



# **Enterprise Mobility Management**

---

**User Guide**

Version R95

English

February 17, 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

Overview .....	i
Enterprise Mobility Management Module Minimum Requirements .....	ii
User Interface.....	iii
Onboarding Customers .....	iii
Onboarding Users .....	vi
Managing Users Manually .....	vii
Importing Users Using CSV.....	vii
Importing Active Directory Users .....	viii
Configuring Active Directory Integration .....	ix
Inviting Users .....	xii
Managing Devices .....	xiii
Command Status .....	xv
Audit Actions .....	xvi
Tracking Actions.....	xvi
Messaging Actions .....	xvi
Lost / Found Actions .....	xvi
Devices Actions .....	xvii
Alerts Actions .....	xvii
Viewing Device Details.....	xvii
Configuring Policies.....	xix
MDM Profiles .....	xxi
Configuring the MDM Security Profile .....	xxi
Configuring the iOS Profile.....	xxi
Configuring a Web Clip Profile .....	xxii
Configuring a WiFi Profile.....	xxii
Configuring a Mail Profile .....	xxiii
Configuring an Apps Profile .....	xxiii
BYOD Profiles .....	xxiv
Managing Apps on Devices.....	xxiv
Configuring the App Catalog.....	xxv
Viewing App Inventory .....	xxvi
WorkBrowser and WorkDocs .....	xxvi
Using WorkBrowser .....	xxvi
Using WorkDocs .....	xxvii
Logging Module Activity .....	xxviii
Reports .....	xxviii
Index .....	31



---

# Overview

**Enterprise Mobility Management** is a new module that provides an enterprise-class, integrated solution for managing mobile devices, apps and secure access to company data by policy. This includes the fastest deployment in the industry for onboarding customer organizations and their users. Mobile devices can be company-owned or employee-owned. Enterprise assets are always isolate from personal data. Data is secured using AES-256 encyption at rest and in flight.

A single easy-to-use, integrated user interface enables you to quickly:

- Onboard new and existing customer organizations into **Enterprise Mobility Management** using a wizard setup.
- Apply high, medium, and low security policies that you can customize.
- Use preset configuration profiles for each level of security.
- Launch invitations to users to register their devices.
  - Registering installs a Kaseya agent app on their device called *MobileManage*.
- Manage multiple devices for each user.
- Require or disallow the installation of apps on mobile devices.
- Identify installed apps on mobile devices.
- Audit each mobile device, providing a detailed inventory of operating system, device information, platform and network properties.
- Enable or disable tracking the location of mobile devices in real time and maintain a location history.
- Force an alarm to sound on devices to help users locate their lost devices.
- Lock, wipe and reset lost or stolen devices.
- Be alerted if a lost device checks in or is out of compliance.
- Send text messages from **Enterprise Mobility Management** to mobile devices.
- Provide mobile device users safe, secure access to their company's internal websites and documents using two container apps.
  - The website browser app is called *WorkBrowser*. You can optionally control access to linked internal websites with *WorkBrowser* using proxy URLs.
  - The document browser app is called *WorkDocs*. *WorkDocs* allows a user to edit and save documents locally or upload changed documents to their company's internal networks.

## Licensing

- Licensing is by the number of users managed by **Enterprise Mobility Management**. Each licensed user can have an unlimited number of devices managed by **Enterprise Mobility Management**.

## Simplified User Interface

The user interface comprises a single page with four tabs. Each tab features drill-down menus for:

- Users
- Devices
- Apps
- Policies

## User Management

- **Active Directory Integration** - Optionally use a customer organization's Active Directory instance to identify the users invited to register their mobile devices. Security policies in **Enterprise Mobility Management** are applied to a device based on its association with an Active Directory user.

**Enterprise Mobility Management** does not store any user credentials but only acts as a relay for Active Directory authentication. *Active Directory is required to use BYOD profiles.*

- **CSV file** - Optionally import user records using a CSV data file.
- **Manual** - You can manually add, edit and delete user data records.

### Mobile Devices Supported

**Enterprise Mobility Management** supports the following mobile devices:

- iOS version 7.0 and above
- Android version 4.0.3 and above

### Upgrading

**Enterprise Mobility Management** is only supported in on premises environments. When upgrading to R9 or later in an on premises environment from a version earlier than R9, Mobile Device Management is removed and **Enterprise Mobility Management** is added. Migration of data from Mobile Device Management to **Enterprise Mobility Management** is not supported.

---

## Enterprise Mobility Management Module Minimum Requirements

#### Kaseya Server

- The Enterprise Mobility Management R95 module requires on premises VSA R95. Mobile Device Management, if installed, is uninstalled on upgrade.

**Note:** SaaS VSA environments continue to use Mobile Device Management on upgrade to R92.

- This module requires the VSA have internet access.

#### Requirements for Each Managed Mobile Device

- iOS version 7.0 and above
- Android version 4.0.3 and above

#### Requirements for Active Directory Servers

- Customer organizations can optionally use Active Directory to add users to Enterprise Mobility Management or import a CSV file. *Active Directory is required to use BYOD profiles.* If using Active Directory, the Active Directory instance must allow access from the VSA. Only the TLS protocol is supported at this time. If the VSA does not share the same intranet as an Active Directory instance, the Active Directory instance must be available on a public IP. For security reasons this IP should only be reachable from the MSP's VSA IP address. Mobile devices relay their authentication requests through the VSA to reach an Active Directory instance. Customer organizations should *whitelist the VSA IP address* for servers hosting customer Active Directory instances.

#### Requirements for WebDAV Servers

- NTLM enabled if authentication is required.
- Allow access from the VSA. If the VSA does not share the same intranet as a WebDAV server, the WebDAV server must be available on a public IP. For security reasons this IP should only be reachable from the VSA IP address. Mobile devices relay their requests through the VSA to reach these WebDAV servers. Customer organizations should *whitelist the VSA IP address* for the servers hosting WebDAV servers.

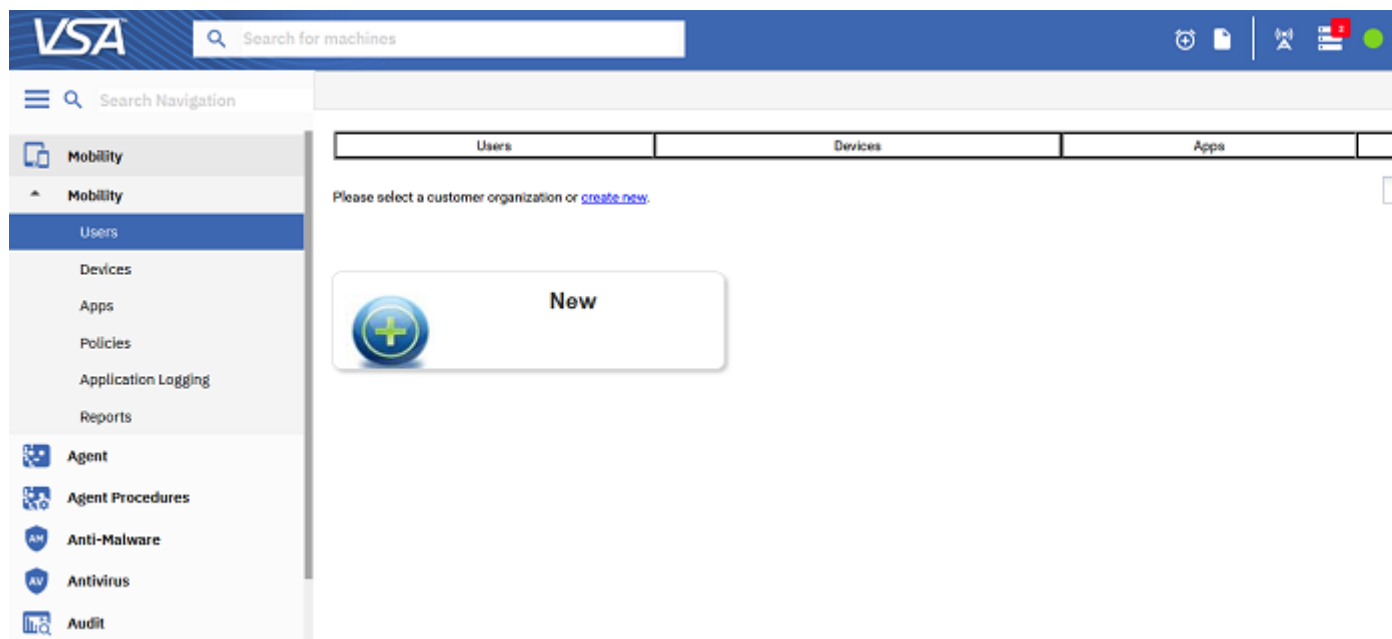
---

# User Interface

**Enterprise Mobility Management** is identified as the **Mobility** module in the navigation pane of the VSA. The module is organized around a single, integrated user interface. The same four main functions run along the top of every page or along the side in the navigation pane:

- Users
- Devices
- Apps
- Policies

The first time you display the **Mobility** module it shows you a tile view of existing customer organizations, similar to the image below. *Every task performed in the **Mobility** module starts with this same user interface.*



---

# Onboarding Customers

Customer organizations must be added to **Enterprise Mobility Management** before inviting users to register their devices.

## Creating a New Organization in the VSA


Follow this procedure if the customer organization you want to add is new to the entire VSA.

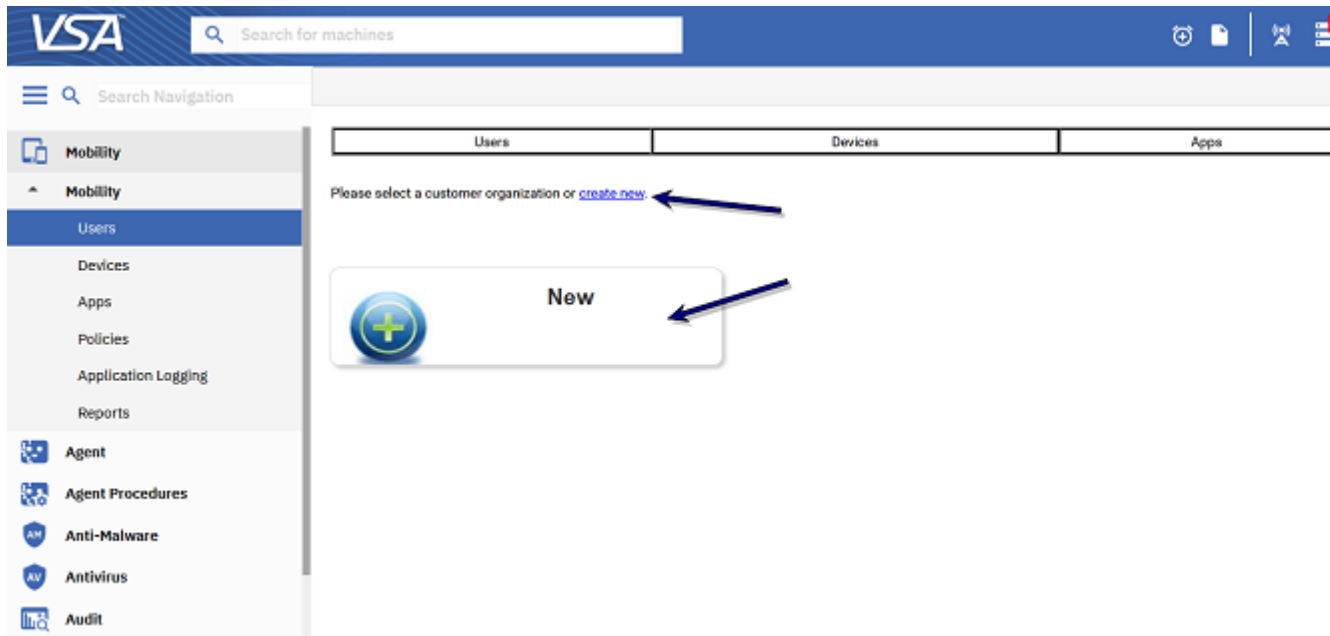
1. Navigate to the System > Orgs/Groups/Depts/Staff > **Manage** page.
2. Click **New** to display the **Add Organization** dialog.
3. Enter an **ID** and **Org Name** to identify the new customer organization.
4. Click **Save**.

Your new customer organization has been created. Now return to the **Mobility** module to add the customer organization to **Enterprise Mobility Management**.

## Adding a Customer Organization in the Mobility Module

1. Click the **New** tile to start the **New Customer Setup Wizard**.

- Click the trashcan icon  in the upper right corner of a tile to *remove* an organization after adding it to **Mobility**. Removing it does not delete the organization from the VSA.
- The tile view can be re-displayed from an existing user page by clicking the **Create New Customer** link.



2. Select the customer organization you want to add to the **Mobility** module.
3. Optionally include a customer logo.
4. Select **MDM only**, **BYOD only** or **MDM & BYOD both**. Your selection determines the policy profiles and options that are displayed to you in the user interface when this customer organization is selected. *Active Directory is required to use BYOD profiles.*


5. Click **Create**.

New Customer Setup Wizard

**Customer Details**

Organization Name\*:

Customer ID\*:



Product signed up for:

☐ MDM only

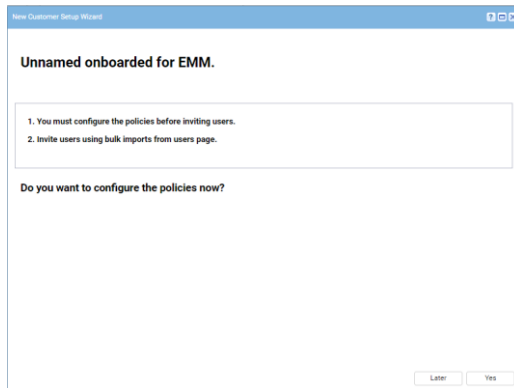
☐ BYOD only

☒ MDM & BYOD both

You must import users from Active Directory for BYOD Apps to work.

6. The last page prompts you with two choices:
- Click **Later** to accept default pre-defined policies for this newly onboarded customer organization. *This option bypasses setting customizable properties that are specific to that customer organisation.*
  - Click **Yes** to configure new customer-specific policies that include both pre-defined and customizable properties.

**Note:** See [Configuring Policies](#) (page xix) for details about selecting this option.



## Onboarding Users

You onboard users from the [Users](#) page for a selected [customer organization](#) (page iii). There are three ways to create device user records in **Enterprise Mobility Management**.

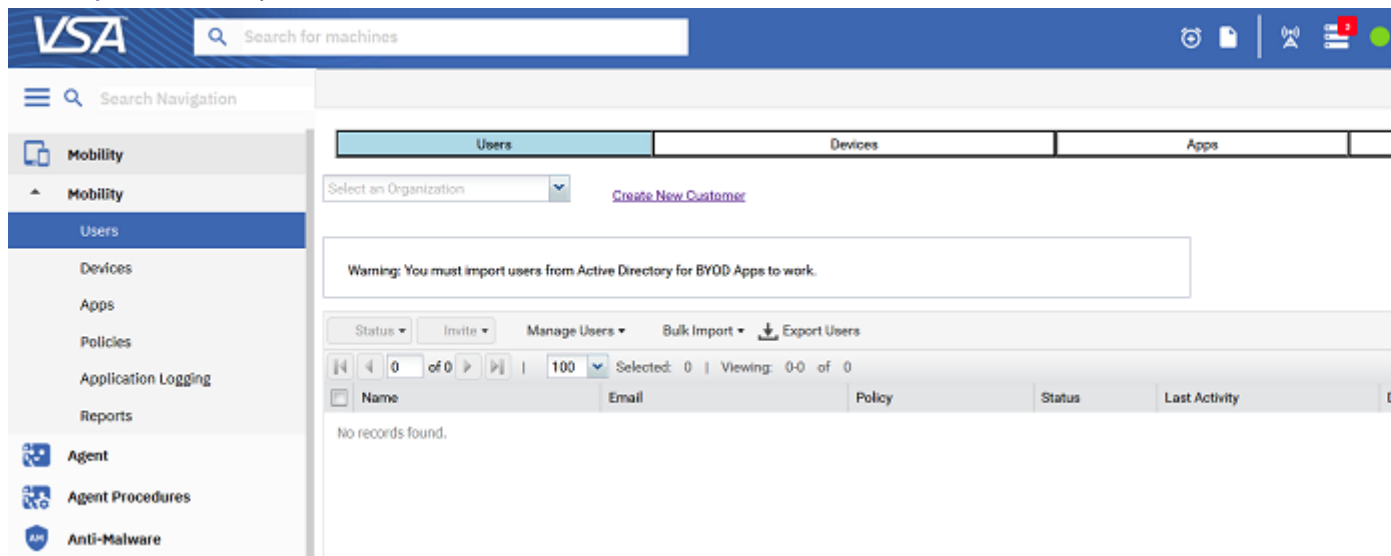
- **Add user records manually** (page vii)
- **Import from Active Directory** (page viii) - *Active Directory is required to use BYOD profiles.*
- **Import from a CSV file** (page vii)

Importing user records overwrites any user records that already exist. Active Directory integration never automatically imports user records.

### Actions

- **Status** - Users default to an activated state.
  - **Activate** - Clicking the activate button for a user 'unblocks' a blocked user, or 'unlocks' a locked user. A user is *blocked* by a VSA administrator. A user is *locked* by exceeding the number of invalid attempts allowed by policy while attempting to log into **BYOD apps** (page xxiv).
  - **Block** - Blocks a user from using **BYOD apps** (page xxiv).
- **Invite Users** (page xii)
- **Manage Users** (page vii)
  - **Add Users** - Adds a single user.
  - **Edit User** - Edits a selected user.
  - **Delete User** - Deletes a user.
- **Bulk Import**
  - **Import from AD** (page viii)
  - **Import from CSV** (page vii)

- **Export Users** - Exports user data to a CSV file.



## Managing Users Manually

You can add, edit and delete users manually. Adding or editing a user record requires the following:

- **Name** - A friendly name for the user that displays in the VSA.
- **Email** - The email address for the user.
- **Userid** - A unique identifier formatted as an email address.
- **Policy** - One of three security policies assigned to this user. The default policies are:
  - High Security Policy
  - Medium Security Policy
  - Low Security Policy

**Note:** Customer-specific security policies can be assigned if they have been defined for a customer organization.

## Importing Users Using CSV

You can optionally bulk import user records using a CSV file.

1. Prepare a CSV file of user data records. Use the following CSV file format.

```
Full Name,Policy Name,Email,User Principal Name
Low Security User,Low,lowsecurityuser@kaseya.com,kaseya\lowsecurityuser
Medium Security
User,Medium,mediumsecurityuser@kaseya.com,mediumsecurityuser@kaseya.com
High Security User,High,highsecurityuser@kaseya.com,highsecurityuser@gmail.com
```

**Note:** You can create a starter CSV file by adding a single user record manually on the **Users** page, then exporting it.

2. Select the **Users** page for an **onboarded customer organization** (page iii).
3. Select the Bulk Import > **Import from CSV**.
4. Browse for the CSV you have prepared and select it for importing.

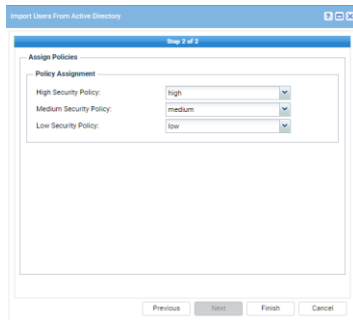
## Importing Active Directory Users

You can optionally import user records from Active Directory. *Active Directory is required to use BYOD profiles.*

1. Select the **Users** page for an **onboarded customer organization** (page iii).
2. Select the Bulk Import > **Import from AD**.
3. Specify the Active Directory parameters **Enterprise Mobility Management** will use to identify users in the customer organization.
  - **Enterprise Mobility Management.** See **Configuring Active Directory for Integration** (page ix).

- **Directory Type** - Active Directory is the only option.
  - **Directory URL (with port)** - Enter an LDAP URL. The default LDAP port to use is 389. Example: ldap://212.54.134.136:389
  - **Username** - Enter an Active Directory username that provides access to the *distinguished name* specified in the **Search Base** field.
  - **Password** - Enter the password.
  - **Search Base** - Enter the *distinguished name* used to search for the three groups of users in this instance of Active Directory that are eligible to register their devices with **Enterprise Mobility Management**. Do not include spaces between commas. Example: OU=Kaseya EMM Groups,DC=company,DC=com
4. Click the **Test Connection** button to verify your Active Directory connection.
    - If successful, click **Next** to populate **Enterprise Mobility Management** with the three groups of users eligible to register their devices with **Enterprise Mobility Management**.
    - If the test fails, check the values entered on this wizard page match your Active Directory configuration. The test must be successful to continue onboarding this customer organization.

5. Assign **Enterprise Mobility Management** mobile device policies to the new customer organization.
  - You can assign one High policy, one Medium policy and one Low policy to each customer organization you register in **Enterprise Mobility Management**.
  - Select the default High, Medium and Low policies if you have not created customer-specific policies yet.



## Configuring Active Directory Integration

**Enterprise Mobility Management** can optionally use a customer organization's Active Directory instance to identify the users invited to register their mobile devices. *Active Directory is required to use BYOD profiles.* Security policies in **Enterprise Mobility Management** are applied to a device based on its association with an Active Directory user.

**Note:** User records can also be managed by importing a CSV file (page vii) of user data records or manually adding new user records.

### Key Integration Concepts

- User records are imported into **Enterprise Mobility Management** from Active Directory.
- See **Enterprise Mobility Management Module Requirements** (page ii) for additional Active Directory requirements.
- The security group a user belongs to in Active Directory determines the policy profile they are assigned in **Enterprise Mobility Management**. Switching a user to a different security group in Active Directory reassigns that user to a different policy profile in **Enterprise Mobility Management**.
- Devices are mapped to the users once they install and register the Kaseya Agent on their devices using the unique activation code emailed to them.
- The user's mobile devices do not need access to Active Directory for authentication. An app request is sent from the device to **Enterprise Mobility Management** which relays the request to Active Directory.
- The AD authentication component within **Enterprise Mobility Management** does not store any user credentials but only acts as a relay for AD authentication.

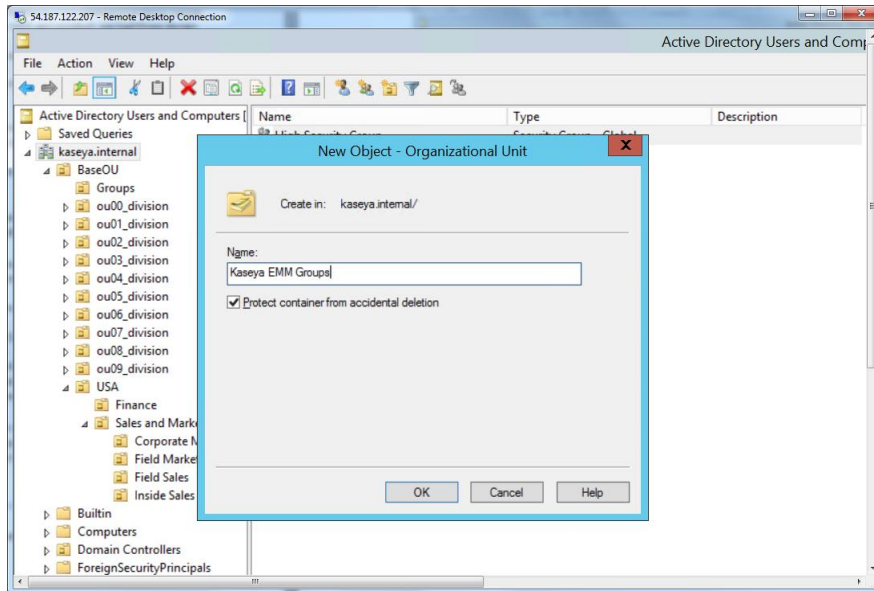
### Creating Three Active Directory Security Groups

**Enterprise Mobility Management** requires three security groups be created in Active Directory. These map to three security policies in **Enterprise Mobility Management**:

- High Security Policy
- Medium Security Policy
- Low Security Policy

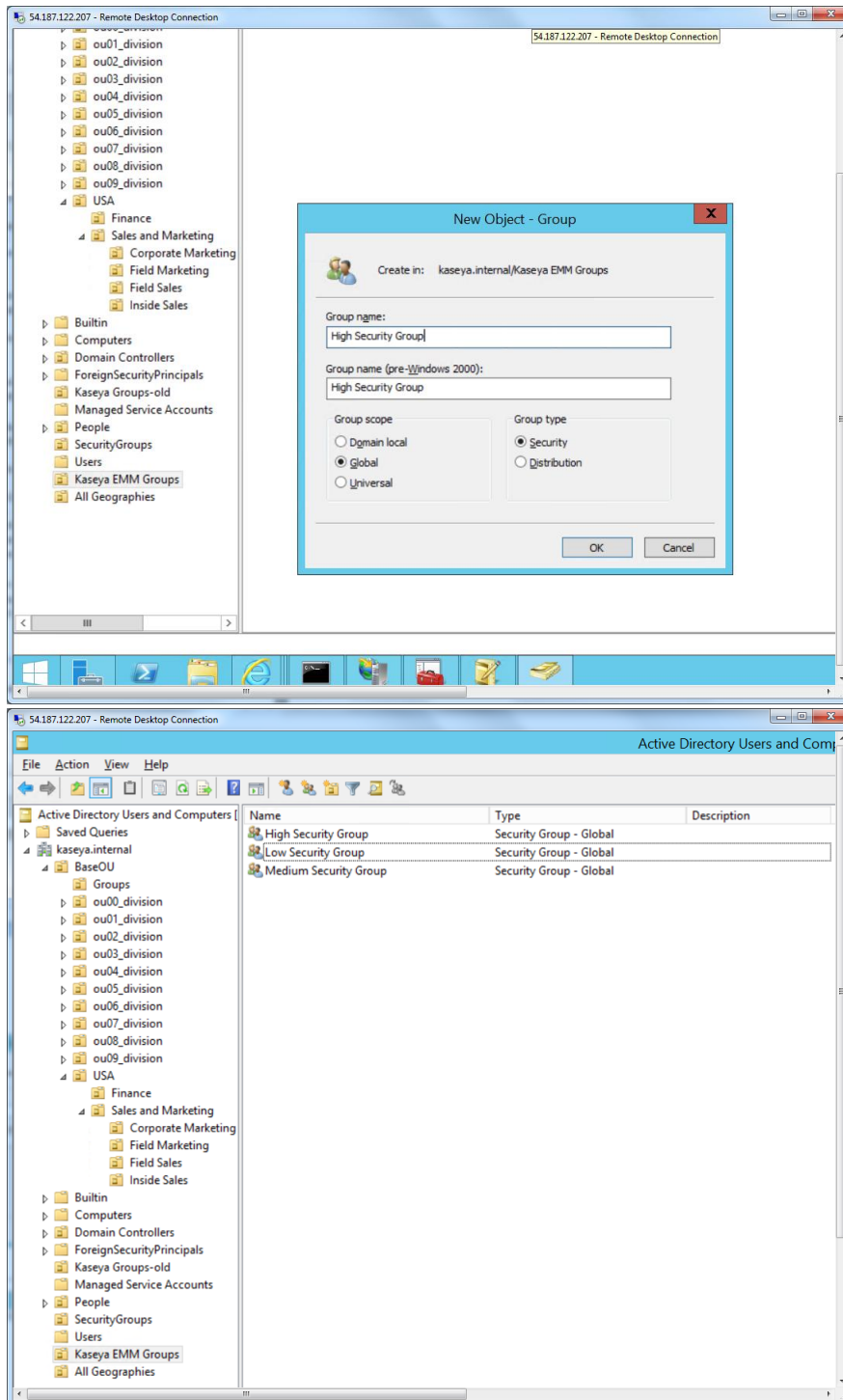
All Active Directory user records intended for import into **Enterprise Mobility Management** must be included in one of these three security groups.

1. Open the Active Directory console and create a new *organizational unit* called Kaseya EMM Groups under the main domain.

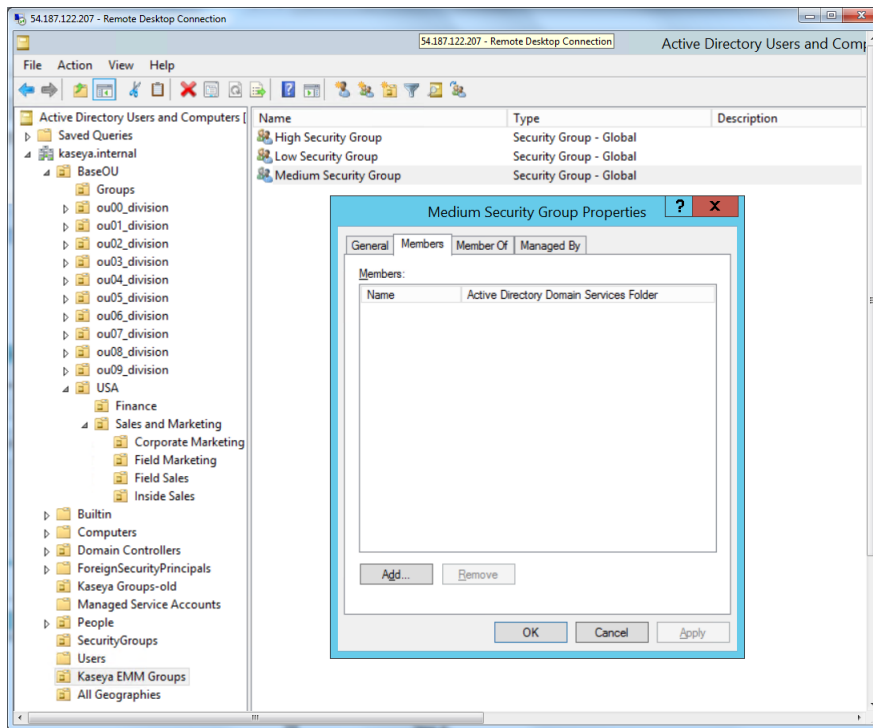


2. Create three security groups under Kaseya EMM Groups. Name them High Security Group, Medium Security Group and Low Security Group.

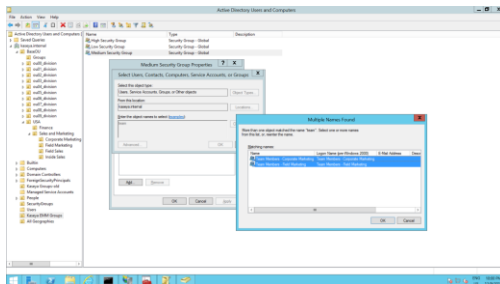
**Note:** You may name these security groups differently. But for ease of mapping with **Enterprise Mobility Management**, we recommend using these names.



- Right click each of the three Kaseya EMM Groups, then click the Properties option. Open the Members tab, then click the Add button.



- Search for users in Active Directory to add to each of the three Kaseya EMM Groups.



Now you have created the three EMM security groups (High Medium and Low) and mapped appropriate users to them.

- Once the configuration is complete, make note of the following. This information is required to connect to any instance of Active Directory you intend to associate with an organization within **Enterprise Mobility Management**.
  - The domain name or IP address of the Active Directory server.
  - Ensure the Active Directory instance can be accessed from the VSA. Only the TLS protocol and port 389 are supported at this time.
  - The base DN (distinguished name) to search for: Example: `OU=Kaseya EMM Groups,DC=company,DC=com` Do not include spaces between commas.
  - The credential to use to authenticate read access to this distinguished name. A dedicated credential is recommended.

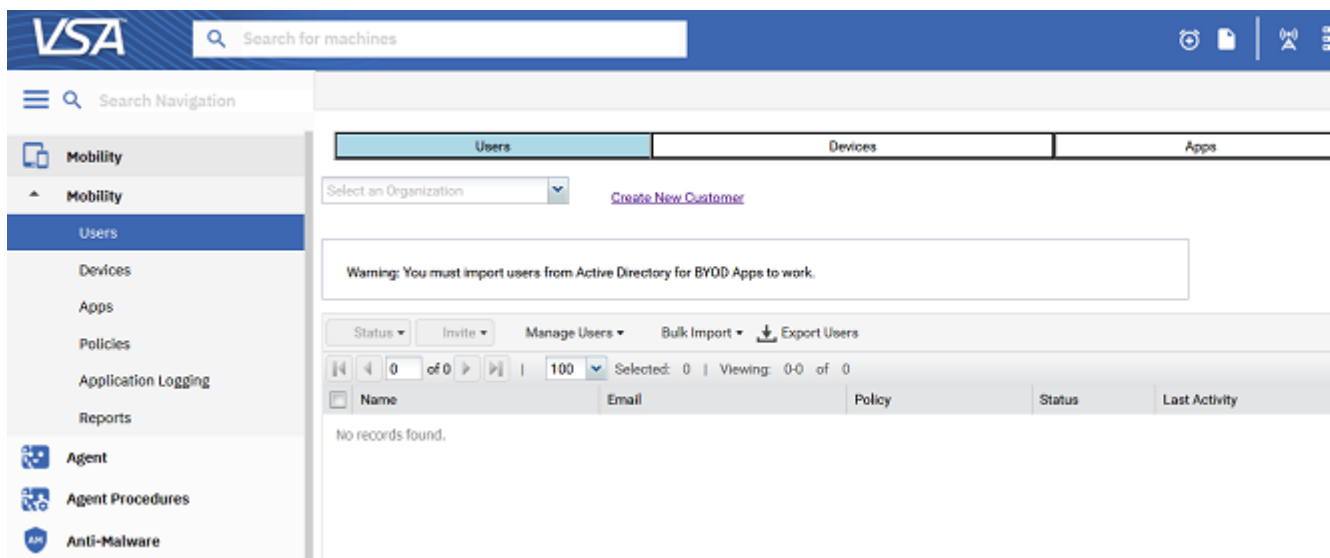
## Inviting Users

Users are automatically invited to install a Kaseya agent on their mobile devices as soon as the user recorded is

created within **Enterprise Mobility Management**. User status will already display **Invited** when you first see users listed on this page. You may wish to invite a user again if he or she failed to receive their original email invitation.

1. Navigate to the **Users** page.
2. Select one or more users.
3. Click the Invite > **Invite Users** option.
  - The **Status** column shows **Invited** when an invitation has been sent to a user.
  - The **Status** column shows **Active** when the user has installed the **Enterprise Mobility Management** agent on at least one or more devices.
  - The number of the devices managed by **Enterprise Mobility Management** for that user is indicated by the device icons in the **Devices** column.

**Note:** See **Managing Devices** (page xiii) for details about mobile device management.



## Managing Devices

Once users have registered devices with **Enterprise Mobility Management** you can manage their devices.

1. Navigate to the **Devices** page.
2. Select a customer organization.
3. Select one of the tiles. Tiles are organized:
  - **by Status**
  - **by Policy**

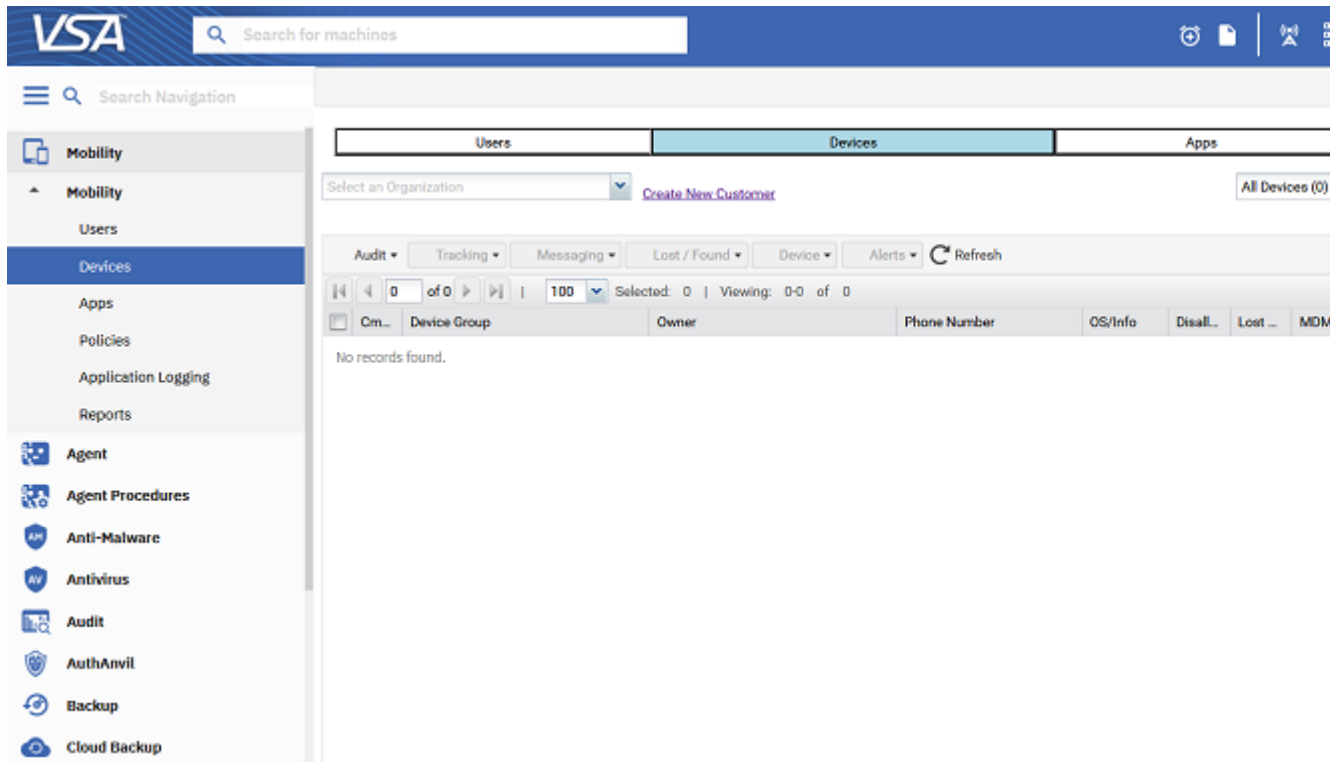
➤ by Category


The screenshot displays the VSA web interface. At the top, there is a search bar labeled 'Search for machines' and a navigation menu with tabs for 'Users', 'Devices', and 'Apps'. The 'Devices' tab is currently selected. Below the navigation bar, there is a section titled 'by Status' which contains four cards: 'All Devices (0)', 'Active Devices (0)', 'Lost Device (0)', and 'Non Compliant (0)'. Below this, there is a section titled 'by Policy' which contains three cards: 'High Security Policy (High Security Policy) (0)', 'Medium Security Policy (Medium Security Policy) (0)', and 'Low Security Policy (0)'. At the bottom, there is a section titled 'by Category' which contains two cards: 'Android Devices (0)' and 'IOS Devices (0)'. On the left side of the interface, there is a sidebar with a search bar and a list of categories: 'Mobility', 'Agent', 'Agent Procedures', 'Anti-Malware', 'Antivirus', 'Audit', 'AuthAnvil', 'Backup', 'Cloud Backup', 'Data Backup', 'Desktop Management', and 'Discovery'. The 'Mobility' category is expanded, showing sub-items: 'Users', 'Devices', 'Apps', 'Policies', 'Application Logging', and 'Reports'. The 'Devices' sub-item is currently selected.

A list of devices for the selected filtering displays.


4. Select one or more rows in the list of devices to enable all the tabs at the top of the table.





**Note:** Clicking the hyperlink for a device name on the **Devices** page displays device details in a series of tabs. See **Device Details** (page xvii) for more information.




5. Clicking the **Command** icon  for a device in the device list displays the **Command Status** (page xv) window.
6. The actions you can perform on devices are organized into the following tabs. See any of the following topics for details.
  - **Audit** (page xvi)
  - **Tracking** (page xvi)
  - **Messaging** (page xvi)
  - **Lost / Found** (page xvi)
  - **Device** (page xvii)
  - **Alerts** (page xvii)

## Command Status

Clicking the **Command** icon  for a device in the device list displays the **Command Status** window. This window 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.

Use the **Mark Complete** option to manually set one or more commands to complete .

---

## Audit Actions

Audits are performed as soon as the user installs a Kaseya agent on his or her mobile device. Audits are run daily by default after that.

- **Schedule Audit** - Schedules an audit for a specified time for selected devices. Schedule once or periodically. Each type of recurrence—Daily, Weekly, Monthly—displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence.
- **Run Audit Now** - Runs an audit of a selected device immediately.
- **Get 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.

---

## Tracking Actions

You can perform any of following **Tracking** actions on a device.

- **Enable Tracking** - Starts location tracking of selected devices. Once started, you can view the tracking of the device on a map using the **Location** tab of a device. See **Viewing Device Details** (page xvii).
- **Disable Tracking** - Stops location tracking of selected devices.
- **Get Current Location** - Returns the current location of a selected device, on demand, without continuously tracking its location.
- **Location History** - Displays the location history of a device. The default start date for the location history is yesterday. The end date is always the current date. Change the start date of the location history, then click **Refresh**.

---

## Messaging Actions

You can perform any of following **Messaging** actions on a device.

- **View** - Displays the history of messages sent to the user.
- **Send** - Displays a dialog you can use to enter and send a text message to the user.

---

## Lost / Found Actions

You can perform any of following **Lost / Found** actions on a device.

- **Sound Stolen Alarm** - If clicked selected devices repeatedly say, "This phone is stolen." whenever they are turned on. See **Silence Alarm** below.
- **Wipe Data** - If clicked, selected devices are reset back to their default settings. **Wiping a device deletes all user data**, including the *MobileManage* app. The *MobileManage* app can no longer check-in after wiping the device.
- **Clear Passcode** - Resets *device-level* passcodes on selected 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 device-level passcode, the user is immediately prompted to enter a new one.
- **Request Checkin** - Users of selected devices are instructed to tap the icon on the *MobileManage* app to open it. Opening the *MobileManage* app causes the app to check in immediately.
- **Mark as Lost** - Marks selected devices as lost.
- **Mark as Found** - Marks selected devices as found.

- **Silence Alarm** - Stops alarms set using the **Sound Stolen Alarm** actions on selected devices.



## Devices Actions

You can perform any of following **Devices** actions on a device.

- **Lock Device** - If clicked, selected devices are locked, preventing user access.
- **Delete** - Deletes selected device accounts in **Enterprise Mobility Management**.

## Alerts Actions

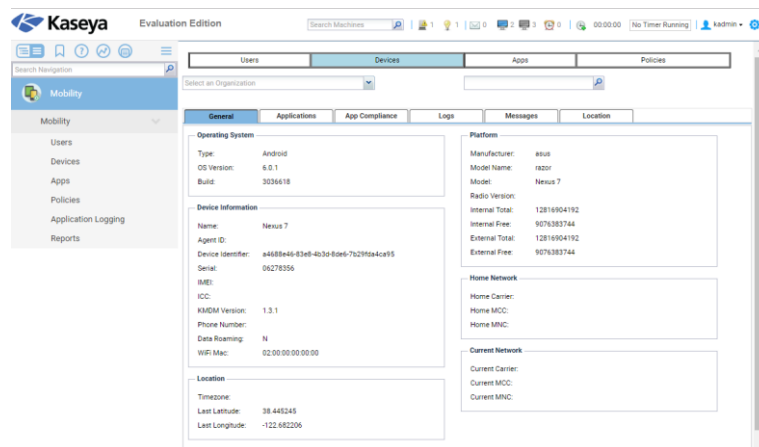
You can perform any of following **Alerts** actions on a device.

- **Details** - Displays an **Alert Details** window for selected devices:
  - **Alert Name** - The alert type: **Lost Device** **Checked In Alert** or **App Compliance Check**.
  - **Enabled** - Alerts are always enabled.
  - **Status** - alert  or ok 
  - **Details** - For an **App Compliance Alert**, displays the counts for **required apps** or **disallowed apps**.
  - **Action** - Resolves the alert, resetting it to an ok status.
- **Resolved** - Resolves alerts, by alert type, for selected devices. Resolving an alert notifies the users of selected mobile devices.

## Viewing Device Details

Clicking the hyperlink beneath a device name on the **Devices** page displays the details of that device in a series of tabs.

- **General**
- **Application**
- **App Compliance**
- **Logs**
- **Messages**
- **Location**



## 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.
- **Agent ID** - The Kaseya agent GUID.
- **Device Identifier** - A unique identifier assigned to the device by the manufacturer.
- **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 *MobileManage* app on the device.
- **Phone Number** - The phone number of the device. Some mobile devices do not have phone numbers.
- **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.
- **Internal Free** - Free memory available and built into the hardware.
- **External Total** - The total memory available externally.
- **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.

## 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 **Required Apps Missing from Device**.



- **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`.

## 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.

## Messages

The **Messages** tab displays a history of messages sent to and from the device.

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

## Location

The **Location** tab 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.

**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.

- **Date and Time** - The location history start date and time. The default start date for the location history is yesterday. The end date is always the current date.
- **Refresh** - Refresh the map after resetting the **Date and Time** filter.

---

# Configuring Policies

The **Policies** page assigns **Enterprise Mobility Management** policies by customer organization and high, medium and low security groups.

You can drill into any policy to:

- Review predefined policies settings. You can edit the options controlled by all preset security profiles.

- Create a new policy and configure customizable settings for that customer organization.

Search for machines

Search Navigation

Mobility

- Mobility
  - Users
  - Devices
  - Apps
  - Policies**
  - Application Logging
  - Reports
- Agent
- Agent Procedures

Select an Organization

Policy	Assigned Group	Total Users	Users Active
<a href="#">High Security Policy</a>	High Security Policy	0	0
<a href="#">Medium Security Policy</a>	Medium Security Policy	0	0
<a href="#">Low Security Policy</a>	Low Security Policy	0	0

## Configuring a Policy

1. On the **Policies** page, select the customer organization you want to view.
2. Click the hyperlink of any of the listed policies.

Search for machines

Search Navigation

Mobility

- Mobility
  - Users
  - Devices
  - Apps
  - Policies**
  - Application Logging
  - Reports
- Agent
- Agent Procedures
- Anti-Malware
- Antivirus
- Audit
- AuthAnvil
- Backup
- Cloud Backup
- Data Backup
- Desktop Management
- Discovery
- Info Center

Select an Organization

[Create New Customer](#)

Policy Name: **High Security Policy** Save Policy Name

Warning: This policy may not be configured completely. [view details](#)

**MDM Profiles**

- ☒ Security Profile
- ☒ IOS Profile
- ☒ Web Clip Profile
- ☒ WiFi Profile
- ☒ Mail Profile
- ☒ Apps Profile

**BYOD Profiles**

- ☒ Access Profile
- ☒ Security Profile
- ☒ URL Profile
- ☒ Document Profile

3. Confirm the correct *policy type* is selected: **High**, **Medium** or **Low** in the drop-down list. Change to the correct policy type, if necessary.
4. Set any of the profiles for the policy you have created.

---

# MDM Profiles

## Configuring the MDM Security Profile

The MDM **Security Profile** configures policies related to the creation of *device-level* PINs (also called a passcode or access code). PINs are used by users to unlock their mobile devices.

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

- **Allow Simple** - If checked, permits users to use sequential or repeated characters in their PINs (passcodes). For example, this would allow the passcodes 3333 or DEFG.
- **Force Password** - For Android devices, if checked, a password is required. If not checked, either a PIN or a password is required. PINs support only digits. Passwords can be alphanumeric. For iOS devices, entering a password is always required.

**Note:** BYOD Profiles may enforce an *app-level* PIN as well. The two PINs are independent of each other.

- **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 checked, requires both alphabetic and numeric characters.
- **Pin History** - If checked, maintains a PIN history.
- **Maximum Grace Period** - Specifies how soon the device can be unlocked again after use, without prompting again for the PIN.

## Configuring the iOS Profile

- **Allow App Installation** - If checked, applications can be installed.
- **Allow Camera** - If checked, the camera on the device is enabled.
- **Maximum Failed Attempts** - If the user exceeds the number of passcode attempts allowed, typically 10, the phone becomes locked. The only way to use it again is to restore the phone to the factory settings, which wipes all data from the phone in the process. After restoring the phone, the phone can be restored to the last backup made.
- **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.
- **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.
- **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.

## Configuring a Web Clip Profile

- This profile type is supported only on iOS devices. For iOS devices, the URL must begin with HTTP or HTTPS.

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.

- **Name** - The name of the profile.
- **URL** - The URL of the web application shortcut.
- **Description** - The description of the profile.
- **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.

## Configuring a WiFi Profile

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

The **WiFi Profile** sets WiFi options on devices.

- **Name** - The name 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.
  - **Open** - Any other type of WiFi protocol. No password it required to connect.
- **Password** - The WiFi password.

## Configuring a Mail Profile

- This profile type is supported only on iOS devices.

The **Email Profile** configures the email client on a managed mobile device.

- **Account Type** - IMAP, POP, Gmail or Exchange.
- **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.
- **Use SSL for Incoming Email** - If Yes, communication with the incoming email server is encrypted using SSL. Your incoming email server must support SSL 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 is enabled, 465.
- **Use Same Password as Incoming Server** - If checked, both incoming and outgoing use the same incoming password. If blank, specify a password.
- **Outgoing Server Requires Password** - If checked, the outgoing email server requires 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 Apps Profile

Custom app profiles can be assigned to a policy. A custom app profile determines the apps that are either required or disallowed on the managed devices of a customer organization.

Before performing this step the following steps should be completed:

- **Managing Apps on Devices** (page xxiv)
- **Configuring the App Catalog** (page xxv)

### Configuring an App Profile in a Policy

1. On the **Policies** page, select the customer organization you want to view.
2. Click the hyperlink of any of the listed policies.
3. Expand the **App Profiles** to add one or more apps to the custom app profile for this customer organization.
4. Click the **Add** button.
5. Select one or more apps to add to the custom app profile.
6. Click the **Add Apps** button.
7. Set the **Status** of the app to either **Disallowed** or **Required**.
  - If an app is **Disallowed**, **Enterprise Mobility 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**, **Enterprise Mobility Management** sends an invitation with a link to install the app to device users.
8. Optionally delete a selected app from the custom app profile using the **Delete Row** option.
9. Click **Save** to complete the configuration.

## BYOD Profiles

**Note:** BYOD Profiles require Active Directory integration (page viii).

You can configure BYOD profiles for a selected customer organization and Active Directory security group.

### Whitelisting the VSA

If the VSA does not share the same intranet as a WebDAV server, the WebDAV server must be available on a public IP. For security reasons this IP should only be reachable from the VSA IP address. Mobile devices relay their requests through the VSA to reach these WebDAV servers. Customer organizations should *whitelist the VSA IP address* for the servers hosting WebDAV servers.

### Access Profile

- **User's device locks out after n failed attempts** - Number of attempts.

### Security Profile

- **Users may email item content to others** - Yes / No.
- **Users may open item content with non suite apps** - Yes / No.
- **Users may save images to device's photo library** - Yes / No.
- **Users may print non-suite content** - Yes / No.
- **Users may copy/paste to non-suite apps** - Yes / No. If no, a **paste blocked by policy** message displays when a user attempts to copy from a secure container app into an external app. Copying from an external app into a secure container app is never blocked.

### URL Profile

Add the URLs that are *directly accessible* to a device's network connection. Users will use **WorkBrowser** (page xxvi) to access these URLs.

- **Name** - Enter a name for this menu item.
- **URL** - Enter a URL.
- **Proxy required** - Recommended for securing access to an internal resource or website.

### Document Profile

Add WebDAV documents you want to make available to mobile users using **WorkDocs** (page xxvii).

- **Name** - A description of the document.
- **URL** - The URL of the WebDAV document source.
- **Proxy required** - Recommended for securing access to an internal resource or website.

The **WorkDocs** container app supports:

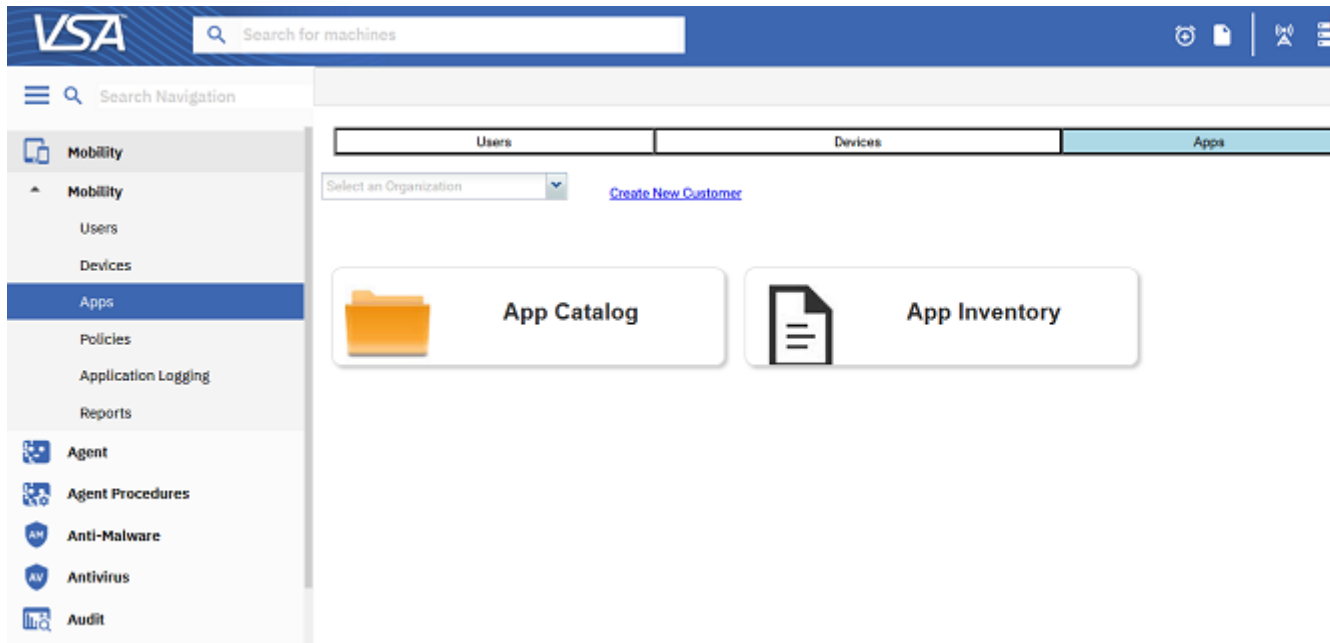
- The display and editing of shared and local Microsoft Office and PDF documents.
- The creation and storage of local secure documents on the user's mobile device. Documents stored locally are encrypted and remain isolated from the rest of the user's environment on the mobile device.

## Managing Apps on Devices

**Enterprise Mobility Management** can either require or disallow selected apps on mobile devices.

1. Navigate to the **Apps** page.

2. Select a customer organization.



3. Click the **App Catalog** (page xxv) tile to maintain a catalog of *app items* for the organization you have selected.

**Note:** The **App Inventory** page generates a list of candidate app items based on an audit of all mobile devices managed by **Enterprise Mobility Management**. Use it to determine the format of app records you want to add to the **App Catalog**.

4. Use the **Apps Profile** (page xxiii) for each organization and security group to to require or disallow apps on user devices. These apps must have previously been added to the **App Catalog** for that organization.

## Configuring the App Catalog

The **App Catalog** maintains a catalog of app items. Each app item uniquely identifies a single app that can be required or disallowed on a mobile device. Once added to the catalog, app items can then be added to the **app profile** (page xxiii) of a policy assigned to a customer organization.

**Note:** An **App Catalog** is maintained for each customer organization individually.

### Adding a New App Item

1. Select the correct customer organization, if necessary.
2. Click **New**.
  - **Store App** - If selected, a **URL** must be specified.
3. If you select a **Store App**, a **New Store App** dialog displays.
  - Select the **Android** or **iOS** radio option.
  - Optionally enter a search term to filter the list of apps returned from the selected store.
  - Select an app in the list.
  - Click either the **Add** or **Add & New** button.

Your app has been added to the **App Catalog**.

## Working with Existing App Items

The **Actions** menu provides the following options for existing apps in the **App Catalog**.

- **Edit** - Edits a selected app item in the **App Catalog**.
- **Delete** - Deletes a selected app item from the **App Catalog**.

## Viewing App Inventory

**Enterprise Mobility Management > Apps > App Inventory**

The **App Inventory** page generates a list of app items based on the apps discovered on managed mobile devices, for the selected customer organization and policy profile. Use it to determine the format of app records you want to add to the **App Catalog** (page xxv).

### 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`.

## WorkBrowser and WorkDocs

**Enterprise Mobility Management** provides mobile device users safe, secure access to their company's internal websites and documents using two container apps.

- **WorkBrowser** (page xxvi) - Provides secure access to internal websites.
- **WorkDocs** (page xxvii) - Enables secure viewing and editing of documents on internal networks or stored locally on mobile devices.

## Using WorkBrowser

The **WorkBrowser** is ideal for anyone who's mobile and needs to stay connected to the office. **WorkBrowser** provides secure access—in flight and at rest—to internal intranets, files and directories. Selected files can be edited using **WorkDocs** (page xxvi).

### Downloading WorkBrowser

- **Apple devices** (<https://itunes.apple.com/us/app/kaseya-workbrowser/id953111090?mt=8>) - Download using the link provided in your email invitation.
- **Android devices** (<https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workbrowser>) - Download using the link provided in your email invitation.

### Requirements for Each Managed Mobile Device

- iOS version 7.0 and above
- Android version 4.0.3 and above

### Passcodes

You may be prompted to create an *app-level* PIN (also called a passcode or access code) to use **WorkBrowser**. Thereafter, you will need to enter this PIN each time you access the **WorkBrowser** app.

## Sites

The [Sites](#) list shows all the websites you have access to via **Enterprise Mobility Management**.

## Viewing and Editing Files

When browsing web sites in [WorkBrowser](#) you can view files. Viewed files can be edited using [WorkDocs](#) (page xxvii).

---

# Using WorkDocs

[WorkDocs](#) enables you to view or edit documents stored on an internal network or stored locally in [Secure Storage](#) on your mobile device. You can also move, copy or delete documents. Documents stored locally are encrypted and remain isolated from the rest of the environment on the mobile device.

## Downloading WorkDocs

- **Apple devices** (<https://itunes.apple.com/us/app/kaseya-workdocs/id953111338?mt=8>) - Download using the link provided in your email invitation.
- **Android devices** (<https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workdocs>) - Download using the link provided in your email invitation.

## Requirements for Each Managed Mobile Device

- iOS version 7.0 and above
- Android version 4.0.3 and above

## Passcodes

You may be prompted to create an *app-level* PIN (also called a passcode or access code) to use [WorkDocs](#). Thereafter, you will need to enter this PIN each time you access the [WorkDocs](#) app.

## Sites

The [Sites](#) list shows all the [WorkDocs](#) sites you have access to via **Enterprise Mobility Management**. Each [WorkDocs](#) site provides access to a navigation tree of folders and documents. *These documents are not stored on your device unless they are in [Secure Storage](#).*

## Secure Storage

The [WorkDocs](#) site also displays a [Secure Storage](#) folder of local documents stored on your device. The same [Secure Storage](#) folder is shared across all the [WorkDocs](#) sites you have access to.

## Authorization

Depending on the authorization assigned to the document you may be prompted to enter credentials.

## Editing Documents

Selecting a file allows you to preview the file. Select the [Edit](#) button over the previewed file to launch the file editor.

When the editor first loads you can select the [File](#) icon and use the [Save as](#) option to save the current file to a new name and/or location. Once you start making edits to the file the [File](#) icon can be used to save the current file to the same name and location of the original file. If a save fails, verify you have write access to the document location.

## Move, Copy and Delete Files

You can move, copy, and delete files from any location.

- Select [Edit](#) from above the document source file list to see these options.
- Select the file(s) you want to perform the move, copy or delete action on.

- For **Copy** and **Move** actions you will be prompted to provide the name and location for the new file. To save a local copy of the file, copy or move to your **Secure Storage**.
- To delete a file, select the **Delete** button. You will be prompted to confirm file deletions.

### Favorites

Any folder beneath the root directory can be saved as a **Favorite**. To mark a folder as a **Favorite** select the 'star' icon at the bottom of the file list. The 'star' icon will darken to show this folder is now a **Favorite**. Folders marked as a **Favorite** are displayed along with your document sources. Selecting the **Favorite** provides a shortcut to go directly to that location.

---

## Logging Module Activity

You can review application activity in the **Mobility** module using the **Application Logs** page. If information has changed or been removed unexpectedly, check this page to determine what events and administrators may have been involved.

Entries include:

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

Logged events include:

Clear Passcode  
 Created Device  
 Deleted Device  
 Found Device  
 Invitation Resent  
 Lock Device  
 Lost Device  
 Mark Commands Complete  
 Process Alert  
 Request Checkin  
 Request Logs  
 Run Audit  
 Scheduled Audit  
 Sound Alarm on Device  
 Start Tracking Device  
 Stop Tracking Device  
 Updated Device  
 Wipe Device

---

## Reports

The **Reports** page displays the user count and device count registered for each customer.

<b>Overview</b> .....	i
<b>Enterprise Mobility Management Module Minimum Requirements</b> .....	ii
<b>User Interface</b> .....	iii
<b>Onboarding Customers</b> .....	iii

<b>Onboarding Users .....</b>	<b>vi</b>
<b>Managing Users Manually .....</b>	<b>vii</b>
<b>Importing Users Using CSV.....</b>	<b>vii</b>
<b>Importing Active Directory Users .....</b>	<b>viii</b>
<b>Configuring Active Directory Integration .....</b>	<b>ix</b>
<b>Inviting Users .....</b>	<b>xii</b>
<b>Managing Devices .....</b>	<b>xiii</b>
<b>Command Status .....</b>	<b>xv</b>
<b>Audit Actions .....</b>	<b>xvi</b>
<b>Tracking Actions.....</b>	<b>xvi</b>
<b>Messaging Actions .....</b>	<b>xvi</b>
<b>Lost / Found Actions .....</b>	<b>xvi</b>
<b>Devices Actions .....</b>	<b>xvii</b>
<b>Alerts Actions .....</b>	<b>xvii</b>
<b>Viewing Device Details.....</b>	<b>xvii</b>
<b>Configuring Policies.....</b>	<b>xix</b>
<b>MDM Profiles .....</b>	<b>xxi</b>
<b>Configuring the MDM Security Profile .....</b>	<b>xxi</b>
<b>Configuring the iOS Profile.....</b>	<b>xxi</b>
<b>Configuring a Web Clip Profile .....</b>	<b>xxii</b>
<b>Configuring a WiFi Profile.....</b>	<b>xxii</b>
<b>Configuring a Mail Profile .....</b>	<b>xxiii</b>
<b>Configuring an Apps Profile .....</b>	<b>xxiii</b>
<b>BYOD Profiles .....</b>	<b>xxiv</b>
<b>Managing Apps on Devices.....</b>	<b>xxiv</b>
<b>Configuring the App Catalog.....</b>	<b>xxv</b>
<b>Viewing App Inventory .....</b>	<b>xxvi</b>
<b>WorkBrowser and WorkDocs .....</b>	<b>xxvi</b>
<b>Using WorkBrowser .....</b>	<b>xxvi</b>
<b>Using WorkDocs .....</b>	<b>xxvii</b>
<b>Logging Module Activity .....</b>	<b>xxviii</b>
<b>Reports .....</b>	<b>xxviii</b>
<b>Index .....</b>	<b>31</b>



# Index

---

## A

Alerts Actions • xvii  
Audit Actions • xvi

## B

BYOD Profiles • xxiv

## C

Command Status • xv  
Configuring a Mail Profile • xxiii  
Configuring a Web Clip Profile • xxii  
Configuring a WiFi Profile • xxii  
Configuring Active Directory Integration • ix  
Configuring an Apps Profile • xxiii  
Configuring Policies • xix  
Configuring the App Catalog • xxv  
Configuring the iOS Profile • xxi  
Configuring the MDM Security Profile • xxi

## D

Devices Actions • xvii

## E

Enterprise Mobility Management Module Minimum  
Requirements • ii

## I

Importing Active Directory Users • viii  
Importing Users Using CSV • vii  
Inviting Users • xii

## L

Logging Module Activity • xxviii  
Lost / Found Actions • xvi

## M

Managing Apps on Devices • xxiv  
Managing Devices • xiii  
Managing Users Manually • vii  
MDM Profiles • xxi  
Messaging Actions • xvi

## O

Onboarding Customers • iii  
Onboarding Users • vi  
Overview • i

## R

Reports • xxviii

## T

Tracking Actions • xvi

## U

User Interface • iii  
Using WorkBrowser • xxvi  
Using WorkDocs • xxvii

## V

Viewing App Inventory • xxvi  
Viewing Device Details • xvii

## W

WorkBrowser and WorkDocs • xxvi