



Kaseya 2

Mobile Device Management

Quick Start Guide

Version 7.0

July 8, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Mobile Endpoints Overview

Mobile Device Management (KMDM) gives IT organizations the visibility they need to efficiently, consistently and reliably track, update and back up mobile devices. The **Mobile Device Management** module enables IT organizations to manage mobile devices from the same Kaseya IT Automation Framework used to manage desktops, laptops and servers.

A **Kaseya Agent** app is deployed to each managed device, using text messages or a web link, and serves as the agent on the mobile device. Once installed, the administrator has complete hardware and software visibility into the device, including serial number, operating system, firmware status, installed applications and other inventory data.

The proprietary nature of cellular networks and mobile devices requires the **Kaseya Agent** app to be more autonomous, saving bandwidth and ensuring executions are completed when the device isn't logged onto a network. Executions by the **Kaseya Agent** app can be triggered manually by an administrator or set to run automatically when certain thresholds or events are met.

Benefits

- Extends IT systems management policies to mobile devices, including the iPhone, iPad, Android phone, Blackberry and tablets.
- Protects business data no matter where it is located.
- Reduces help desk requests such as mobile email configuration through remote and automatic management capabilities.
- Manages all devices—from desktops and servers to mobile devices—from a single pane of glass for consistency and transparency throughout the organization.

Features

- Automates email configuration and settings to one or many devices.
- Audits each managed device, providing a detailed inventory of hardware, operating systems and applications being used.
- Tracks the location of mobile devices in real time and maintains a location history.
- Forces an alarm to sound on devices to help users locate their lost devices.
- Locks, wipes and resets lost or stolen devices.
- Backs up and restores contact lists on mobile devices.
- Sends text messages from the VSA to mobile devices.

Functions	Description
Mobile Workflow	Demonstrates workflows for a variety of module activities.
Dashboard	Provides a summary view of the status of all devices managed by the module.
Device Status	Installs and uninstalls the Mobile Device Management management app on mobile devices.
Device Summary	Schedules and runs audits of the software and hardware attributes of a selected device.
Device Messages	Creates and sends messages that display as popup messages on selected mobile devices.
Lost Devices	Marks devices as lost and initiates additional actions to

Mobile Device Management Module Requirements

	locate and recover the lost devices.
Contacts	Backs up and restores contact lists on devices.
Application Logs	Displays a log of Mobile Device Management activity.
Locate Multiple Devices	Displays the current locations of selected devices.
Track a Single Device	Displays location tracking data for a selected device.
Create Profiles	Defines configuration profiles that can be assigned to devices.
Assign Profiles	Assigns configuration profiles to selected devices.
Device Alerts	Configures alerts for devices.
Group Alerts	Configures alerts for all devices in an organization or machine group.
System Settings	Sets system options for the Mobile Device Management module.
Server Settings	Sets server options for the Mobile Device Management module.

Mobile Device Management Module Requirements

Kaseya Server

- The Mobile Device Management 7.0 module requires VSA 7.0.
- This module requires the VSA have internet access.

Requirements for Each Managed Device

- IOS 6.0 or greater
- Android 2.3 or greater
- Blackberry 6.0 or greater.
- Jailbroken devices are not supported

Note: See general **System Requirements**

(<http://help.kaseya.com/WebHelp/EN/VSA/7000000/reqs/index.asp#home.htm>).

Mobile Management Licensing

The following events affect **Mobile Device Management** license counts:

- **Mobile Device Management** devices use the same type of license used to license an agent installed on a machine.
- A license is counted as "used" after the mobile device completes its first audit, confirming that the **Kaseya Agent** app is installed.

- If the account is deleted in **Mobile Device Management**, regardless of what happens to the **Kaseya Agent** app on the device, the license changes to "unused".

Installing the Kaseya Agent App

Mobile Device Management provides two methods of creating an account and installing the **Kaseya Agent** app on a device.

- **Create an account and send an invitation** - *Used to register a single device that has a phone number.* Just after the account is created using the Device Status page, an SMS message is sent to the phone number of the device. The SMS message requests the user install the **Kaseya Agent** app on that device and provides a download link. Since the message was created and sent by a specific VSA, the user does not have to identify which VSA the **Kaseya Agent** app should check into. That information is included in the SMS message for the **Kaseya Agent** app to use when the **Kaseya Agent** app is installed. Once installed, the **Kaseya Agent** app checks into **Mobile Device Management** for the first time, completing the registration of the device. The **Kaseya Agent** app can be downloaded from one of three websites:
 - **Google Play** (<https://market.android.com/details?id=com.kaseya.mdm>)
 - **iTunes App Store** (<http://itunes.apple.com/us/app/kaseya-agent/id458392368?mt=8>)
 - **Blackberry App World** (<http://appworld.blackberry.com/webstore/content/69915/>)
- **Send an email with the server ID** - *Used to register multiple devices, whether or not the devices have phone numbers.* The advantage of this method is that the VSA user does not have to manually create each account in advance. A unique server ID is generated for each **Mobile Device Management** module, the first time it is installed on a VSA. The server ID is identified on the System Settings page. The VSA user must create an email with instructions for downloading the **Kaseya Agent** app on to a device. The instructions must include the download link and the unique server ID the user enters just after the **Kaseya Agent** app is installed on the device. Once the server ID is entered, the **Kaseya Agent** app checks in for the first time, creating the account in the **Mobile Device Management** module, completing the registration of the device. The email message can be as simple as: Click here to install the Kaseya Agent app:
`https://mobile.kaseya.com/vsaws/v1 Use this registration code:
<yourServerID>"`

First Time Check-In

The first time the **Kaseya Agent** app checks in, the following tasks are performed on the device.

- An audit of hardware settings
- An audit of all apps installed on the device
- All device settings are retrieved
- A **Get Current Location** command is executed, if permitted by the device

Note: See **Manually Deploying the Mobile Device Management App to BlackBerry 5.x Devices**
 (<http://help.kaseya.com/WebHelp/en/KMDM/7000000/kmdm-blackberry70.pdf#zoom=70&navpanes=0>)

Agentless Installs

Mobile Device Management can manage iOS devices without installing the Kaseya Agent app on the iOS devices. Instead a certificate is installed on the device. The certificate gives the **Mobile Device Management** permission to send commands to the iOS device. The iOS acts on the commands sent by **Mobile Device Management** using functionality native to the iOS operating system rather than

Communicating with Devices

relying on an installed agent.

You can customize the messages sent to invite iOS users to perform an *agentless install*, using the System settings page.

Communicating with Devices





For the most part, communication between the **Mobile Device Management** module and the devices they manage are transparent for both device users and VSA users. The VSA user should be aware of the following concepts when sending commands to devices.

Command Processing

1. Commands are queued for a device and kept on the server.
2. When the **Kaseya Agent** app on a device checks in, the device processes every command in the queue.
3. Check-ins occur at set intervals, unless an immediate check-in is requested by a VSA user.
4. If a VSA user requests an immediate check-in for a device, a message is sent requesting the device user open the **Kaseya Agent** app on the device, causing the **Kaseya Agent** app to check-in immediately.

Command Status

Clicking the **Command Status** button on the Device Status page displays the status of each command sent to a device, past or pending. A command can be in the following states:

-  - The command is pending. The agent has not checked-in to retrieve it.
-  - The agent is processing the command.
-  - The operation is complete.
-  - Command failed.

Agent Check-in Interval

By default a device checks into **Mobile Device Management** every 720 minutes (12 hours). When checking in, any tracking data collected since the last check-in is sent to the server. Any commands queued on the server are also sent to the device. Some commands may be pushed to the device immediately for devices that support push functionality, such as iOS devices.

Requesting an Immediate Agent Check-in

You can request any device—iOS or Android—to check-in immediately. Clicking the **Request Checkin** button on the Device Status page:

- For iOS, sends a message through AppleMDM that appears on the device's screen.
- For Android, sends a text message to the device.

In both cases the user of the device is instructed to tap the icon on the **Kaseya Agent** app to open it. Opening the **Kaseya Agent** app causes the app agent to check in immediately.

Conserving Battery Life of Devices

Turning device tracking off contributes the most to conserving the battery life of devices. Setting the agent check-in interval to a longer interval will also conserve the battery life of devices.

VSAs Without an Internet Connection

Mobile Device Management is not supported on private VSA networks.

Managing Lost Devices

The **Lost Devices** page marks a device as lost or found and sets the actions that can be taken. Actions include:

- **Mark Device as Lost** - Marks selected devices as lost.
- **Mark Device as Found** - Marks selected devices as found.
- **Send Message** - Sends a message to the device.
- **Lock Device** - If checked, the device is locked, preventing user access.
- **Sound Alarm on Device** - If checked, the device repeatedly says "This phone is stolen." whenever it is turned on. This alarm can be disabled by wiping the device.
- **Wipe Device** - If checked, the device is reset back to its default settings. Wiping a device deletes all user data, including the management app (agent) Kaseya Agent app. The Kaseya Agent app can no longer check-in after wiping the device.
- **Clear Passcode** - Resets passcodes on managed iOS devices. A reset unlocks the device, allowing the user to either use the device with no passcode or to set a new passcode. Clearing the passcode does not change the underlying security profile. If the device is configured to require a passcode, the user is immediately prompted to enter a new one.

Backing Up and Restoring Device Contact Lists

The **Contacts** page backs up and restores the contact lists of devices. If a device is lost or stolen, the contact list can be restored to a new device. A contact list may also need to be restored to an existing device if the device is wiped (reset) and all user data is deleted. The contact information returned by a selected backup displays on the right side of the **Contacts** page. If multiple backups exist, you can select the backup to display.

Tracking the Locations of Devices

A location history is maintained for each device that returns location data. **Mobile Device Management** provides two methods of collecting location data for devices.

- **Get Current Location** - If you only need to know the location of a device "on demand" then select a device and click the **Get Current Location** button. This button is available on the Device Status, Locate Multiple Devices and Track a Single Device pages.
- **Enable Tracking** - When tracking is enabled for a device, the device keeps a log of its movements from one location to next. *Location entries are filtered*, based on the parameters specified for the device by its Device Location and Tracking Profile.









*Real time tracking is not supported. A filtered set of location data points is uploaded to the **Mobile Device Management** module only when the **Kaseya Agent** app on the device checks in.* Whichever method of location data collection you choose, the results are displayed on a map using the following two pages:

- Locate Multiple Devices
- Track a Single Device

Managing Devices Using Profiles

The [Create Profiles](#) page defines configuration profiles. Profiles determine how devices are configured and managed using **Mobile Device Management**. Each profile represents a different set of options. Changes to a profile affect all devices assigned that profile. A profile is assigned to devices using Mobile > Assign Profiles.

Types of Profiles

- Email Profile  - Configures the email client on a managed mobile device. Currently applies only to iOS devices. Multiple profiles of this type can be assigned to the same device.
- Security Profile  - Configures policies related to the creation of PINs. PINs are used by a device users to unlock their devices.
- Web Clip Profile  - Specifies a web application "shortcut" to a URL that the device can access. Currently applies only to iOS devices. Multiple profiles of this type can be assigned to the same device.
- iOS 4 Device Feature Profile  - Applies to iOS devices earlier than iOS 5. Enables and disables popular features on iOS 4 devices.
- iOS Device Feature Profile  - Applies to iOS5, iOS6, iOS7 only. Enables and disables popular features on iOS devices.
- Device Location and Tracking Profile  - Sets check-in and location options on devices. This is the only profile that applies to Blackberries.
- Custom iOS Configuration Profile  - A profile generated using Apple's **iPhone Configuration Utility** (<http://support.apple.com/kb/DL1466>) and imported into **Mobile Device Management**.
- WiFi Profile  - Sets WiFi options on devices. Multiple profiles of this type can be assigned to the same device.

Uninstalling the Kaseya Agent App

If the device account in the VSA is deleted, you must delete the Kaseya Agent app on the device manually.

Deleting the Kaseya Agent app Manually from the Device

Android

1. On the device, go to **Settings > Location & Security**.
2. Locate and press **Select device administrators**.
3. Uncheck **Kaseya Agent**.
4. When prompted, press **Deactivate**. Click **Ok** to confirm the deactivation.
5. Go to **Settings > Applications > Manage Applications** and click **Kaseya Agent**.
6. When prompted, press **Uninstall** to remove the app. Click **Ok** to confirm the uninstall.

iOS

Applies to iPad, iPod, iTouch and iPhone

1. On the device, locate the icon of the **Kaseya Agent** app.
2. Tap and hold down the icon. After a few moments, the icon will start to "wobble" and an **X** will appear next to each of the app.

3. Tap the **X** next to the icon.
4. When prompted, select **Delete** to remove the app.

Managing Apps on Devices

Mobile Device Management can require or disallow apps on mobile devices. App profiles determine which apps are required to be installed or disallowed from being installed on mobile devices. Each app profile represents a different set of apps. All apps belonging to the same app profile are either all required or all disallowed. You can assign multiple app profiles to a single mobile device. Changes to an app profile affect all devices assigned that app profile. Supports the management of apps downloaded from app stores as well as proprietary *enterprise apps*.

- The App Profiles page specifies the apps belonging to each app profile and whether they are required or disallowed.
- An app profile is assigned to managed mobile devices using Assign App Profiles page.
- The App Catalog page maintains a catalog of *app items*. An app item is a record that uniquely identifies a single app that can be required or disallowed on a mobile device.
- The App Inventory page generates a list of app items based on an audit of all mobile devices managed by **Mobile Device Management**. Rather than specify app items manually in the **App Catalog**, you can use this page to add an automatically created app item to the **App Catalog**.
- An **App Compliance** tab displays on the **Device Summary** page. The tabs shows all required apps missing from the device and all disallowed apps installed on the device. An **Application** tab shows all apps on the device regardless of their compliance status.
- Two alerts tabs on the Device Alerts page can notify you about app compliance: **Disallowed Apps** and **Required Apps**.
- You can customize the messages sent to invite users to install a required app, using the System Settings page.
- App management is supported by two options on the Server Settings page: **Retention Time for App Invite Logs** and **Threshold for Resending App Invites**.

Module Settings

Two pages define settings for the entire **Mobile Device Management** module.

- System Settings - Provides default settings for profiles created using the Create Profiles page.
- Server Settings - Sets settings that apply to the **Mobile Device Management** server or the entire **Mobile Device Management** module.

Alerts

Mobile Device Management provides three general types of alerts.

- **Device Alerts** - Device-specific alerts include:
 - **Device Offline** - The device has failed to check-in a specified number of minutes.
 - **Lost Device Checks In** - A device checks in after being marked as lost.
 - **Device Checks In** - A device checks in.
 - **Prompt Agent** - Prompts the user of the device, after the device has failed to check in a specified number of minutes. Applies to iOS only.

Logs

- **Group Alerts** - Creates an alert when a new device joins a specified organization or machine group.
- **System Alerts** - Creates an alert when a specified number of unused device licenses are available.

When a **Mobile Device Management** alert is enabled and the alert condition occurs, options include sending an email or creating a ticket.

Note: Alarms and the running of agent procedures are not supported for mobile device-based alerts.

Logs

Two logs are maintained by **Mobile Device Management**

- **Application Log** - The Application Logs page displays a log entry of every VSA user action performed in the **Mobile Device Management** module. System events triggered by the **Mobile Device Management** module itself are not included.
- **Device Log** - *The device log is for Kaseya support purposes only.* The device log shows the actual messages sent back and forth between the VSA and a selected device. Since service providers do not require this information, device logs do not display for a selected device unless the **Request Log** button is clicked on the Device Summary page. Device log entries then display in the **Logs** tab. Clicking the **View Log Detail** button for a selected log entry displays the text of the message.

Note: Mobile-device based events and logs do not display anywhere else in the VSA.

Reports

The following reports are provided with **Mobile Device Management**. Each report can be sorted and filtered by several columns of information.

- **Device Applications** - Lists the applications installed on each device.
- **Device Status** - Lists the status of each device.
- **Device Summary** - Lists audit information for each device.
- **Lost Devices** - Lists all lost devices and the actions taken on those lost devices.