11

Setting

Setting

Customize various settings in the Admin Portal. Set the Knox Manage Agent policies for user devices and configure Keepalive, the program which is used for checking the statuses of devices. You can also manage the templates of messages for users and the master data related to user information. In addition, you can change the logo and header or manage other administrators' accounts.

This chapter explains the following topics:

Configuring the environment

Configure the environment settings for the Admin Portal. You can customize the values for the provided setting options.

To configure the environment, complete the following steps:

1. Navigate to **Setting** > **Configuration** > **Basic Configuration**.
2. On the "Basic Configuration" page, customize the environment settings. For more information about the environment settings, see List of environment settings.
3. Click **Save**.

List of environment settings

The environment settings by category are as follows. All options have default values and the values can be modified.

Preferences

Country/Time

Option	Description
Default Country Code	Select the country of the Admin Portal. The country code and the corresponding language are used for user agreements, privacy policy, administrator/user enrollment, and public application enrollment on user devices.
Time Zone	Select the time zone of the Knox Manage server. Based on the time zone, the information in the Admin Portal is displayed, tasks and events scheduled by administrators are performed, and user and device statistics are collected.

Logo

For more information about setting the log, see Setting the logo.

Option	Description
Logo Image	Click **Select Image** and upload the image file of your company logo. The image must be a GIF, JPG, PNG, or BMP file. The file cannot be larger than 190 x 33 and must be 1 MB or lower.Click **Default** to use the default image as your company logo.
Header Color	Click the color box and set a color for the header.
Header Font Color	Click the color box and set a color for the header text.
Preview	Preview the company logo.

Authentication/Login

Configure the settings about the login environment and the administrator account.

Option	Description
Two-Factor Authentication	Enable the use of OTP authentication as well as an account ID and password when administrators sign in to the Admin Portal. For OTP authentication, the administrator's mobile phone number or email address is required.
Allow Multi-point Logins	Allow concurrent logins to the Admin Portal.
Action When Admin Login Fails	Select the response of the Knox Manage server when there are successive failed login attempts. • **Deactivate account until an upper level admin unlocks** • **Disable login for 10 mins** • **No action**
Maximum Failed Login Attempts	Enter the maximum number of failed login attempts. When users exceed the maximum, their accounts are locked. You can enter a value from 3 to 10.
Inactivity Limit on Admin Accounts (days)	Enter an inactivity limit for administrator accounts. If sub-administrators or read-only administrators do not sign in for longer than the limit you set, their accounts are locked. To unlock their accounts, they must ask the super administrator. You can enter a value from 10 to 9999.
Maximum Session Timeout (min)	Enter the maximum session time limit for the Admin Portal. If the limit is exceeded, you will be signed out automatically. You can enter a value from 1 to 60.

Device

Device

Configure the device management settings.

Option	Description
Based on Last Seen (time)	Enter the standard time gap for connection of the device and server. This standard is used for displaying information in the **Last Seen** column of the device list in the **Device** menu. • If the gap between the current time and the last connected time of a device does not exceed the standard, the Last Seen information of the device is displayed in green. • If the gap between the current time and the last connected time of a device exceeds the standard, the Last Seen information of the device is displayed in red. The value is entered in hours.
Limited Enrollment	Enable enrollment of mobile devices using their IMEI or serial numbers.
Device Location View Period (days)	Enter the period for saving device location data. You can view the location of devices saved during that time period.
Maximum Number of Active Devices per User	Select the number of devices that can be enrolled per user.
APNs Topic for iOS	When you register an APNs certificate in the Admin Portal, this value is automatically entered. If the value is different from the value in the Current Subject Name field in **Setting** > **iOS** > **APNs Setting**, complete the following steps: 1. Start the command prompt on your PC. 2. Enter `C:/> keytool -v -list -storetype pkcs12 -keystore {APNS certificate filename}.p12 | find "UID"`. 3. Change the APNs Topic value to the value appearing after "`UID=`".
Daily retries for device commands in queue	Select how many notifications you will receive per day to send device commands which have been sent but not applied successfully. • **0**: You will receive no notification. • **1**: You will receive a notification at 11 PM local time per tenant. • **2**: You will receive a notification at 10 AM and 10 PM local time per tenant. Unapplied device commands are listed in **History** > **Device Command in Request**.
Camera Option from Lock Screen for iOS	Enable the camera feature on iOS devices when the device screen is locked.
Delete App upon Unenrollment	Enable the applications installed on a device to be deleted when the device is unenrolled. The deletion targets are internal applications for Android devices and all applications installed through Knox Manage for iOS devices.

Option	Description
Notification that policy is not applied	Enable sending a notification to the device when no profile is applied to a group or organization. When the user turns off the alarm in the device's setting menu, notifications on whether the profile is applied will not appear.
Direct boot command polling interval for Android (min)	Set the polling cycle to send the Knox Manage command for Android devices. If the polling interval is 0, polling will not be performed. However, polling is executed once after the Knox Manage Agent is started.

Inventory Scheduler

Configure the interval to collect the device inventory by mobile OS.

Option	Description
Inventory Collection Interval for Android (hr)	Enter the interval for collecting the inventory information for Android devices. You can enter a value from 4 to 24 or 0 (the device inventory is not collected). **NOTE** To set an interval for collecting the location data of Android devices, navigate to **Profile**. Click a profile name and click **Modify Policy** > **Android Enterprise** or **Android (Legacy)** > **Location** > **Report device location interval**. For more information, see Location (Android Enterprise) or Location (Android Legacy).
Inventory Collection Interval for iOS (hr)	Enter the interval for collecting the inventory information for iOS devices. You can enter a value from 4 to 24 or 0 (the device inventory is not collected).
Inventory Collection Interval for Windows (hr)	Enter the interval for collecting the inventory information for Windows devices. You can enter a value from 4 to 24 or 0 (the device inventory is not collected).

App & Service Desk

Application

Configure the application deletion setting.

Option	Description
Manage Deletion	Select the area to delete applications from. • **Console**: Deletes applications only from the application list in the Admin Portal. • **Console + Device**: Deletes applications from the application list and also from the devices in the assigned groups/organizations.

Knox Manage App Store

Configure the activation of the review feature in the Knox Manage App Store.

Option	Description
Knox Manage App Store Review	Enable users to evaluate and write a review about applications in the Knox Manage App Store.

Service Desk

Enter the service desk information displayed on user devices.

Option	Description
Service Desk Email	Enter the service desk email address.
Service Desk Phone	Enter the service desk phone number.

Setting Knox Manage Agent policies

You can set policies, such as login, screen lock, and compliances, for the Knox Manage Agent. When the user runs the Knox Manage Agent, the defined policies are applied to the device.

To configure policies for the Knox Manage Agent, complete the following steps:

1. Navigate to **Setting** > **Configuration** > **Knox Manage Agent Policy**.
2. On the “Knox Manage Agent Policy” page, click the ”Default” tab.
   - The policies set in the “Default” tab will be applied to every group or organization that is not assigned specific policies in your tenant.
   - To apply different agent policies to specific groups or organizations, click + and configure an agent policy set.
3. Configure the policy details. For more information about the applicable policies, see Applicable policies for Knox Manage Agent.
4. Click **Save & Apply**.
5. In the "Save Changes" window, click **OK**.

Applicable policies for Knox Manage Agent

The following policies are available for Knox Manage Agent:

Policy	Description	Supported devices
Maximum Failed Sign-in Attempts	Set the maximum number of incorrect password attempts before access is restricted. The value can be between 0 - 10 times.	Android iOS Windows 10
> Sign-in Failure Policy	Select the action to be performed when the maximum number of failed attempts is reached. • **None**: The device is unrestricted. • **Factory reset**: Resets the user device. • **Lock device**: Locks the device. • **Lock Knox Manage Agent**: Locks the Knox Manage Agent.	Android iOS Windows 10
Use Lock Screen	Allows the use of the lock screen for the Knox Manage Agent.	Android iOS Windows 10

Policy	Description	Supported devices
Install Area	Select where the Knox Manage Agent will be installed. • **General Area** • **Knox Workspace**	Android
Lock Screen After (sec)	Set the duration for locking the device when the user has not set up a password for the screen lock. The value can be between 300 – 3600 seconds.	Android iOS Windows 10
Lock Knox Workspace Screen After (sec)	Set the duration for locking the Knox Workspace area screen when the application is not used for a certain period of time. The value can be between 300 – 3600 seconds. **NOTE** The KWS license is required to set this policy.	Android
> Fingerprint Authentication	Allows the use of the fingerprint unlock control.	Android iOS
> Maximum Password Entry Attempts	Set the maximum number of incorrect password attempts before access is restricted. The value can be between 0 - 10 times.	Android iOS Windows 10
>> Password Entry Failure Policy	Select the action to be performed when the maximum number of failed attempts is reached. • **None**: The device is unrestricted. • **Factory reset**: Resets the user device. • **Lock device**: Locks the device. • **Lock Knox Manage Agent**: Locks the Knox Manage Agent.	Android iOS Windows 10
> Minimum Password Length	Set the minimum length of the password. The value can be between 6 – 20 characters.	Android iOS Windows 10
> Requirements for Password	Select to include which character type in a password. • **At least 1 capital letter** • **At least 1 number** • **At least 1 special character**	Android iOS Windows 10
> Allow 3 Consecutive Characters	Allows 3 or more consecutive characters to be used in a password.	Android iOS Windows 10

Policy	Description	Supported devices
KM Agent Auto Update	Sends a notification to the user when a new version of the KM agent is available on the device and prompts the user to update it.	
Allow Unenroll Request	Allows the disabling buttons on the device so that deactivation requests can be sent.	Android iOS
Show All Applied Policies	Allows showing all of the policies applied on the policy list in the Knox Manage Agent.	Android iOS
Limitation of the Download Screen Display in the Public Application	Limits the display of the download screens of public applications in the Knox Manage Agent. Only the registered public applications are displayed on the download screen.	Android iOS
Availability for Android Version Control	Checks the Android OS version and performs actions when the device violates the OS version and conditions.	Android
> Recommended Version	Sets the Android OS version.	Android
> Conditions for Checking OS Version	Sets the conditions for the recommended OS version to apply the violation measures. • **Allow recommended version only** • **Allow recommended version or below only** • **Allow recommended version or above only**	Android
> OS Version Violation Policy	Select an action to perform when the device violates the OS version and conditions. • **Lock device**: Locks the device. • **Lock EAS**: The preloaded email application will be hidden and the user cannot use it.	Android
Availability for iOS Version Control	Checks the iOS OS version and performs actions when the device violates the OS version and the conditions.	iOS
> Recommended Version	Sets the iOS OS version.	iOS
> Version Control Policy	Sets the conditions for the recommended OS version to apply the violation measures. • **Allow recommended version only** • **Allow recommended version or below only** • **Allow recommended version or above only**	iOS
> OS Version Violation Policy	Select an action to perform when the device violates the OS version and the conditions. • **Lock device**: Locks the device.	iOS

Policy	Description	Supported devices
Windows 10 Desktop Data Deployment	Sets the data distribution mechanisms for Windows 10 desktops.	Windows 10
> PPKG File	Select a data provisioning package (PPKG) file to apply to the desktops. In the TMS Admin Portal, navigate to **Management** > **Service Profile**, and click . Then, navigate to **Settings** > **Windows 10** > **PPKG File Management**, and select a provisioning package.	Windows 10
Windows 10 Mobile Data Deployment	Sets the data distribution mechanisms for the Windows 10 mobile devices.	Windows 10
> PPKG File	Select a data provisioning package (PPKG) file to apply on the mobile devices. In the TMS Admin Portal, navigate to **Management** > **Service Profile**, and click . Then, navigate to **Settings** > **Windows 10** > **PPKG File Management**, and select a provisioning package.	Windows 10

Configuring the Keepalive settings

You can configure the Keepalive settings to check the connection between the Knox Manage server and the device. The Knox Manage server checks the connection between the server and the device at the set interval.

To configure the Keepalive settings, complete the following steps:

1. Navigate to **Setting** > **Configuration** > **Keepalive**.
2. Click next to **Keepalive** to enable the feature.
3. Select a target type between **Global Setting** and **Set by Group/Organization**.
   - **Global Setting**: Applies the Keepalive settings to all policies.
   - **Set by Group / Organization**: Applies the Keepalive settings to selected groups or organizations.

4. Configure the Keepalive settings.
    - **Keepalive Expiration (days)**: Select a period between 3 and 365 days. If there is no communication between the Knox Manage server and a device for the set period, it attempts to re-establish a connection directly. If the device still fails to establish communication, then its status changes to Disconnected.
    - **Keepalive Expiration (hours)**: Select a cycle to check the connection status by checking the last time the device and the server communicated.
    - **Group / Organization**: Click **Select** and select user groups or organizations to apply the Keepalive settings.
5. Click **Save**.

Adding a notice

Add a notice for device users. When you add multiple notices, the notice periods cannot overlap. On user devices, notices are displayed in the language that the user sets when signing in to Knox Manage.

To add a notice, complete the following steps:

1. Navigate to **Setting** > **Notice**.
2. On the “Notice” page, click **Add**.
3. Enter the subject and content of the notice and set the notice period.
    - The start date of the notice must be within a month of the current day.
    - Do not enter a space at the end of the notice content.
4. Click **Save**.

Managing message templates

Knox Manage provides message templates and helps you send text messages or emails with a good and standardized format. In addition to basic message templates, you can add new templates for general emails or emails to send temporary passwords to users.

Basic message templates

The basic message templates are as follows:

Template type	Message type	Template name
Email	Agent Installation	Email_Agent Installation
	Administrator Authentication	Email_Admin OTP
	Administrator Account Information	Email_Admin ID
	Administrator Temporary Password	Email_Admin Temporary Password
	User Temporary Password	Email_User Password Reset
	Apple VPP	Email_Apple VPP Invite: The email template for inviting VPP users
		Email_Apple VPP Redeem: The email template for installing purchased VPP applications through redeemable codes
SMS	Agent Installation	• User Credential • Public Store Address • Direct Installation • KME Activation Address
	Administrator Authentication	Admin OTP SMS
	Administrator Temporary Password	Admin Temporary Password

Adding message templates

You can add general purpose email templates or templates for sending out temporary passwords.

To add a new template, complete the following steps:

1. Navigate to **Setting** > **Message Template**.
2. On the “Message Template” page, click **Add**.
3. On the “Add Message Template” page, enter the following information:
   - **Template Name**: Enter the template name.
   - **Template Type**: Select a type of the message template between **Email** and **SMS**.
   - **Message Type**: Select the purpose of the email.
   - **Description**: Enter a brief description of the template.
   - **Message Subject**: Enter the email subject line.
   - **Content**: Enter the body of the message.
     - If you click **Search**, you can select reference items that will be replaced with actual values when the email is sent. Double-click an item to add it to content. For emails that send a temporary password to a user, **Temporary Password** must be added.
     - To add an image to the template, click  and add an image in the URL format.
4. Click **Save**.
5. In the "Save Message Template" window, click **OK**.

NOTE

- Among the reference items in the “Reference Items” window, **Copyright**, **EMM/TMS Service URL**, **OTP Issuing URL** are provided by Knox Manage. When you add one of the items, their actual values are displayed in the template. If the values remain blank, contact the Knox Manage Support team.
- Some characters can be automatically converted due to a cross-site scripting (XSS) issue while adding a new template. For example, “onclick” is converted to “on-click.”

  The following characters are converted: onafterprint, onbefor, onerror, onhashchange, onload, onmessage, onoffline, ononline, onpage, onpopstate, onresize, onstorage, onunload, onblur, onchange, oncontextmenu, onfocus, oninput, oninvalid, onreset, onsearch, onselect, onsubmit, onkey, onclick, ondblclick, ondrag, ondrop, onmouse, onscroll, onwheel, oncopy, oncut, onpaste, onabort, oncanplay, oncuechange, ondurationchange, onemptied, onended, onpause, onplay, onprogress, onratechange, onseek, onstalled, onsuspend, ontimeupdate, onvolumechange, onwaiting, onshow, ontoggle, script, frame, object, embed, meta, div, style, form, isindex, body, base, bgsound, xml, document, applet, grameset, layer, alert

Managing added message templates

You can modify or delete newly added message templates. Basic message templates cannot be modified or deleted.

Modifying message templates

To modify message templates, complete the following steps:

1. Navigate to **Setting** > **Message Template**.
2. On the “Message Template” page, click the checkbox for the template you want to modify.
3. On the “Modify Message Template” page, modify the existing information.
4. Click **Save**.
5. In the "Save changes" window, click **OK**.

Deleting message templates

To delete message templates, complete the following steps:

1. Navigate to **Setting** > **Message Template**.
2. On the “Message Template” page, click the checkbox for the template you want to delete.
3. In the "Delete" window, click **OK**.

Managing master data

Master data contains the following user information. The data appears as select options when you add a single user.

- Position: The user's position in the company
- Security Level: The user's security level related to their access of company data
- Site: The user's work site

Adding master data

To add a new value for master data, complete the following steps:

1. Navigate to **Advanced** > **Master Data**.
2. In the "Category" area, select a category between **Position**, **Security Level**, and **Site**.
3. In the "Master Data" area, click **Add**.
4. In the "Add Master Data" window, enter the data information.
   - **Category**: The data category that you selected in step 2 is pre-entered.
   - **Key**: Enter a key or code.
   - **Value**: Enter a value.
   - **Select or not**: Select the value to be the default in the data category.

   NOTE If you want to add additional reference codes, click **Reference Code** > + and add a reference code.

5. Click **Save**.

Modifying master data

To modify master data, complete the following steps:

1. Navigate to **Advanced** > **Master Data**.
2. On the "Master Data" page, select a category and search for the value you want to modify.
3. Click the checkbox for the value you want to modify and click **Modify**.
4. In the "Modify Master Data" window, modify the existing information.
5. Click **Save**.

Deleting master data

To delete master data, complete the following steps:

1. Navigate to **Advanced** > **Master Data**.
2. On the “Master Data” page, select a category and search for the value you want to delete.
3. Click the checkbox for the value you want to delete and click **Delete**.
4. In the "Delete" window, click **OK**.
    - The keys provided as master data by default cannot be deleted.

Setting the logo

Change the Knox Manage logo to your company logo and customize the color for the header and/or header text.

To set the logo, complete the following steps:

1. Navigate to **Setting** > **Configuration** > **Basic Configuration**.
2. Modify the logo image and/or the colors.
    - **Logo Image**: Click **Select Image** and upload the image file of your company logo. The image must be a GIF, JPG, PNG, or BMP file. The file cannot be larger than 190 x 33 and must be 1 MB or lower. Click **Default** to use the default image as your company logo.
    - **Header Color / Font Color**: Click the color box and set a color for the header and the header text.
    - **Preview**: Preview the company logo.
3. Click **Save**.

Managing administrator accounts

Add and manage other administrators' accounts. Management of administrator accounts includes changing passwords, selecting profiles and organizations to manage for administrators, and activating technical support administrator access to user devices.

Administrators in Knox Manage are categorized into three types:

Type	Description
Super administrators	• Add, modify, delete, activate, and deactivate sub-administrator accounts. • Grant sub-administrators administration rights. • Select profiles to manage for sub-administrators. • Select organizations to manage for sub-administrators.
Sub-administrators	• Manage the profiles designated by a super administrator or the profiles they created. • Manage the organizations designated by a super administrator or the organizations they created.
Read-only administrators	Only view all menus, including menus for administrators, in the Admin Portal.
Service administrators (read only)	Sends device commands. You can allow all device commands or select specific device commands for service administrator use.

Adding an administrator

To add an administrator account, complete the following steps:

1. Navigate to **Setting** > **Administrator**.
2. On the "Administrator" page, click **Add**.
3. On the "Add Administrator" page, enter the following information:
   - **Event Type**: Select how to add an administrator.
     - **New**: Create a new administrator account.
     - **EMM User**: Select a user from among the previously added users to be an administrator.
   - **Admin ID**: Enter the administrator ID.
   - **Admin Name**: Enter the administrator name.
   - **Email**: Enter the administrator's email address.

- **Mobile Number**: Enter the mobile phone number of the administrator.
- **Type**: Select the administrator type.
- **Menu**: Select the administration rights to give to the administrator.
- **Service Type**: Select which device commands service administrators are allowed to use.
  - **Allow All Device Command**: Allows service administrators to use all device commands.
  - **Selected Device Command Only**: Allows service administrators to use only selected device commands.
- **Device Command**: Select a device command to allow for service administrators.

4. Click **Save**.

Changing passwords (super administrators)

Super administrators can change their account passwords and the passwords of sub-administrator accounts.

To change passwords, complete the following steps:

1. Navigate to **Setting** > **Administrator**.
2. On the "Administrator" page, click the checkbox for an administrator you want to change the password of, and then click **Change Password**.
3. In the “Change Password” window, enter a new password.
4. Click **Save**.

Changing passwords (sub-administrators)

The initial password is designated by the super administrator. Sub-administrators must ask the super administrator for an initial password for their first login. After the initial login, the “Change Password” window will appear, allowing sub-administrators to change the password.

Selecting profiles to manage for sub-administrators

To select profiles to manage for sub-administrators, complete the following steps:

1. Navigate to **Setting** > **Administrator**.

2. On the "Administrator" page, click the checkbox for a sub-administrator you want to give profiles to manage to, and then click **Assign**.
3. In the “Select Profile” window, click the checkbox for profiles on the profile list, and then click **Assign**.
   - To delete the selected profiles from the selected profile list, click the checkbox that is checked already to delete them.
4. Click **Save**.

Selecting organizations to manage for sub-administrators

To select organizations to manage for sub-administrators, complete the following steps:

1. Navigate to **Setting** > **Administrator**.
2. On the "Administrator" page, click the checkbox for a sub-administrator you want to give organizations to manage to, and then click **Assign**.
3. In the “Select Organization” window, select an organization from the All Organizations area and click **Assign**.
   - To delete the selected organizations from the assigned organization list, click in the row of the organization you want to delete in the Selected Organization area.
4. Click **Save**.

Activating administrator accounts

When administrators do not sign in to Knox Manage for a long time, their accounts become inactive. If inactive accounts are used to attempt to sign in to Knox Manage, a message notifying that the account has been locked appears and the login attempt fails. Inactive accounts can be activated again only by super administrators.

To activate administrator accounts, complete the following steps:

1. Navigate to **Setting** > **Administrator**.
2. On the "Administrator" page, click the checkbox for an administrator you want to activate, and then click **Change Status**.
3. In the "Change Status" window, click **OK**.

NOTE If you click **Active** in the row of an administrator, you can deactivate the administrator.

Activating technical support administrators

When technical support is necessary, you can allow technical support administrators to control the Admin Portal. By activating technical support and setting the activation period, technical support administrators can access the Admin Portal through the TMS admin portal and provide technical support.

To activate technical support administrators, complete the following steps:

1. On the header, click ⓘ next to the account ID.
2. Click **Technical Support**.
3. On the "Technical Support" window, click **Activate Technical Support** and set the access period.
   - The start date of the access period is automatically set to the current date and can be modified.
4. Click **Save**.
5. In the “Save” window, click **OK**.