



---

# **Mobile Device Management**

---

**User Guide**

Version R95

English

February 4, 2021

## **Copyright 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."

# Contents



# Contents

Mobile Device Management Overview .....	i
Mobile Device Management Module Minimum Requirements .....	ii
Mobile Management Licensing .....	iii
Installing the Kaseya Agent App.....	iii
Agentless Installs .....	iii
Communicating with Devices.....	iv
Managing Lost Devices.....	v
Backing Up and Restoring Device Contact Lists .....	v
Tracking the Locations of Devices .....	v
Managing Devices Using Profiles .....	v
Uninstalling the Kaseya Agent App.....	vi
Managing Apps on Devices .....	vii
Module Settings .....	vii
Alerts.....	vii
Logs .....	viii
Reports .....	viii
Mobile Workflow .....	viii
Dashboard.....	ix
Device Status .....	ix
Device Summary.....	xii
Device Messages.....	xvi
Lost Devices .....	xvii
Contacts .....	xviii
Application Logs .....	xix
Locate Multiple Devices.....	xx
Track a Single Device.....	xxi
App Profiles .....	xxiii
New / Edit App Profile .....	xxiv
Assign App Profiles .....	xxiv
App Catalog .....	xxv
Add / Edit Master App Catalog Item.....	xxv
App Inventory .....	xxvi
Create Profiles .....	xxvi
Email Profile .....	xxvii
Security Profile .....	xxviii
Web Clip Profile .....	xxix
iOS 4 Device Feature Profile.....	xxix
iOS Device Feature Profile.....	xxix
Custom iOS Configuration Profile .....	xxx

**Mobile Device Management Overview**

**Device Location and Tracking Profile .....xxxi**  
**WiFi Profile .....xxxii**  
**Assign Profiles .....xxxiii**  
**Device Alerts.....xxxiv**  
**Group Alerts.....xxxviii**  
**System Settings.....xxxix**  
**Server Settings .....xxxix**  
**Mobile Device Management Reports .....xl**  
**Mobile Devices - Device Applications .....xli**  
**Mobile Devices - Device Status.....xlii**  
**Mobile Devices - Device Summary .....xlii**  
**Mobile Devices - Lost Devices .....xliii**  
**Index .....45**

---

# Mobile Device Management Overview

**Note:** The Mobile Device Management R95 module requires SaaS VSA R95. On premises VSA environments uninstall Mobile Device Management on upgrade and install the new Enterprise Mobility Management module in its place.

**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
<b>Mobile Workflow</b> (page viii)	Demonstrates workflows for a variety of module activities.
<b>Dashboard</b> (page ix)	Provides a summary view of the status of all devices managed by the module.
<b>Device Status</b> (page ix)	Installs and uninstalls the Mobile Device Management management app on mobile devices.
<b>Device Summary</b> (page xii)	Schedules and runs audits of the software and hardware attributes of a selected device.
<b>Device Messages</b> (page )	Creates and sends messages that display as popup

<i>xvi)</i>	messages on selected mobile devices.
<b>Lost Devices</b> ( <i>page xxxii</i> )	Marks devices as lost and initiates additional actions to locate and recover the lost devices.
<b>Contacts</b> ( <i>page xviii</i> )	Backs up and restores contact lists on devices.
<b>Application Logs</b> ( <i>page xix</i> )	Displays a log of Mobile Device Management activity.
<b>Locate Multiple Devices</b> ( <i>page xx</i> )	Displays the current locations of selected devices.
<b>Track a Single Device</b> ( <i>page xxi</i> )	Displays location tracking data for a selected device.
<b>Create Profiles</b> ( <i>page xxvi</i> )	Defines configuration profiles that can be assigned to devices.
<b>Assign Profiles</b> ( <i>page xxxiii</i> )	Assigns configuration profiles to selected devices.
<b>Device Alerts</b> ( <i>page xxxiii</i> )	Configures alerts for devices.
<b>Group Alerts</b> ( <i>page xxxiv</i> )	Configures alerts for all devices in an organization or machine group.
<b>System Settings</b> ( <i>page xxxix</i> )	Sets system options for the Mobile Device Management module.
<b>Server Settings</b> ( <i>page xxxix</i> )	Sets server options for the Mobile Device Management module.

## Mobile Device Management Module Minimum Requirements

### Kaseya Server

- The Mobile Device Management R95 module requires SaaS VSA R95.

**Note:** On premises VSA environments uninstall Mobile Device Management on upgrade and install the new Enterprise Mobility Management module in its place.

- This module requires the VSA have internet access.

### Requirements for Each Managed Device

- IOS 6.0.x, 6.1.x, 7.0.x, 7.1.x, 8.0.x, 8.1.x, 8.2, 8.3, 8.4.x, 9.0.x, 9.1, 9.2.x, 9.3.x, 10.0.x, 10.1, 10.2.x, 10.3.x and 11.0.x, 11.1.x, 11.2.x, 11.3.x, 11.4.x
- 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/9050000/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 ix) 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 xxxix) 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

---

# 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 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 xxxix) 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 ix) 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 ix) 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** (page ix), **Locate Multiple Devices** (page xx) and **Track a Single Device** (page xxi) pages.
- **Enable Tracking** - When tracking is enabled for a device, the device keeps of 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** (page xxix).

*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** (page xx)
- **Track a Single Device** (page xxi)









---

## Managing Devices Using Profiles

The **Create Profiles** pages 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** (page xxxiii).

### Types of Profiles

- **Email Profile** (page xxvii)  - 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** (page xxviii)  - Configures policies related to the creation of PINs. PINs are used by a device users to unlock their devices.
- **Web Clip Profile** (page xxix)  - 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** (page xxix)  - Applies to iOS devices earlier than iOS 5. Enables and disables popular features on iOS 4 devices.
- **iOS Device Feature Profile** (page xxix)  - Applies to iOS5, iOS6, iOS7 only. Enables and disables popular features on iOS devices.
- **Device Location and Tracking Profile** (page xxxi)  - Sets check-in and location options on devices. This is the only profile that applies to Blackberries.
- **Custom iOS Configuration Profile** (page xxxi)  - A profile generated using Apple's **iPhone Configuration Utility** (<https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>) and imported into **Mobile Device Management**.
- **WiFi Profile** (page xxxii)  - 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 "wiggle" 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 xxiii) 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 xxiv) page.
- The **App Catalog** (page xxv) 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 xxvi) 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 xxxiv) 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 xxxix) page.
- App management is supported by two options on the **Server Settings** (page xxxix) 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** (page xxxix) - Provides default settings for profiles created using the **Create Profiles** (page xxvi) page.
- **Server Settings** (page xxxix) - 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.
- **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 xix*) 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 xii*) 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.

---

## Mobile Workflow

**Mobile > Operations > Mobile Workflow**

The **Mobile Workflow** page provides a summary view of the workflows for configuring and operating mobile devices using **Mobile Device Management**. Help links are provided for each item shown in the flow chart to provide more information.

- **Individual Deployment** - Create a single **Mobile Device Management** account for a device and initiate the installation of the **Kaseya Agent** app on 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/>)
- **Bulk Deployment** - Send an email with the unique server ID. Users can use the email to install **Kaseya Agent** app on their devices. When the agent checks-in for the first time, the **Mobile Device Management** account is created. See **Installing the Kaseya Agent App** (*page iii*) for a description of bulk deployments.
- **Email Configuration** - Applies only to iOS in version 1.1. Configure and install a separate email client app on the managed device.
- **Audit** - Perform an audit of the software and hardware attributes of the managed device.



- **Tracking** - Track the location of the device.
- **Lost and Found** - Mark a device as lost or found. A lost device can be locked, sent a message, sound an alarm, or wiped. The passcode can be cleared on an iOS devices.
- **Backup** - Backup and restore the contact list of a device.

---

## Dashboard

Mobile > Operations > Dashboard

The **Dashboard** page provides a summary view of the status and properties of all devices managed using **Mobile Device Management**. Using the device ID/group ID filter at the top of page affects the statistics displayed. Pie charts show the percentage and device counts for each status or property charted. Hover the cursor over any pie slice to emphasize an individual percentage and device count.

- **Device Status** - Normal, Command Pending, Invited
- **Device Manufacturer** - The manufacturer of the device.
- **Device Current Carrier** - The carrier currently being used by the device.
- **Device OS** - The operating system used by the device.
- **Device Home Carrier** - The home carrier used by the device.
- **Lost Devices** - Not lost, Lost, Wiped

---

## Device Status

Mobile > Operations > Device Status

The **Device Status** page creates and deletes **Mobile Device Management** accounts for mobile devices. It also initiates the installation and uninstallation of the Kaseya Agent app on mobile devices. Multiple **Mobile Device Management** accounts can be created by importing data. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.

### Actions





- **New** - Creates a **Mobile Device Management** account for a mobile device. A message is sent to the device, requesting the user install the Kaseya Agent app on that device. Once installed, the management app checks into **Mobile Device Management**, completing the registration.
  - **Country Code** - Enter the country code.
  - **Phone Number** - Enter the phone number.
  - **Name** - Enter a device name. This name identifies the mobile device throughout the VSA. Similar to creating a machine ID account name for a computer in the VSA.
  - **Owner** - The owner of the mobile device.
  - **Email Address** - An email address associated with this device, for reference purposes only.
  - **Email Account** - The email account associated with an email address.
  - **Group** - The VSA machine group the device is a member of.

**Note:** See **Installing the Kaseya Agent App** (page iii) for a description of *bulk deployments*.












- **Enrollment Type**
  - ✓ **iOS Agentless** - See **Agentless Installs** (page iii).
  - ✓ **iOS, Android or Blackberry Agent** - See **Installing the Kaseya Agent App** (page iii).
- **Invitation Via**
  - ✓ **SMS** - Typically used with phone devices.

- ✓ **Email** - Typically used with tablet devices.
- ✓ **Email including Android App** - For Android devices only, includes the Kaseya Agent app as an attachment in the email invitation, rather than downloading the app from a URL.




**Note:** The **Device Invitation Message** field on the **System Settings** (page xxxix) page specifies the text of the invitation message.

- **Resend Invitation** - Resends the message inviting the user to install the Kaseya Agent app on the user's mobile device.
- **Edit** - Changes the account information associated with a mobile device. See **New** above.
- **Delete** - Deletes selected accounts.
- **Import** - Creates **Mobile Device Management** accounts for devices by importing formatted data from an edit text box. Each line of the imported text must have the following format:  
first,last,phone number
- **Command Status** - Shows the status of commands sent to a device.
  -  - 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.
- **Get Current Location** - Returns the current location of the device, on demand, without continuously tracking its location. The last location of a device—either from a **Get Current Location** command—or if tracking is started, is shown on a map using **Locate Multiple Devices** (page xx).
- **Start Tracking** - Starts location tracking of the device. Once started, you can view the tracking of the device on a map using **Track a Single Device** (page xxi).
- **Stop Tracking** - Stops location tracking of the device.
- **Location History** - Displays the location history of a device. Location data is returned by both **Get Current Location** commands and by tracking the device.
- **Request Checkin** - 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.
  - For IOS, a message is sent through AppleMDM that appears on the device's screen.
  - For Android, an SMS message is sent to the device.
- **Refresh** - Refreshes the page.

### Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing



-  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - Blackberry
- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **Device.GroupID** - The device identifier and machine group. Click **Edit** on the **Device Status** (*page ix*) page to change this value.
- **Owner** - The owner of the device. Click **Edit** on the **Device Status** (*page ix*) page to change this value.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers. Click **Edit** on the **Device Status** (*page ix*) page to change this value.
- **OS Version** - The version of operating system used by the device.
- **Last Check-in** - The date/time the Kaseya Agent app on the device last checked into **Mobile Device Management**.
- **KMDM Version** - The version of the Kaseya Agent app on the device.
- **Timezone** - The timezone used by the device.
- **Last Latitude** - The last latitude returned by the device.
- **Last Longitude** - The last longitude returned by the device.
- **Last Audit** - The date/time of the latest audit.
- **Next Audit** - The date/time the next audit is scheduled.
- **First Check-in** - The date/time the management app first checked into **Mobile Device Management**.
- **Email Address** - The email address associated with the device, for reference purposes only. Click **Edit** on the **Device Status** (*page ix*) page to change this value.
- **Email Account Name** - The email account associated with an email address.
- **Build** - The build number of the operating system used by the device.
- **Manufacturer** - The manufacturer of the device hardware.
- **Model name** - The model name of the device hardware.
- **Model** - The model number of the device hardware.
- **Radio version** - The version of modem firmware used by the device. Also called the "baseband" version.
- **Internal total** - The total memory available and built into the hardware.
- **External total** - The total memory available externally.
- **Internal free** - Free memory available and built into the hardware.
- **External free** - Free memory available externally.
- **Serial** - The serial number of the device.
- **IMEI** - The unique identifier of the device's main assembly, independent of the SIM card plugged into the device. The IMEI number applies to GSM, WCDMA and iDEN mobile phones.
- **ICC** - The unique identifier of the SIM card plugged into a device.
- **Data roaming** - True or False.
- **WiFi MAC** - The MAC ID of the device.
- **Home carrier** - The main service provider of the device.

- **Home MCC** - The home mobile country code of the device. Large countries can have more than one mobile country code.
- **Home MNC** - The mobile network code for the home operator/carrier of the device.
- **Current carrier** - The carrier currently being used by the device.
- **Current MCC** - The mobile country code currently being used by the device.
- **Current MNC** - The mobile network code of the operator/carrier currently being used by the device.

---

## Device Summary




### Mobile > Operations > Device Summary












The **Device Summary** page schedules and runs audits of the software and hardware attributes of a selected device. All audit information collected for a single, selected device displays on multiple tabs in the lower pane on this page. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.

### Actions




- **Schedule Audit** - Schedules an audit for a specified time for a selected device. Schedule once or periodically. Each type of recurrence—Once, Hourly, Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence. Options can include:
  - **Schedule will be based on the timezone of the agent (rather than server)** - If checked, time settings set in the Scheduler dialog reference the local time on the agent machine to determine when to run this task. If blank, time settings reference server time, based on the server time option selected in System > Preferences. Defaults from the System > Default Settings page.
  - **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading. For example, if the scheduled time for a task is 3:00 AM, and the distribution window is 1 hour, then the task schedule will be changed to run at a random time between 3:00 AM and 4:00 AM.
  - **Skip if offline** - If checked and the machine is offline, skip and run the next scheduled period and time. If blank and the machine is offline, run the task as soon as the machine is online again. Applies only to recurring schedules, a 'Once' schedule always executes the next time the agent is online.
  - **Exclude the following time range** - **Applies only to the distribution window.** If checked, specifies a time range to exclude the scheduling of a task within the distribution window. Specifying a time range outside of the distribution window is ignored by the scheduler.
- **Run Audit Now** - Runs an audit of a selected device.
- **Request Logs** - *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.
- **Refresh** - Refreshes the page.

### Table Columns



- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.

-  - Invitation rejected
-  - Installing
-  - Install failed
-  - Normal - The app is installed and working normally.
-  - Command pending
-  - Command sent
-  - Unresponsive
-  - Processing
-  - Command sent - retry
-  - Opt out
-  - Command sent - failed

- **(Device OS)**

-  - Android
-  - Apple
-  - BlackBerry

- **Track**

-  - Tracking has started and the device is checking in.
-  - Tracking is pending and will start when the device checks-in.
- (blank) - Tracking is not enabled.

- **Device.GroupID** - The device identifier and machine group. Click **Edit** on the **Device Status** (page ix) page to change this value.
- **Last Check-in** - The date/time the Kaseya Agent app on the device last checked into **Mobile Device Management**.
- **Last Audit** - The date/time of the latest audit.
- **Next Audit** - The date/time the next audit is scheduled.
- **First Check-In** - The date/time the management app first checked into **Mobile Device Management**.
- **Email Address** - The email address associated with the device. for reference purposes only. Click **Edit** on the **Device Status** (page ix) page to change this value.

See the *General tab* section below for all other field definitions.

## General tab

### Operating System

- **Type** - The type of operating system on the device.
- **OS Version** - The version of operating system used by the device.
- **Build** - The build number of the operating system.

### Device Information

- **Name** - The name the device uses to identify itself. Click **Edit** on the **Device Status** (page ix) page to change this value.
- **Agent ID** - The Kaseya agent GUID.
- **Device Identifier** - A unique identifier assigned to the device by the manufacturer. Click **Edit** on the **Device Status** (page ix) page to change this value.
- **Serial** - The serial number of the device.

- **IMEI** - The unique identifier of the device's main assembly, independent of the SIM card plugged into the device. The IMEI number applies to GSM, WCDMA and iDEN mobile phones.
- **ICC** - The unique identifier of the SIM card plugged into a device.
- **KMDM Version** - The version of the **Kaseya Agent** app on the device.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers. Click **Edit** on the **Device Status** (*page ix*) page to change this value.
- **Data roaming** - True or False.
- **WiFi MAC** - The MAC ID of the device.

#### Location

- **Timezone** - The timezone used by the device.
- **Last Latitude** - The last latitude returned by the device.
- **Last Longitude** - The last longitude returned by the device.

#### Platform

- **Manufacturer** - The manufacturer of the device hardware.
- **Model name** - The model name of the device hardware.
- **Model** - The model number of the device hardware.
- **Radio version** - The version of modem firmware used by the device. Also called the "baseband" version.
- **Internal total** - The total memory available and built into the hardware.
- **External total** - The total memory available externally.
- **Internal free** - Free memory available and built into the hardware.
- **External free** - Free memory available externally.

#### Home network

- **Home carrier** - The main service provider of the device.
- **Home MCC** - The home mobile country code of the device. Large countries can have more than one mobile country code.
- **Home MNC** - The mobile network code for the home operator/carrier of the device.

#### Current network

- **Current carrier** - The carrier currently being used by the device.
- **Current MCC** - The mobile country code currently being used by the device.
- **Current MNC** - The mobile network code of the operator/carrier currently being used by the device.

### Settings tab

These device settings are set by assigning a **Device Location and Tracking Profile** (*page xxxi*) to a device.

- **Checkin Only When Connected to WiFi** - If checked, the Kaseya Agent app checks in only if a WiFi connection is available. If unchecked, the Kaseya App, will check in by cell phone network if a WiFi connection is not available.
- **Track Device** - If checked, tracking is enabled. Location data is filtered against a number or predefined parameters to ensure that only accurate and useful location data is actually sent to the VSA. *Recorded location data is only sent to the VSA when the agent next checks in.* The following general criteria is used -
  - **Accuracy** - Each location update received from a GPS tower or satellite has an accuracy rating, estimating the confidence GPS source has in the accuracy of the location data.

- **Age** - A device caches location data and may at times pass old location data to the **Kaseya Agent** app if a new location update has not recently been received.
- **Distance traveled** - The distance the device has moved since the previous location update. This could be zero if the device has not moved.
- **Agent Check-in Time (minutes)** - *This field is ignored by agents installed using Kaseya Agent app version 1.1 and later.* Sets the minimum time between check-in attempts. A number of environmental and device operating factors govern exactly when check-in takes place. The lower this value the more battery power is consumed.
- **Tracking Accuracy (meters)** - This value is passed to the GPS receiver as a hint for how accurate the location information pass through should be. The more accurate the request, a lower value, the longer it takes to get the location and more power used.
- **Minimum Accuracy Before Ignore (meters)** - This value controls what location information is considered useful enough to send to the VSA and save. When a device is moving quickly—in a car or train for example—location tracking information becomes less accurate and, at some point, is no longer useful. Location points that are less accurate than this value are filtered out and are not recorded or sent to the VSA. This value more than any other governs the quantity and quality of the location info send from the device.
- **Tracking Movement Distance** - This value defines the minimum distance the device must move, in meters, for a location update event to be triggered and sent to the agent. It also is used by the agent to decide if the location point should be recorded and sent to the VSA. For example if this value is set for 500 meters and the device only moves 10 meters then the agent does not record this point, unless the **Minimum / Maximum Tracking Time (minutes)** allows it.
- **Minimum / Maximum Tracking Time (minutes)** - These values define how frequently location information points should be recorded. The minimum value defines the minimum time between points. For example if the value is 10 minutes then the location info reported to the agent is not recorded nor sent to the VSA for at least 10 minutes from the last time a good location was reported. However if a good location point has not be recorded within the time period governed by the maximum value, then regardless of accuracy or distance traveled, this point *is* recorded.

*An example of recording a point:*

- A point is requested at the appropriate tracking accuracy.
- If the point returned is has an accuracy value greater than specified in minimum accuracy before ignore, the point is discarded.
- If the device has not moved at least the distance specified in tracking movement distance the point is discarded.
- If the time elapsed between this point and the previous one recorded is less than the minimum tracking time, the point is discarded.
- If the time between this point and the previous one recorded is greater than the maximum tracking time, then the point is recorded, even if the previous checks would have discarded it.

## Applications tab



The **Applications** tab displays a list of the apps installed on the selected managed mobile device.

## App Compliance tab

The **App Compliance** tab shows two app compliance lists for a selected mobile device. See **Managing Apps on Devices** (*page vii*) for more information.

- **Required Apps Missing from Device**
- **Disallowed Apps Installed on Device**

*Table Columns*

- **(App Type)**
  - **Store App** -  - If selected, a **URL** must be specified.
  - **Enterprise App** -  - If selected, an **App Binary** must be specified.

- **Package Name** - The full name of the app in reverse-domain format. Example: `com.kaseya.enterprise.agent`.
- **App Name** - The friendly name of the app. Example: Agent.
- **Version** - The application version number. Example: `1.2.0.0`.
- **Invite Last Sent** - The date/time an invitation to install this app was last sent to the mobile device.

### Logs tab

The **Logs** tab displays device log entries. *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.

## Device Messages
















Mobile > Operations > Device Messages

The **Device Messages** page creates and sends messages that display as popup messages on selected mobile devices. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.

### Actions

- **Send Message** - Displays a dialog you can use to enter a text message. Click the dialog's **Send Message** button to send the message to a selected device.
- **Resend Message** - Resends a selected message.
- **Remove** - Removes a selected message.
- **Refresh** - Refreshes the page.

### Device Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing
  -  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android



- Apple



- BlackBerry

- **Device.GroupID** - The device identifier and machine group.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Owner** - The owner of the device.

### Message Table Columns

- **Direction of Message** -
  - Sent from the device.
  - Sent from the VSA administrator.
- **Message Date** - Date/time of the message.
- **From** - *Applies to device messages only.* The device identifier and machine group.
- **Message** - Text of the message.

## Lost Devices

Mobile > Operations > Lost Devices

The **Lost Devices** page marks a device as lost or found and sets the actions to be taken if a device is lost or stolen. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.













### Actions

- **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 Stolen 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.
- **Refresh** - Refreshes the page.

### Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  - Created
  - Invitation failed
  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  - Invitation rejected
  - Installing
  - Install failed
  - Normal - The app is installed and working normally.



-  - Command pending
-  - Command sent
-  - Unresponsive
-  - Processing
-  - Command sent - retry
-  - Opt out
-  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - Blackberry
- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **Device.GroupID** - The device identifier and machine group.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Lost** - If checked, the device has been marked as lost or stolen.
- **Wipe** - If checked, the phone has been wiped (reset) back to its default settings. Wiping a device deletes all user data.
- **Lock** - If checked, the device is locked, preventing user access.
- **Sound Alarm** - If checked, the device repeatedly says "This phone is stolen." whenever it is turned on, unless the phone wiped (reset) back to its default settings. Wiping a device deletes all user data.

---

## Contacts

### Mobile > Operations > Contacts

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. If multiple backups exist, you can select the backup to display. When a backup is selected, the names of the contacts are listed on the right side of the page. Clicking a name displays the available information for that contact: emails, addresses, phone numbers and notes. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.




















### Actions

- **Backup Now** - Backs up contacts list of selected device immediately.
- **Restore** - Restores contact lists of selected devices. A dialog displays so you can select the backup you want to restore.
- **Delete** - Deletes contact list backups of selected devices.
- **Refresh** - Refreshes the page.
- **Backup** - Selects the contacts to display on the right side of the page.

### Device Tables Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.



-  - Created
-  - Invitation failed
-  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
-  - Invitation rejected
-  - Installing
-  - Install failed
-  - Normal - The app is installed and working normally.
-  - Command pending
-  - Command sent
-  - Unresponsive
-  - Processing
-  - Command sent - retry
-  - Opt out
-  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - BlackBerry
- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **Device.GroupID** - The device identifier and machine group.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Number of Backups** - Number of backups created.
- **Date of Latest Backup** - Date/time of latest backup.
- **Date of Latest Restore** - Date/time of latest restore.

---

## Application Logs

Mobile > Operations > Application Logs

The **Application Logs** page displays a log of **Mobile Device Management** application activity by:

- **Event ID**
- **Event Name**
- **Message**
- **Admin**
- **Event Date**

If information has changed or been removed unexpectedly, check this page to determine what events and administrators may have been involved.

This table supports **selectable columns, column sorting, column filtering and flexible column widths** (<http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#6875.htm>).

Logged events include:

Backup Device  
 Change Server Settings  
 Change System Settings  
 Clear Passcode  
 Create Device  
 Created Device  
 Delete Profile  
 Deleted Device  
 Found Device  
 Found Device  
 Invitation resent  
 Lock Device  
 Lost Device  
 Mark Commands Complete  
 Process Alert  
 Request Checkin  
 Request Checkin  
 Request Logs  
 Restore Device  
 Run Audit  
 Scheduled Audit  
 Sound Alarm on Device  
 Start Tracking Device  
 Stop Tracking Device  
 Updated Device  
 Wipe Device

---

## Locate Multiple Devices

### Mobile > Location > Locate Multiple Devices

The **Locate Multiple Devices** page displays the current location of one or more selected devices on a map. Each numbered marker on the map references a numbered list on the right side of the map. The numbered list identifies the name of each device, its phone number, and when each device last identified its location. The display of data is filtered by a specified start date and time. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.

**Note:** If you don't see a location marker for a device you're tracking, try resetting the filter to display an earlier date range.

### Actions




















- **Get Current Location** - Returns the current location of the device, on demand, without continuously tracking its location. The last location of a device—either from a **Get Current Location** command—or if tracking is started, is shown on a map using **Locate Multiple Devices** (page xx).
- **Start Tracking** - Starts location tracking of the device. Once started, you can view the tracking of the device on a map using **Track a Single Device** (page xxi).
- **Stop Tracking** - Stops location tracking of the device.
- **Location History** - Displays the location history of a device. Location data is returned by both **Get Current Location** commands and by tracking the device.

### Using the Map

1. Select one or more devices in the middle pane.

2. **Date and Time** - Optionally change the date and time filter. The filter limits the display of device locations to later than a specified start date and time.
3. **Refresh** - Refresh the map after resetting the **Date and Time** filter.

### Device Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing
  -  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - BlackBerry
- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **Data** - If checked, device has location data.
- **Device.GroupID** - The device identifier and machine group.
- **Phone** - The phone number of the device.
- **Owner** - The owner of the device.
- **Count** - Number of locations tracked.

---

## Track a Single Device

### Mobile > Location > Track a Single Device

The **Track a Single Device** page displays location tracking data for a selected device. Each numbered marker on the map references a numbered list on the right side of the map. The numbered list identifies the date and time the device was at that location. The display of data is filtered by a specified range of dates and times. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.

**Note:** If you don't see a location marker for a device you're tracking, try resetting the filter to display an earlier date range.




















## Actions

- **Get Current Location** - Returns the current location of the device, on demand, without continuously tracking its location. The last location of a device—either from a **Get Current Location** command—or if tracking is started, is shown on a map using **Locate Multiple Devices** (page xx).
- **Start Tracking** - Starts location tracking of the device. Once started, you can view the tracking of the device on a map using **Track a Single Device** (page xxi).
- **Stop Tracking** - Stops location tracking of the device.
- **Location History** - Displays the location history of a device. Location data is returned by both **Get Current Location** commands and by tracking the device.

## Using the Map

1. Select a single device in the middle pane.
2. **Date and Time** - Optionally change the date and time filter. The filter limits the display of device locations to a range of dates and times.
3. **Refresh** - Refresh the map after resetting the **Date and Time** filter.

## Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing
  -  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - BlackBerry
- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **Device.GroupID** - The device identifier and machine group.

- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Owner** - The owner of the device.
- **Count** - Number of locations tracked.

---

## App Profiles

### Mobile > App Management > App Profiles

The **App Profiles** page defines app profiles. App profiles determine which apps are required to be installed or disallowed from being installed on managed mobile devices. Each app profile represents a different set of apps. All apps belonging to the same app profile are either required or disallowed. You can assign multiple app profiles to a single mobile device. Changes to a profile affect all devices assigned that app profile. An app profile is assigned to managed mobile devices using Mobile > **Assign App Profiles** (page xxiv).





- If an app is disallowed, Mobile Device Management does not automatically uninstall the app. The user is asked to perform the uninstall manually.
- If an app is required and the app is a *store app*, Mobile Device Management sends an invitation with a link to install the app to device users. If an app is required and the app is an *enterprise app*, the app is pushed automatically to the device. See **Add Master App Catalog Item** (page xxv) for more information about these two types of apps.

The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.



### Actions

- **New - Adds a new app profile** (page xxiv).
- **Edit - Edits a selected app profile** (page xxiv).
- **Delete** - Deletes a selected app profile.
- **Add Apps From Master Catalog** - Adds apps from the **App Catalog** (page xxv) to a selected app profile.
- **Remove** - Removes a selected app from a selected app profile.

### App Profile Table Columns

- **OS**
  -  - Android
  -  - Apple
- **Type** - Type of app profile.
  -  - Disallowed
  -  - Required
- **Name** - Name of the app profile.

### App Table Columns

- **(App Type)**
  - **Store App** -  - If selected, a **URL** must be specified.
  - **Enterprise App** -  - If selected, an **App Binary** must be specified.
- **Package Name** - The full name of the app in reverse-domain format. Example: `com.kaseya.enterprise.agent`.
- **App Name** - The friendly name of the app. Example: `Agent`.

## New / Edit App Profile

Mobile > App Management > App Profiles > New / Edit App Profile

The **New / Edit App Profile** dialog specifies an app profile. An app profile determines whether apps are required to be installed or disallowed from being installed on managed mobile devices.

- **Name** - The name of the app profile.
- **Type** - Determines the rule for all apps assigned to this app profile.
  - **Required** - Apps added to this app profile are required to be installed on the managed mobile device.
  - **Disallowed** - Apps added to this app profile are prevented from being installed on the managed device.
- **OS** - Android or iOS.

## Assign App Profiles






Mobile > App Management > Assign App Profiles

The **Assign App Profiles** page assigns mobile devices to selected app profiles. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.





### Actions

- **Assign** - Assigns selected mobile devices to a selected app profiles.
- **Remove** - Removes select app profiles from selected mobile devices.

### Device Table Columns

- **Track**
  -  - Tracking has started and the device is checking in.
  -  - Tracking is pending and will start when the device checks-in.
  - (blank) - Tracking is not enabled.
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - BlackBerry
- **Device.GroupID** - The device identifier and machine group.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.

### App Profile Table Columns

- **OS**
  -  - Android
  -  - Apple
- **Type** - Type of app profile.
  -  - Disallowed
  -  - Required
- **Name** - Name of the app profile.

---

# App Catalog

Mobile > App Management > App Catalog

The **App Catalog** page maintains a catalog of app items. Each app item uniquely identifies a single app that can be required on a mobile device or disallowed from a mobile device. Once added to the catalog, app items can then be added to **app profiles** (page *xxiii*). An app profile is a list of app items that determines whether apps are required or disallowed from managed mobile devices.

## Action

- **Add** - Creates a new app item in the **App Catalog**.
- **Edit** - Edits a selected app item in the **App Catalog**.
- **Delete** - Deletes a selected app item from the **App Catalog**.
- **Send Install Invite** - Sends a message inviting the user to install an app on the user's mobile device.

## Table Columns

- **Package Name** - The full name of the app in reverse-domain format. Example: `com.kaseya.enterprise.agent`.
- **App Name** - The friendly name of the app. Example: `Agent`.
- **Device OS** - Android or iOS.
- **App Type** - Specifies whether the app is installed from an app store or downloaded from the VSA as an enterprise built app.
  - **Store App** - 📦 - If selected, a **URL** must be specified.
  - **Enterprise App** - 🍏 - If selected, an **App Binary** must be uploaded.
- **URL** - Specifies the URL mobile devices use to download the app from the app store.
- **App Binary** - Specifies an app bundle to upload to the VSA. The app bundle is either an Android `.apk` file or an iOS `.ipa` file. Once uploaded, the VSA manages the distribution of the app to managed mobile devices.

---

## Add / Edit Master App Catalog Item

Mobile > App Management > App Catalog > Add / Edit Master App Catalog Item

The **Add Master App Catalog Item** dialog uniquely identifies a single app that can be installed on a managed mobile device or disallowed from a device. The first four values **must match the values returned by an app audit of a mobile device exactly**.

- **Package Name** - The full name of the app in reverse-domain format. Example: `com.kaseya.enterprise.agent`.
- **App Name** - The friendly name of the app. Example: `Agent`.
- **Device OS** - Android or iOS.
- **App Type** - Specifies whether the app is installed from an app store or downloaded from the VSA as an enterprise built app.
  - **Store App** - 📦 - If selected, a **URL** must be specified.
  - **Enterprise App** - 🍏 - If selected, an **App Binary** must be specified.
- **URL** - Specifies the URL mobile devices use to download the app from the app store.
- **App Binary** - Specifies an app bundle to upload to the VSA. The app bundle is either an Android `.apk` file or an iOS `.ipa` file. Once uploaded, the VSA manages the distribution of the app to managed mobile devices.

# App Inventory

Mobile > App Management > App Inventory

The **App Inventory** page generates a list of app items based on the apps discovered on managed mobile devices. Rather than specify app items manually, add an app item generated automatically by **App Inventory** to the **App Catalog**. The list of devices shown in **App Inventory** depends on the Device ID / Machine Group filter.

## Actions

- **Add to App Catalog** - Adds selected app items to the **App Catalog** (page xxv).
- **Send Message** - Displays a dialog you can use to enter a text message. Click the dialog's **Send Message** button to send the message to a selected device.

## Table Columns









- **OS** - Android or iOS.
- **Package Name** - The full name of the app in reverse-domain format. Example: `com.kaseya.enterprise.agent`.
- **App Name** - The friendly name of the app. Example: `Agent`.
- **Version** - The application version number. Example: `1.2.0.0`.

# Create Profiles

Mobile > Profiles > Create Profiles

The **Create Profiles** pages 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** (page xxxiii).

## Types of Profiles

- **Email Profile** (page xxvii)  - 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** (page xxviii)  - Configures policies related to the creation of PINs. PINs are used by a device users to unlock their devices.
- **Web Clip Profile** (page xxix)  - 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** (page xxix)  - Applies to iOS devices earlier than iOS 5. Enables and disables popular features on iOS 4 devices.
- **iOS Device Feature Profile** (page xxix)  - Applies to iOS5, iOS6, iOS7 only. Enables and disables popular features on iOS devices.
- **Device Location and Tracking Profile** (page xxxi)  - Sets check-in and location options on devices. This is the only profile that applies to Blackberries.
- **Custom iOS Configuration Profile** (page xxxi)  - A profile generated using Apple's **iPhone Configuration Utility** (<https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>) and imported into **Mobile Device Management**.
- **WiFi Profile** (page xxxii)  - Sets WiFi options on devices. Multiple profiles of this type can be assigned to the same device.



## Actions

- **New** - Add a new profile.
- **Edit** - Edit a selected profile.
- **Delete** - Delete a selected profile.

---

# Email Profile

## Mobile > Profiles > Create Profiles > New/ Edit > Email Profile

- This profile type is supported on iOS devices.
- If the User Display Name, Email Address, User Name or Password fields are blank, they will be populated from the device record.
- This profile type is partially supported on Android devices.
- This profile type is not supported on Blackberry devices.

The **Email Profile** configures the email client on a managed mobile device. Multiple profiles of this type can be assigned to the same device.

- **Name** - The name the profile.
- **Description** - A description of the profile.
- **Account Type** - IMAP, POP, Gmail or Exchange. The Gmail option is a predefined IMAP configuration for a Gmail account. Only the username and password fields have to be entered to complete this Gmail IMAP configuration. See **Configuring an Exchange Email Profile** below.
- **User Display Name** - The display name of the email account.

**Note:** For iOS, if the **User Display Name** and **Email Address** fields are left blank the device user is prompted to enter in his or her user name and email address when the profile is applied to the device.

- **Email Address** - The email address of the user.
- **Incoming Server IP or Hostname** - The IMAP or POP3 incoming email server. For example, pop.youremail.com or imap.youremailserver.com.
- **Incoming Server Port** - The port number used by the incoming email service. For POP3, typically 110, or if SSL/TLS is enabled, 995. If IMAP is enabled, typically 143 or if SSL/TLS is enabled, 993.
- **Incoming Server Requires Password** - If checked, the incoming email server requires a password.
  - **Incoming Server Password** - Enter the password.
- **Use SSL for Incoming Email** - If Yes, communication with the incoming email server is encrypted using SSL/TLS. Your incoming email server must support SSL/TLS to use this feature.
- **Leave Messages on the Server** - If Yes, email remains stored on the incoming email server after it is delivered to the device.
- **Outgoing Server IP or Hostname** - The SMTP outgoing email server. For example, smtp.youremailserver.com.
- **Outgoing Server Port** - The port number using the outgoing email server. Typically 25, or if SSL/TLS is enabled, 465.
- **Outgoing Server User Name** - If outgoing authentication is checked, the outgoing email server username.
- **Use Same Password as Incoming Server** - If checked, both incoming and outgoing use the same incoming password. If blank, specify a password.
  - **Outgoing Server Password** - Enter a password.
- **Use SSL for Outgoing Email** - If Yes, communication with the outgoing email server is encrypted using SSL/TLS. Your outgoing email server must support SSL/TLS to use this feature.

## Configuring an Exchange Email Profile

Set the following to configure an exchange email profile in **Mobile Device Management**:

- **Account Type** - Select Exchange.
- **Email address** - Enter an email address.
- **Incoming Server IP or Hostname** - Enter the exchange server host name.
- **Incoming Server User Name** - Enter a domain username, in the format domain\username
- **Incoming Server Requires Password** - Check this checkbox.
- **Password** - Enter the password for the domain username.
- **Incoming Server Port** - Defaults to 143.
- **Outgoing Server Port** - Defaults to 25.
- **Use SSL for Incoming Email** - Defaults to checked.
- **Use Same Password as Incoming Password** - Check this checkbox.

**Note:** For iOS devices only, if you leave the user name, email address and password blank on an Exchange email profile, you must apply the profile using the iPhone Configuration Utility. Otherwise you must create separate profiles in **Mobile Device Management** for each iOS email profile and specify the user name, email address and password.

---

## Security Profile

**Mobile > Profiles > Create Profiles > New/ Edit > Security Profile**

- This profile type is supported on iOS devices.
- This profile type is partially supported on Android devices. Supported fields include: Allow Simple, Force Pin, Maximum Failed Attempts, Maximum Inactivity, Minimum Length, Require Alpha Numeric
- This profile type is not supported on Blackberry devices.

The **Security Profile** configures policies related to the creation of PINs. PINs are used by a devices users to unlock their devices.

**Note:** Android only supports the following settings: allow simple, force pin, minimum length, require alpha, max inactivity and max failed attempts.

- **Profile Type** - The type of profile.
- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **Allow Simple** - If checked, permits users to use sequential or repeated characters in their passcodes. For example, this would allow the passcodes 3333 or DEFG.
- **Force PIN** - If checked, the user must supply a PIN. If not checked, no password is required.
- **Maximum Failed Attempts** - Determines how many failed PIN attempts can be made before the device is wiped. The default behavior is device manufacturer dependent.
- **Maximum inactivity** - The number of seconds to wait while a user does not use the device before locking the device.
- **Maximum PIN Age in Days** - The maximum number of days to use the same PIN.
- **Minimum Complex Characters** - The minimum number of complex characters required in a PIN.
- **Minimum Length** - The minimum length required for a PIN.
- **Require Alphanumeric** - If check, requires both alphabetic and numeric characters.
- **PIN History** - If checked, maintains a PIN history.
- **Manual Fetching When Roaming** - When blank, devices that are roaming sync only when an account is accessed by the user.

- **Maximum Grace Period** - Specifies how soon the device can be unlocked again after use, without prompting again for the PIN.

---

## Web Clip Profile

*Mobile > Profiles > Create Profiles > New/ Edit > Web Clip Profile*

- This profile type is supported on iOS devices. For iOS devices, the URL must begin with HTTP or HTTPS.
- This profile is not supported on Android and Blackberry devices.

The **Web Clip Profile** specifies a web application "shortcut" to a URL that the device can access. An organization may want to install shortcuts on devices pointing to its web pages or support documents. Multiple profiles can be assigned to a device, with one shortcut defined for each **Web Clip Profile**. Currently applies only to iOS devices.

### Table Columns

- **Name** - The name of the profile.
- **Description** - The description of the profile.
- **URL** - The URL of the web application shortcut
- **Label** - A friendly name for the web application shortcut.
- **Icon** - Upload a png file to serve as the icon for the shortcut.
- **Is Removable** - If checked, the user can remove the web application shortcut.

---

## iOS 4 Device Feature Profile

*Mobile > Profiles > Create Profiles > New/ Edit > iOS 4 Device Feature Profile*

- This profile type is supported on iOS devices.
- This profile is not supported on Android and Blackberry devices.

The **iOS 4 Device Feature Profile** enables and disables popular features on iOS devices. Applies to iOS devices earlier than iOS5.

### Table Columns

- **Profile Type** - The type of profile.
- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **Allow App Installation** - If checked, applications can be installed.
- **Allow Camera** - If checked, the camera on the device is enabled.
- **Allow Explicit Content** - If checked, disables the filtering of profane content.
- **Allow Screen Shot** - If checked, the device can create snapshots of its own screen.
- **Allow YouTube** - If checked, YouTube™ is enabled.
- **Allow iTunes** - If checked iTunes™ is enabled.
- **Allow Safari** - If checked, the Safari web-browser is enabled.

---

## iOS Device Feature Profile

*Mobile > Profiles > Create Profiles > New/ Edit > iOS Device Feature Profile*

- This profile type is supported on iOS devices.
- This profile is not supported on Android and Blackberry devices.

The **iOS Device Feature Profile** enables and disables popular features on iOS 5 and later devices.

### Table Columns

- **Profile Type** - The type of profile.
- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **Allow App Installation** - If checked, applications can be installed.
- **Allow Camera** - If checked, the camera on the device is enabled.
- **Allow Explicit Content** - If checked
- **Allow Screen Shot** - If checked, the device can create snapshots of its own screen.
- **Allow YouTube** - If checked, YouTube™ is enabled.
- **Allow iTunes** - If checked iTunes™ is enabled.
- **Allow Safari** - If checked, the Safari web-browser is enabled.
- **Allow Face Time** - If checked, users can place or receive FaceTime video calls.
- **Allow automatic sync while roaming** - If checked, devices sync while roaming. If unchecked, devices sync only when an account is accessed by the user.
- **Allow Siri** - If checked, users can use Siri, voice commands, or dictation.
- **Allow voice dialing** - If checked, users can dial their phone using voice commands.
- **Allow In-App Purchase** - If checked, users can make in-app purchases.
- **Force user to enter iTunes Store password for all purchases** - If checked, users are required to enter their Apple ID password before making any purchase. Normally, there's a brief grace period after a purchase is made before users have to authenticate for subsequent purchases.
- **Allow multiplayer gaming** - If checked, users can play multiplayer games in the Game Center.
- **Allow adding Game Center friends** - If checked, users can add friends in the Game Center.
- **Enable autofill** - If checked, Safari remembers what users enter in web forms.
- **Force fraud warning** - If checked, Safari warns users when visiting websites identified as being fraudulent or compromised.
- **Enable JavaScript** - If checked, Safari executes javascript on websites.
- **Block pop-ups** - If checked, Safari's pop-up blocking feature is enabled.
- **Accept cookies** - Choose when to accept all cookies: **Never**, **From visited sites**, **Always**.
- **Allow backup** - If checked, users can back up their device to iCloud.
- **Allow document sync** - If checked, users can store documents in iCloud.
- **Allow Photo Stream (disallowing can cause data loss)** - If checked, users can enable Photo Stream.

**Warning:** If unchecked, applying this configuration profile will erase Photo Stream photos from the user's device and prevent photos from the Camera Roll from being sent to Photo Stream. If there are no other copies of these photos, they may be lost.

- **Allow diagnostic data to be sent to Apple** - If checked, iOS diagnostic information is sent to Apple.
- **Allow user to accept untrusted TLS certificates** - If checked, users will be asked if they want to trust certifications that cannot be verified. This setting applies to Safari and to Mail, Contacts, and Calendar accounts.
- **Force encrypted backups** - If unchecked, then in iTunes the user can choose to encrypt or not encrypt a backup from the device to a local machine. If checked, then in iTunes the user is forced to encrypt the backup. When a backup is encrypted, a message box on the device prompts the user to enter an encryption password.
- **Allow explicit music and podcasts** - If checked, explicit music or video content in the iTunes Store is displayed instead of hidden. Explicit content is flagged by content providers, such as record labels, when listed on the iTunes Store.
- **Ratings Region** - Select a ratings region for movies, TV shows, and apps.

- **Movies** - Select the maximum allowed ratings for movies.
- **TV Shows** - Select the maximum allowed rating for TV shows.
- **Apps** - Select the maximum number of apps allowed.

---

## Custom iOS Configuration Profile

Mobile > Profiles > Create Profiles > New/ Edit > Custom iOS Configuration Profile

- This profile type is supported on iOS devices.
- This profile is not supported on Android and Blackberry devices.

The **Custom iOS Configuration Profile** is a profile generated using Apple's **iPhone Configuration Utility** (<https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>) and imported into **Mobile Device Management**. Enter the following.

- **Name** - The name to call the profile in **Mobile Device Management**.
- **Description** - A description of the profile.
- **Config File** - Browse to the select the configuration profile to import.

---

## Device Location and Tracking Profile

Mobile > Profiles > Device Location and Tracking Profile

- This profile type is supported on iOS, Android and Blackberry devices.

The **Device Location and Tracking Profile** sets check-in and location options on devices. *This is the only profile that applies to Blackberry devices.*

### Table Columns

- **Profile Type** - The type of profile.
- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **Checkin only when connected to WiFi** - If checked, the agent only checks in if a WiFi connection is available. This feature is not yet supported.
- **Checkin Only When Connected to WiFi** - If checked, the Kaseya Agent app checks in only if a WiFi connection is available. If unchecked, the Kaseya App, will check in by cell phone network if a WiFi connection is not available.
- **Track Device** - If checked, tracking is enabled. Location data is filtered against a number or predefined parameters to ensure that only accurate and useful location data is actually sent to the VSA. *Recorded location data is only sent to the VSA when the agent next checks in.* The following general criteria is used -
  - **Accuracy** - Each location update received from a GPS tower or satellite has an accuracy rating, estimating the confidence GPS source has in the accuracy of the location data.
  - **Age** - A device caches location data and may at times pass old location data to the **Kaseya Agent** app if a new location update has not recently been received.
  - **Distance traveled** - The distance the device has moved since the previous location update. This could be zero if the device has not moved.
- **Agent Check-in Time (minutes)** - *This field is ignored by agents installed using Kaseya Agent app version 1.1 and later.* Sets the minimum time between check-in attempts. A number of environmental and device operating factors govern exactly when check-in takes place. The lower this value the more battery power is consumed.

- **Tracking Accuracy (meters)** - This value is passed to the GPS receiver as a hint for how accurate the location information pass through should be. The more accurate the request, a lower value, the longer it takes to get the location and more power used.
- **Minimum Accuracy Before Ignore (meters)** - This value controls what location information is considered useful enough to send to the VSA and save. When a device is moving quickly—in a car or train for example—location tracking information becomes less accurate and, at some point, is no longer useful. Location points that are less accurate than this value are filtered out and are not recorded or sent to the VSA. This value more than any other governs the quantity and quality of the location info send from the device.
- **Tracking Movement Distance** - This value defines the minimum distance the device must move, in meters, for a location update event to be triggered and sent to the agent. It also is used by the agent to decide if the location point should be recorded and sent to the VSA. For example if this value is set for 500 meters and the device only moves 10 meters then the agent does not record this point, unless the **Minimum / Maximum Tracking Time (minutes)** allows it.
- **Minimum / Maximum Tracking Time (minutes)** - These values define how frequently location information points should be recorded. The minimum value defines the minimum time between points. For example if the value is 10 minutes then the location info reported to the agent is not recorded nor sent to the VSA for at least 10 minutes from the last time a good location was reported. However if a good location point has not be recorded within the time period governed by the maximum value, then regardless of accuracy or distance traveled, this point *is* recorded.

*An example of recording a point:*

- A point is requested at the appropriate tracking accuracy.
- If the point returned is has an accuracy value greater than specified in minimum accuracy before ignore, the point is discarded.
- If the device has not moved at least the distance specified in tracking movement distance the point is discarded.
- If the time elapsed between this point and the previous one recorded is less than the minimum tracking time, the point is discarded.
- If the time between this point and the previous one recorded is greater than the maximum tracking time, then the point is recorded, even if the previous checks would have discarded it.

---

## WiFi Profile

### Mobile > Profiles > WiFi Profile

- This profile type is supported on iOS and Android devices.
- This profile is not supported on Blackberry devices.

The **WiFi Profile** sets WiFi options on devices. Because of the greater cost associated with transmitting data using a cellular network, there is an option to only communicate with the VSA using WiFi. This can be specified as a system default or by applying a **Device Location and Tracking Profile** (page xxxi). When WiFi only is enabled, no communication between the device and the VSA occurs unless a WiFi connection is available to the device. Once a WiFi connection is available, the device may process a number of commands that have queued up, including location tracking data. Multiple profiles of this type can be assigned to the same device.

### Table Columns

- **Profile Type** - The type of profile.
- **Name** - The name of the profile.
- **Description** - A description of the profile.
- **SSID** - A unique identifier of a wireless network.
- **Hidden Network** - If checked, the wireless network does not broadcast its SSID.

- **Encryption Type** - The type of encryption used by the wireless network. Make sure that these values exactly match the capabilities of the network access point. If you're unsure about the encryption type, or would prefer that it applies to all encryption types, use the value "Any".
  - WEP - Wired Equivalent Privacy
  - WPA - WiFi Protected Access. Includes both WPA and WPA2.
  - Any - Any other type of WiFi protocol
- **Password** - The WiFi password.

# Assign Profiles

Mobile > Profiles > Assign Profiles

The **Assign Profiles** page assigns profiles to devices. Profiles are created using the **Create Profiles** (page xxvi) page. The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.
















## Assigning Profiles

1. Select a single device in the middle panel.
2. Click the **Assign** button in the middle panel or right-hand panel. A list of available profiles displays.
3. Select one profile in the list.
4. Click **Save**.

## Removing Profiles

1. Select one or more devices in the middle panel.
2. Select a profile in the right-hand panel.
3. Click the **Remove** button.

## Device Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing
  -  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android





- Apple



- BlackBerry

- **Device.GroupID** - The device identifier and machine group.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Owner** - The owner of the device.

## Profile Table Columns

- **Profile Type**
  - **Email Profile** (page xxvii) - 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** (page xxviii) - Configures policies related to the creation of PINs. PINs are used by a device users to unlock their devices.
  - **Web Clip Profile** (page xxix) - 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** (page xxix) - Applies to iOS devices earlier than iOS 5. Enables and disables popular features on iOS 4 devices.
  - **iOS Device Feature Profile** (page xxix) - Applies to iOS5, iOS6, iOS7 only. Enables and disables popular features on iOS devices.
  - **Device Location and Tracking Profile** (page xxxi) - Sets check-in and location options on devices. This is the only profile that applies to Blackberries.
  - **Custom iOS Configuration Profile** (page xxxi) - A profile generated using Apple's **iPhone Configuration Utility** (<https://developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html>) and imported into **Mobile Device Management**.
  - **WiFi Profile** (page xxxii) - Sets WiFi options on devices. Multiple profiles of this type can be assigned to the same device.
- **Name** - Name of profile.
- **Details** - Selected details about the profile.

---

# Device Alerts

## Mobile > Alerts > Device Alerts

The **Device Alerts** page sets alert conditions for devices and can optionally send a message to one or more devices. Types of 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.
- **Disallowed Apps** - A disallowed app has been detected on a device.
- **Required Apps** - A required app is missing from a device.

The list of device IDs you can select on this page depends on the Device ID / Machine Group filter and the scope you are using.





















## Summary tab

Provides a summary view of all alert conditions configured and enabled for each device.

### Action

- **Send Message** - Sends a message to one or more selected devices. IOS devices receive a push notification. Android devices receive an SMS message.

### Table Columns

- **(Device Status)** - The status of the Kaseya Agent app on the user's device.
  -  - Created
  -  - Invitation failed
  -  - Invited - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  -  - Invitation rejected
  -  - Installing
  -  - Install failed
  -  - Normal - The app is installed and working normally.
  -  - Command pending
  -  - Command sent
  -  - Unresponsive
  -  - Processing
  -  - Command sent - retry
  -  - Opt out
  -  - Command sent - failed
- **(Device OS)**
  -  - Android
  -  - Apple
  -  - Blackberry
- **Track** - If checked or the tracked icon  displays, the device is being tracked.
- **Device.GroupID** - The device identifier and machine group.
- **Owner** - The owner of the device.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **Device Offline** - If checked, a device failed to check-in a specified number of minutes.
- **Lost Device Checks In** - If checked, a device marked as lost has checked in.
- **Device Checks In** - If checked, a device checks in.
- **Prompt Agent** - If checked, prompts the user of the device, after the device has failed to check in a specified number of minutes.

## Device Offline tab

A **Device Offline** alert occurs when a device fails to check-in within a specified number of minutes.

### Action

- **New / Edit** - Creates or edits a **Device Offline** alert condition.
  - **Device has not checked in for (minutes)** - Specifies the number of minutes to wait after the last check in from the device.

- **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
- **Create Ticket** - Creates a ticket in response to the alert condition.
- **Email Recipients (Comma separate multiple addresses)** - Email recipients to be notified in response to an alert condition.
- **Subject** - The subject of the email notification.
- **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.

**Note:** This tab shares the same table column descriptions as described above.

### Lost Device Checks In tab

A **Lost Device Checks in** alert occurs when a device checks in after being marked as lost.

#### Action

- **New / Edit** - Creates or edits a **Lost Device Checks in** alert condition.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.

**Note:** This tab shares the same table column descriptions as described above.

### Device Checks In tab

A **Device Checks in** alert occurs when a device checks in.

#### Action

- **New / Edit** - Creates or edits a **Device Checks in** alert condition.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.

- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.

**Note:** This tab shares the same table column descriptions as described above.

### Prompt Agent tab

A **Prompt Agent** alert prompts the user of the device, after the device has failed to check in a specified number of minutes. Applies to iOS devices only.

#### Action

- **New / Edit** - Creates or edits a **Prompt Agent** alert condition.
  - **Device has not checked in for (minutes)** - Specifies the number of minutes to wait after the last check in from the device.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.
- **Send Message Now** - Sends the prompt immediately.

**Note:** This tab shares the same table column descriptions as described above.

### Disallowed Apps tab

A **Disallowed App** alert occurs when a disallowed app has been detected on a device.

#### Action

- **New / Edit** - Creates or edits a **Disallowed App** alert condition.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.

**Note:** This tab shares the same table column descriptions as described above.

### Required Apps tab

A **Required Apps** alert occurs when a required app is missing from a device.

#### Action

- **New / Edit** - Creates or edits a **Required Apps** alert condition.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.
- **Enable** - Re-enables the alert condition.
- **Disable** - Disables the alert condition without permanently deleting it. No alerts will be created while the alert condition is disabled.

**Note:** This tab shares the same table column descriptions as described above.

---

## Group Alerts

Mobile > Alerts > Group Alerts

The **Group Alerts** page creates an alert when a new device joins a selected organization or machine group. The list of organizations and machine groups you can see depends on your **scope** (<http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4578.htm>).

#### Action

- **New / Edit** - Creates or edits a **Group Alert** alert condition.
  - **Rearm alert after (minutes)** - Once the alert has been created, specifies how long to wait before resending another email or creating another ticket. Rearm is canceled if the alert condition no longer exists.
  - **Create Ticket** - Creates a ticket in response to the alert condition.
  - **Email Recipients (Comma separate multiple addresses)** - Email recipients to be notified in response to an alert condition.
  - **Subject** - The subject of the email notification.
  - **Message** - The body text of the email notification.
- **Delete** - Deletes the alert condition.

#### Table Columns

- **Name** - The name of the organization or machine group.

**Note:** Other table columns are already defined above.

---

# System Settings

Mobile > Configure System > System Settings

The **System Setting** page sets default settings that apply to every device managed by **Mobile Device Management**.

## System Settings

The following invitation defaults are used when creating an invitation on the **Device Status** (page ix) page.

- **Server Id** - The unique ID of the server.
- **Default Country Code** - The default country code displayed when the dialog for a new invitation displays.
- **Default Group** - The default machine group displayed when the dialog for a new invitation displays.
- **Device Invitation Message** - The text of the message sent to invite the user to install a Kaseya mobile agent. Used when the admin manually creates new account for known device and sends an invitation to user of that device to install the agent. See **Installing the Kaseya Agent App** (page iii).
- **App Invitation Message** - The text of the message sent to invite the user to install a required app. See **Managing Apps on Devices** (page vii).
- **Agentless Invitation Message** - The text of the message sent to invite the user to install a Kaseya mobile agent.
- **Default number of location points to display** - Limits the number of location points to display on the **Track a Single Device** (page xxi) page.

## Message Tags

The following tags can be embedded in the invitation messages specified on this page.

- `{address}` = invitation service URL
- `{serverId}` = device server ID
- `{agentlessUrl}` = enrollment URL
- `{name}` = app name
- `{url}` = app location URL

## Web Server Settings

The following fields override the default port 80 for HTTP and port 443 for HTTPS settings and the default URL used to access **Mobile Device Management** web services, which is `http://<your-KServer>/vsaws/kmdmws.asmx`.

- **Protocol** - HTTP or HTTPS
- **External name / IP address of server**
- **Port for web services**

## Actions

- **Save** - Saves changes to this page's settings.
- **Use Defaults** - Resets this page to its initial values.

---

# Server Settings

Mobile > Configure System > Server Settings

The **Server Settings** page sets server options for the **Mobile Device Management** module.

**System Settings**

- **Retention Time for Server Logs** - The number of days to store server logs. Logs are stored in the \<KServerInstallDirectory>\WebPages\ManagedFiles\Mobile\Logs directory.
- **Retention Time for App Invite Logs** - The number of days to store app invite logs. These logs are stored in the database.
- **Threshold for Resending App Invites** - Waits this number of days to resend an invite to a user to install a required app.

**Actions**

- **Save** - Saves changes to this page's settings.
- **Use Defaults** - Resets this page to its initial values.

---

# Mobile Device Management Reports

<b>Mobile Device Management Overview</b> .....	<b>i</b>
<b>Mobile Device Management Module Minimum Requirements</b> .....	<b>ii</b>
<b>Mobile Management Licensing</b> .....	<b>iii</b>
<b>Installing the Kaseya Agent App</b> .....	<b>iii</b>
<b>Agentless Installs</b> .....	<b>iii</b>
<b>Communicating with Devices</b> .....	<b>iv</b>
<b>Managing Lost Devices</b> .....	<b>v</b>
<b>Backing Up and Restoring Device Contact Lists</b> .....	<b>v</b>
<b>Tracking the Locations of Devices</b> .....	<b>v</b>
<b>Managing Devices Using Profiles</b> .....	<b>v</b>
<b>Uninstalling the Kaseya Agent App</b> .....	<b>vi</b>
<b>Managing Apps on Devices</b> .....	<b>vii</b>
<b>Module Settings</b> .....	<b>vii</b>
<b>Alerts</b> .....	<b>vii</b>
<b>Logs</b> .....	<b>viii</b>
<b>Reports</b> .....	<b>viii</b>
<b>Mobile Workflow</b> .....	<b>viii</b>
<b>Dashboard</b> .....	<b>ix</b>
<b>Device Status</b> .....	<b>ix</b>
<b>Device Summary</b> .....	<b>xii</b>
<b>Device Messages</b> .....	<b>xvi</b>
<b>Lost Devices</b> .....	<b>xvii</b>
<b>Contacts</b> .....	<b>xviii</b>
<b>Application Logs</b> .....	<b>xix</b>
<b>Locate Multiple Devices</b> .....	<b>xx</b>
<b>Track a Single Device</b> .....	<b>xxi</b>
<b>App Profiles</b> .....	<b>xxiii</b>
<b>New / Edit App Profile</b> .....	<b>xxiv</b>
<b>Assign App Profiles</b> .....	<b>xxiv</b>
<b>App Catalog</b> .....	<b>xxv</b>
<b>Add / Edit Master App Catalog Item</b> .....	<b>xxv</b>

App Inventory .....	xxvi
Create Profiles .....	xxvi
Email Profile .....	xxvii
Security Profile .....	xxviii
Web Clip Profile .....	xxix
iOS 4 Device Feature Profile.....	xxix
iOS Device Feature Profile.....	xxix
Custom iOS Configuration Profile .....	xxxi
Device Location and Tracking Profile .....	xxxi
WiFi Profile .....	xxxii
Assign Profiles .....	xxxiii
Device Alerts.....	xxxiv
Group Alerts.....	xxxviii
System Settings.....	xxxix
Server Settings .....	xxxix
Mobile Device Management Reports.....	xl
Mobile Devices - Device Applications .....	xli
Mobile Devices - Device Status.....	xlii
Mobile Devices - Device Summary .....	xlii
Mobile Devices - Lost Devices .....	xliii
Index .....	45

**In This Section**

Mobile Devices - Device Applications	xli
Mobile Devices - Device Status	xlii
Mobile Devices - Device Summary	xlii
Mobile Devices - Lost Devices	xliii

---

## Mobile Devices - Device Applications

Info Center > Reporting > Reports > Mobile Devices - Device Applications

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Applications** report definition generates a report listing the application installed on a device.

### Filtering and Sorting Parameters

- **Operating System Type** - Android, Apple
- **Manufacturer** - The manufacturers of device hardware.
- **Home carrier** - The main service providers of devices.
- **Current carrier** - The carriers currently being used by devices.
- **Application Name** - The name of applications installed on devices.

---

## Mobile Devices - Device Status

Info Center > Reporting > Reports > Mobile Devices - Device Status

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Status** report definition generates a report listing the status of each device.

### Filtering and Sorting Parameters

- **Mobile Device Status** - *Only the most common commands are listed below.*
  - **Invited** - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  - **Normal** - The app is installed and working normally.
  - **Command Pending** - A command is pending for the Kaseya Agent app on the user's device.
- **Operating System Type** - **Android**, **Apple**
- **Track** - **True**, **False**

---

## Mobile Devices - Device Summary

Info Center > Reporting > Reports > Mobile Devices - Device Summary

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Device Summary** report definition generates a summary report of all audit information of selected devices.

### Filtering and Sorting Parameters

- **Mobile Device Status** - *Only the most common commands are listed below.*
  - **Invited** - An invitation is sent to the user to install the Kaseya Agent app on the user's device.
  - **Normal** - The app is installed and working normally.
  - **Command Pending** - A command is pending for the Kaseya Agent app on the user's device.
- **Operating System Type** - **Android**, **Apple**
- **Manufacturer** - The manufacturers of device hardware.
- **Home carrier** - The main service providers of devices.

### Detail Tables to Display

- **Show Operating System Detail**
- **Show Device Info Detail**
- **Show Platform Detail**
- **Show Home Network Detail**
- **Show Current Network Detail**

### Detail Charts to Display

- **Show Mobile Device Status Chart**
- **Show OS Type Chart**
- **Show Manufacturer Chart**
- **Show Home Carrier Chart**
- **Show Current Carrier Chart**



---

# Mobile Devices - Lost Devices

Info Center > Reporting > Reports > Mobile Devices - Lost Devices

- Displays only if the **Mobile Device Management** add-on module is installed.

The **Lost Devices** report definition generates a report of all lost devices.

## Time Range

- **From** - Filters the report date range by this start date.
- **To** - Filters the report date range by this end date.



---

# Index

**A**

Add / Edit Master App Catalog Item • xxv  
 Agentless Installs • iii  
 Alerts • vii  
 App Catalog • xxv  
 App Inventory • xxvi  
 App Profiles • xxiii  
 Application Logs • xix  
 Assign App Profiles • xxiv  
 Assign Profiles • xxxiii

**B**

Backing Up and Restoring Device Contact Lists • v

**C**

Communicating with Devices • iv  
 Contacts • xviii  
 Create Profiles • xxvi  
 Custom iOS Configuration Profile • xxxi

**D**

Dashboard • ix  
 Device Alerts • xxxiv  
 Device Location and Tracking Profile • xxxi  
 Device Messages • xvi  
 Device Status • ix  
 Device Summary • xii

**E**

Email Profile • xxvii

**G**

Group Alerts • xxxviii

**I**

Installing the Kaseya Agent App • iii  
 iOS 4 Device Feature Profile • xxix  
 iOS Device Feature Profile • xxix

**L**

Locate Multiple Devices • xx  
 Logs • viii  
 Lost Devices • xvii

**M**

Managing Apps on Devices • vii  
 Managing Devices Using Profiles • v  
 Managing Lost Devices • v  
 Mobile Device Management Module Minimum  
 Requirements • ii  
 Mobile Device Management Overview • i  
 Mobile Device Management Reports • xl

Mobile Devices - Device Applications • xli  
 Mobile Devices - Device Status • xlii  
 Mobile Devices - Device Summary • xlii  
 Mobile Devices - Lost Devices • xliii  
 Mobile Management Licensing • iii  
 Mobile Workflow • viii  
 Module Settings • vii

**N**

New / Edit App Profile • xxiv

**R**

Reports • viii

**S**

Security Profile • xxviii  
 Server Settings • xxxix  
 System Settings • xxxix

**T**

Track a Single Device • xxi  
 Tracking the Locations of Devices • v

**U**

Uninstalling the Kaseya Agent App • vi

**W**

Web Clip Profile • xxix  
 WiFi Profile • xxxii