryption using Credant FVE or SecureDoc 6.1 is now correctly detected.
- The purchase date can now also be displayed for Dell computers.
- The following products are correctly detected:
  - MacBook Pro 13 Inch with Retina Display (late 2012)
  - Mac mini (late 2012)
  - iMac 21.5 Inch (late 2012)
  - iMac 27 Inch (late 2012)
- Renamed information item: **Hardware Information** > **System Information** > **Apple Purchase Date** is now **Computer Purchase Date**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1.5

- AbsoluteSafe is now also available for Android. It can be downloaded from the Resource Center.
- Microsoft System Center Configuration Manager 2012 (SCCM 2012) is supported.
- The iMac introduced in late 2012 is correctly detected.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1.4

- The following products introduced in September 2012 are correctly detected:
  - iPad (4th generation)
  - iPad mini
  - iPod touch (5th generation)
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1.3

- Software packages can now be exported from the Server Center, using the new **Export Package** command when software packages are displayed.
  Exported software packages can be imported on other computers running Absolute Manage Admin using the **File** > **Import** > **Software Packages** command.
  Both exporting and importing packages requires an administrator account with the Modify Software Packages privilege.
  Exporting patch packages, agent update packages, or packages with uncommitted changes is not possible.
  An exported packages is saved as a folder (as a package on a Mac) that includes both the package specification and the installation binaries. Do not edit the contents of this folder in any way.
- License specifications can now be exported from the Server Center, using the new **Export License** command when license specifications are displayed.
  Exported license specifications can be imported on other computers running Absolute Manage Admin using the **File** > **Import** > **License Specifications** command.
  Both exporting and importing license specifications requires an administrator account with the Modify License Specifications privilege.
- The iPhone 5 introduced in September 2012 is correctly detected.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1.2

- Absolute Manage now lets you create placeholder records for mobile devices that allows you to assign devices you expect to enroll to policies so that they will automatically be configured upon their enrollment.
- The new **Set Enrollment User** context menu command lets you change the Active Directory or Open Directory account with which a device is associated.
- The ownership information of a mobile device can now also be set to "guest" or "undefined".
- OS X 10.8 (Mountain Lion) is supported.
- Windows 8 is supported.
- The new MacBook Pro and MacBook Air computers introduced in June 2012 are correctly detected.
- New information item **Software Information** > **System Information** > **Computrace Identifier**
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1.1

- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.1

- Configuration profiles are now also available for Android and Windows Phone devices. In addition to general Android settings, additional vendor-specific settings are supported for certain Lenovo and Motorola devices.
- Absolute Manage adds the capability to create configuration profiles for specific apps. This requires support by the apps authors; an SDK will be made available. The app included with Absolute Manage can already be configured with a configuration profile.
- AbsoluteApps for Android has a new section to display and remove installed profiles.
- Smart policies can now include actions that are executed every time a mobile device joins the policy. Actions include sending notifications to administrators or the user, applying roaming settings, freezing the device, refreshing the information stored on the server for the device, removing profiles, or ending MDM management for the device.
- For messages sent by actions, a number of variables are available that let you customize the message, e.g., by putting the name of the device into the message.
- Media files can be assigned to policies in new ways. In addition to the existing way, in which the media files were available for optional download on devices belonging to the policy and were forcibly removed when the device left the

policy (now called "On-demand, Auto-remove" there are three new categories:
  - Auto-install: Media files are downloaded automatically when a device enters the policy but not automatically removed.
  - On-demand media: Media files can be downloaded manually by the users of devices belonging to the policy and are not automatically removed.
  - Auto-install, Auto-remove: Media files are downloaded automatically when the device enters the policy and removed automatically when the device leaves.
- In addition to individual media files, entire folders of media files can now be imported in a single step.
- Optionally, a media file can be restricted to be transferred only over WiFi connections.
- XML and XSL have been added as supported media types; they can be displayed in AbsoluteSafe. (Safari web archives can also be displayed, which was always possible but so far not documented.)
- Similar to media files (see above), in-house apps can be assigned to policies in new ways. The existing category "Allowed in-house apps" has been renamed "On-demand", and there are three new categories:
  - Auto-install: Apps are downloaded automatically when a device enters the policy but not automatically removed.
  - Auto-install, Auto-remove: Apps are downloaded automatically when the device enters the policy and removed automatically when the device leaves.
  - On-demand, Auto-remove: Apps can be downloaded manually by the users of devices belonging to the policy. They are automatically removed when the device leaves the policy.
- When a passcode on a managed Android device is cleared, you can now optionally specify a new passcode.
- Erasing an Android device now optionally lets you erase any SD cards present in the device as well.
- On Android devices supporting persistence, the Absolute Manage client software now survives removal attempts and factory resets. The new **Mobile Device Supports Persistence** information item shows which devices support this feature.
- On Android devices supporting persistence, push installations and removals of in-house apps are now silent, i.e., without any user intervention.
- AbsoluteSafe now supports background downloads (downloading one document while viewing another) and multiple downloads can be queued.
- Users can flag favorite files in AbsoluteSafe for quicker access.
- AbsoluteApps for iOS is no longer distributed on the Absolute Manage disk. If you require manual deployment of AbsoluteApps, contact Absolute Professional Services.
- The version of AbsoluteApps for iOS available in the App Store no longer supports geotracking and downloading in-house apps on-demand.
- Support for user-owned devices has been enhanced: A new information item (Mobile Device Ownership) indicates whether

the device is owned by the company or the user. The information can be set by the user during enrollment or later by the administrator.
It is possible to display a policy agreement to the user that must be accepted to complete the enrollment of user-owned devices.

- E-mail notifications or text messages (SMSs) can now be sent when server maintenance or ODBC export fails.
- There are new information items for reporting the encryption status of managed desktop devices.
- Absolute Manage now includes the Absolute Remote remote control application. It can be configured as the preferred way to view remote computers' screens and is then launched automatically whenever an administrator wants to view or control a remote computer.
  The Agent now includes screen-sharing functionality that allows Absolute Remote connections without requiring any third-party software. This screen-sharing function can be disabled from Absolute Manage Admin.
- There is now a Windows version of Absolute Manage InstallEase. Similar to the Mac OS X version, it lets you create custom MSI installers based on installing and configuring the software on a sample computer.
- The new iPads introduced in March 2012 are correctly detected.
- New information items:
  - **Agent Information** > **Agent Settings** > **Absolute Remote Enabled**
  - **Agent Information** > **Agent Settings** > **Absolute Remote Port**
  - **Agent Information** > **Agent Settings** > **Absolute Remote User Confirmation Required**
  - **Software Information** > **System Information** > **Disk Encryption Product**
  - **Software Information** > **System Information** > **Disk Encryption Version**
  - **Software Information** > **System Information** > **Disk Encryption Status**
  - **Software Information** > **System Information** > **Disk Encryption Algorithm**
  - **Software Information** > **System Information** > **Disk Encryption Key Size**
  - **Server Center** > **Administration** > **Administrators** > **Modify Mobile Actions**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Ownership**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Supports Persistence**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Information Last Change**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Installed Software Last Change**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Installed Configuration Profiles Last Change**

  - **Mobile Device Information** > **Device Information** > **Mobile Device Installed Certificates Last Change**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Installed Provisioning Profiles Last Change**
  - **Mobile Device Information** > **Installed Configuration Profiles** > **Mobile Device Installed Profile Type**
  - **Mobile Device Information** > **Mobile Configuration Profile Definitions** > **Mobile Profile Type**
  - **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Assignment Rule**
  - **Mobile Device Information** > **Application Packages** > **App Assignment Rule**
  - **Mobile Device Information** > **Mobile Configuration Profile Definitions** > **Assigned Mobile Profile Assignment Rule**
  - **Mobile Device Information** > **Mobile Media** > **Assigned Media Assignment Rule**
  - **Mobile Device Information** > **Mobile Actions** (new category)
- Renamed information items:
  - **Server Center** > **Administration** > **Administrators** > **Modify iOS Configuration Profiles** is now **Modify Mobile Configuration Profiles**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Name** is now **Mobile Device Installed Profile Name**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Description** is now **Mobile Device Installed Profile Description**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Organization** is now **Mobile Device Installed Profile Organization**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Identifier** is now **Mobile Device Installed Profile Identifier**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile UUID** is now **Mobile Device Installed Profile UUID**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Version** is now **Mobile Device Installed Profile Version**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Encrypted** is now **Mobile Device Installed Profile Encrypted**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Managed** is now **Mobile Device Installed Profile Managed**.
  - **Mobile Device Information** > **Installed Configuration Profiles** > **iOS Installed Profile Allow Removal** is now **Mobile Device Installed Profile Allow Removal**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Name** is now **Mobile Device Inst. Profile Name**.

  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Count** is now **Mobile Device Inst. Profile Count**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Managed Count** is now **Mobile Device Inst. Profile Managed Count**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Description** is now **Mobile Device Inst. Profile Description**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Identifier** is now **Mobile Device Inst. Profile Identifier**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile Organization** is now **Mobile Device Inst. Profile Organization**.
  - **Mobile Device Information** > **Installed Configuration Profile Statistics** > **iOS Inst. Profile UUID** is now **Mobile Device Inst. Profile UUID**.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.0.3

- Absolute Manage can now administer Windows Phone clients through the Exchange Server MDM functionality.
  Not all commands and information items are available for managed Windows Phone devices.
- In addition to individual media files, entire folders of files can now be imported into Absolute Manage.
- New information items:
  - **Mobile Device Information** > **Device Information** > **Mobile Device AbsoluteApps Supports Tracking**
  - **Mobile Device Information** > **Device Information** > **Mobile Device OS Language**
  - **Mobile Device Information** > **Device Information** > **Mobile Device GUID**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Identity**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Enable Outbound SMS**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Last Policy Update Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Remote Wipe Supported**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Ack Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Request Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Wipe Sent Time**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Last Device Wipe Requestor**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Number of Folders Synched**

  - **Mobile Device Information** > **Device Information** > **Mobile Device Access Control Rule**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Access State**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Access State Reason**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Status**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Status Note**
  - **Mobile Device Information** > **Mobile Configuration Profile Definitions** > **Mobile Platform Type** (the category has been renamed; see below)
  - **Mobile Device Information** > **EAS Policies** (new category)
- Renamed information items:
  - **Server Center** > **Administration** > **Administrators** > **Modify iOS Configuration Profiles** is now **Modify Mobile Configuration Profiles**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** (category) is now **Mobile Configuration Profile Definitions**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Name** is now **Mobile Profile Name**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Description** is now **Mobile Profile Description**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Organization** is now **Mobile Profile Organization**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Identifier** is now **Mobile Profile Identifier**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile UUID** is now **Mobile Profile UUID**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Allow Removal** is now **Mobile Profile Allow Removal**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **iOS Profile Variables Used** is now **Mobile Profile Variables Used**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability** is now **Assigned Mobile Profile Availability**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability Start Time** is now **Assigned Mobile Profile Availability Start Time**.
  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability End Time** is now **Assigned Mobile Profile Availability End Time**.

  - **Mobile Device Information** > **Mobile Media** > **Media File Can Leave App** is now **Media File Can Leave AbsoluteSafe**.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.0.1

New features in Absolute Manage 6.0.1 include:

- Absolute Apps can now simply be downloaded from Apple's App Store. It must no longer be signed and manually distributed, although this is still possible.
- Creating and specifying the MDM push certificates required for managing iOS devices has been simplified. There is now a built-in assistant that is automatically called when a certificate must be specified.
- You no longer need an enterprise developer account to create an MDM push certificate, just a normal Apple ID.
- When the **Policies** category has been selected in the sidebar of the **Mobile Devices** window, the context menu of the main window area now contains commands to display the members of the individual policies.
- The default category for recommended apps is now "Utilities".
- The MacBook Pro Models introduced in October 2011 are correctly recognized.
- Various performance improvements and bug fixes.

Changes in Absolute Manage 6.0

New features in Absolute Manage 6.0 include:

- MDM support for devices running iOS 5 has been greatly expanded over the functions available for iOS 4 devices:
  - Managed apps are now supported that can be directly installed (without requiring a policy) and remotely removed.
  - The backup of app data can be suppressed.
  - The removal of the MDM management profile can be registered and can trigger the deletion of specific apps on the device.
  - Roaming options can be set and monitored remotely.
- Absolute Manage now manages Android devices in addition to iOS devices. Almost all functions that are available for iOS devices are also supported for Android.
- iOS device data from iTunes installed on managed desktop computers is no longer gathered. That means that mobile devices are now supported only through an MDM server.
- A new iOS application, Absolute Safe, allows the distribution of media files to managed mobile devices. Media files can optionally be protected against further distribution. The capability to manage these media files has been added to

Absolute Manage Admin and Absolute Manage Server. Absolute Safe is currently available only for iOS devices.

- There is a new command for installing apps onto mobile devices without using policies. This command also provides a more direct installation process in which apps are not merely made available in AbsoluteApps but the user is actively prompted to install them.
- For in-house iOS apps imported into Absolute Manage, you can now specify on which types of devices (iPod, iPhone, iPad) they can be installed.
- Build numbers are displayed for imported in-house applications and commercial apps that are installed directly (without a policy).
- The availability of configuration profiles that are applied to mobile devices through policies can be restricted to a one-time period or a daily interval.
- Policies can be locked to profiles. Such policy-locked profiles are automatically installed when a device is added to the policy and deleted when the device is removed from the policy.
- The detail views of app packages and configuration profiles display a list of policies to which the item is assigned.
- All mobile devices listed in the sidebar of the **Mobile Devices** window now include a subcategory displaying the profiles (iOS devices only), media and apps assigned to them. If a profile is assigned through more than one policy, only the assignment with the highest precedence is listed. (For example, if a profile is assigned as forbidden in one policy and required in another, it is listed as required.)
- Importing volume purchase codes now adds them to the existing list of codes (instead of overwriting the list).
- Tracking can now be activated on multiple devices in one step. This requires a global passphrase to be used.
- A new context menu command, **Send Re-enrollment Message to Device**, lets you easily re-enroll iOS devices. Re-enrolling is necessary when the MDM privileges are changed.
- Absolute Manage now includes all components required for reinstalling Windows PCs. Using an additional FOG server is no longer required, although it still is fully supported.
- Concurrent changes to administrator accounts, license monitoring settings, or software distribution settings are now handled smarter: Instead of blocking other administrators from changing these settings once one administrator has begun editing them, Absolute Manage now allows any number of administrators to work on the settings simultaneously and then intelligently merges them. If there are conflicting changes, users are asked to resolve the conflict manually.
- Smart groups for desktop and mobile devices can now be created based on the presence or absence of specified software on the devices.
- There are new environment variables for identifying the registry paths for 32-bit and 64-bit software.
- Context menu commands for creating groups and smart groups have been rephrased for increased clarity.
- Warranty information is now also displayed for computers from Dell and Lenovo.

- The version information for installed software on desktop devices is now available as a number (in addition to as a string) to allow sorting and comparison.
- The Mobile Device Name information item can now be specified as a key field when custom information field data is imported.
- New information items:
  - **Software Information** > **Installed Software** > **Inst. Software Version**
  - **Hardware Information** > **System Information** > **Computer Express Service Tag (Dell)**
  - **Server Center** > **Administrators** > **Modify Mobile Media**
  - **Server Center** > **Software Distribution** > **Distribution Points** > **Distribution Point OS Platform**
  - **Mobile Device Information** > **Device Information** > **Mobile Device WiFi Network**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Is Tablet**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Display Resolution**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Battery Level**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Voice Roaming Enabled**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Board**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Brand**
  - **Mobile Device Information** > **Device Information** > **Mobile Device CPU Name**
  - **Mobile Device Information** > **Device Information** > **Mobile Device CPU Speed**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Info**
  - **Mobile Device Information** > **Device Information** > **Mobile Device IMEISV**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Internal Storage Available**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Internal Storage Total**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Kernel Version**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Manufacturer**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Network Type**
  - **Mobile Device Information** > **Device Information** > **Mobile Device Product**
  - **Mobile Device Information** > **Device Information** > **Mobile Device SDCard 1 Available**
  - **Mobile Device Information** > **Device Information** > **Mobile Device SDCard 1 Total**
  - **Mobile Device Information** > **Device Information** > **Mobile Device SDCard 2 Available**

- **Mobile Device Information** > **Device Information** > **Mobile Device SDCard 2 Total**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Cache Available**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Cache Total**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Memory Available**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Memory Total**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Storage Available**
- **Mobile Device Information** > **Device Information** > **Mobile Device System Storage Total**
- **Mobile Device Information** > **Device Information** > **AbsoluteApps Build Number**
- **Mobile Device Information** > **Device Information** > **AbsoluteApps Version**
- **Mobile Device Information** > **Device Information** > **Record Creation Date**
- **Mobile Device Information** > **Device Information** > **MDM Profile Up-to-date**
- **Mobile Device Information** > **Installed Applications** > **Mobile Device Installed App Data Dictionary**
- **Mobile Device Information** > **Installed Applications** > **Mobile Device Managed App Status**
- **Mobile Device Information** > **Installed Applications** > **Mobile Device Managed App Prevent Data Backup**
- **Mobile Device Information** > **Installed Applications** > **Mobile Device Managed App Bound to MDM**
- **Mobile Device Information** > **Installed Applicationm Statistics** > **Mobile Device Inst. App Platform**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App OS Platform**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Is Universal**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Supported Devices**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Min OS Version**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Prevent Data Backup**
- **Mobile Device Information** > **Mobile Application Packages** > **Mobile App Remove When MDM Is Removed**
- **Mobile Device Information** > **Application Packages** > **App Prevent Data Backup**
- **Mobile Device Information** > **Application Packages** > **App Remove When MDM Is Removed**
- **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability**
- **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability Start Time**

  - **Mobile Device Information** > **iOS Configuration Profile Definitions** > **Assigned iOS Profile Availability End Time**
  - **Mobile Device Information** > **Mobile Media** (new category)
  - **Windows Reinstallation Tasks** > **AM Reinstallation Tasks** (new category)
- Renamed information items:
  - **Software Information** > **Installed Software** > **Inst. Software Version** is now **Inst. Software Version String**.
  - **Hardware Information** > **System Information** > **Apple Warranty Info** is now **Computer Warranty Info**. This item now also applies to some PCs.
  - **Hardware Information** > **System Information** > **Apple Warranty End** is now **Computer Warranty End**. This item now also applies to some PCs.
  - **Mobile Device Information** > **Device Information** > **Mobile Device IMEI** is now **Mobile Device IMEI/MEID**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Name** is now **App Name**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Category** is now **App Category**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Min OS Version** is now **App Min OS Version**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Is Universal** is now **App Is Universal**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Platform** is now **App Supported Devices**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App OS Platform** is now **App OS Platform**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Short Description** is now **App Short Description**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App Long Description** is now **App Long Description**
  - **Mobile Device Information** > **App Store Application Packages** > **App Store App URL** is now **App URL**
  - **Windows Reinstallation Tasks** > **FOG** is now **FOG Reinstallation Tasks** (category renamed)
- Other information item changes:
  - **Software Information** > **Network Adapters** > **Link Status** now also applies to some PCs.
- Various performance improvements and bug fixes.

Changes in LANrev and Absolute Manage 5.4.2 and earlier

For information on changes in LANrev and Absolute Manage 5.x, see the release notes of any Absolute Manage version up to 6.9.2

For changes in LANrev 5.0 and earlier, see the release notes of any LANrev 5.x version.