SAMSUNG

EMM

Administrator's Guide

Solution version 2.2.5

Published: January 2023

Table of Contents

Table of Contents

Table of Contents

Table of Contents

8

Content

9

Integration Services

Table of Contents

Table of Contents

12

Monitoring

13

Appendix

Table of Contents

Before using this information and the product it supports, be sure to read the general information on this page.

Publisher Samsung SDS Co., Ltd

Address 125, 35-Gil, Olympic-Ro, Songpa-Gu, Seoul, South Korea.

Email ems.support@samsung.com

Website www.samsungsds.com

DFARS Limited Rights Notice

LIMITED RIGHTS

Contractor Name: Samsung SDS Co. Ltd., via its distributor in the U.S., Samsung SDS America, Inc.

Contractor Address: Samsung SDS America, Inc.: 100 Challenger Road, 6th Fl., Ridgefield Park, NJ 07660 U.S.A.

The US Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(3) of the Rights in Technical Data--Noncommercial Items clause contained in the US Government contract under which the US Government has obtained a license to use this computer software. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the US Government, who has been provided access to such data must promptly notify the above named Contractor.

(End of legend)

FAR Limited Rights Notice

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under the US Government contract under which the US Government has obtained a license to use these data. These data may be reproduced and used by the US Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the US Government; except that the US Government may disclose these data outside the US Government for the following purposes, if any; provided that the US Government makes such disclosure subject to prohibition against further use and disclosure (if any).

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(End of notice)

Preface

Before getting started

For enhanced security on mobile devices, applications, and content, Samsung SDS EMM (hereinafter “EMM”) gathers personal information regarding users and devices. This may be prohibited by laws and regulations in your region. Please consult with your legal team to check related laws and regulations before gathering and utilizing personal information. Make sure to notify users of the terms of service, including privacy policies.

Users of this guide

This guide is written for administrators who utilize Samsung SDS EMM solution. It also covers users who manage the EMM service management, device and user management, policy management, security setting via certificates, and service environment. In order to use this solution effectively, the administrator must have the understanding and experience of the following:

- General knowledge on how to operate systems
- General knowledge on how to manage system data
- General knowledge on security setting via certificates
- General knowledge on how to manage and control devices
- General knowledge on how to use web applications

Conventions

This document uses the following conventions:

Convention	Description
Boldface	**Boldface** is used to graphical user interface elements, menus, navigation trees and directories within the main text.
“ “	“ “ double quotation marks using as below: • Graphical user interface pages, portals, windows • Referring to other booklets, white papers, etc., mention the author or publisher of the publication and mark the title of the book in double quotation marks
“Cross-reference”	“Cross-reference” is used to reference documents or other chapters in a document. If click the cross reference, it moves to the specified location.
`Monospace`	`Monospace` is used to commands, parameters, file names and codes. Also, the monospace font uses Courier New.
Picture	The picture is used to graphics, illustrations, screen captures, etc. to help understand documents.
Table	The table is used to easily identify and display large amounts of information in the document.

Notes

The Note is used to add additional information such as tips, recommendations, exceptions, and limitations.

NOTE In order to reflect filtered data again, click Refresh Data on the Add Common Group window.

Revision history

Solution version	Manual version	Manual revised date	Revised details
1.0.0	1.0.0	November 2014	Initially published.
1.0.1	1.0.1	December 2014	Version 1.0.1 published.
1.1.0	1.1.0	March 2015	Improved usability and security.
1.1.1	1.1.1	June 2015	Version 1.1.1 published.
1.1.2	1.1.2	June 2015	Version 1.1.2 published.
1.2.0	1.2.0	September 2015	High security and Enterprise security package
1.2.2	1.2.2	October 2015	The official terms are changed and UI/UX is improved. Profile settings are changed.
1.2.3	1.2.3	December 2015	The official terms are changed and UI/UX is improved.
1.3.0	1.3.0a	April 2016	Usability improvements • Support Android for work, etc.
1.4.0	1.4.0a	July 2016	• New Knox functions are supported. • Windows10 are supported for mobile, tablet and PC. • Convenience enhancement for IT administrators and users by enhancing Kiosk functions and enabling device activation by QR code.
1.4.1	1.4.1a	September 2016	Add the description for Audit logs.
1.5.0	1.5a	October 2016	Add the function. • The Sync service and KME service • Managing profile by using the components
1.5.1	1.5.1a	December 2016	• Add the option for searching Audit types • Add device status
1.6.0	1.6.0a	March 2017	Support Tizen Wearable devices.
1.6.1	1.6.1a	May 2017	• Improved Dashboard UI/UX. • Add an external sync service. • Add app access permission settings.

Solution version	Manual version	Manual revised date	Revised details
2.0	2.0a	September 2017	• Added an activation function for a device registered with IMEI. • Added the AppWrapper tool.
2.0.2	2.0.2a	February 2018	• Added APNs certificate settings. • Added a feature that can be used to deploy profiles upon changing organizations/groups. • Added a feature that can be used to apply profiles.
2.1	2.1a	April 2018	• Added DEP settings for iOS devices. • Added DeX policies for Android.
2.1.6	2.1.6a	December 2018	• Added Mobile Admin Portal guide. • Added Android Enterprise, VPP service • Improved functions and UX of E-FOTA, Kiosk Wizard.
2.2.0	2.2.0a	March 2019	• Added Samsung Cloud Connector guide. • Added Android Enterprise Enrollment. • Added Android Enterprise App Deployment • Added Android Enterprise Activation. • Added device commands.
2.2.4	2.2.4a	November 2019	Overall revisions to the guide due to improvements to the Admin Portal's UI/UX: • Added anti-malware service. • Added the E-FOTA Advanced service. • Added network usage monitoring. • Added SSO (Single Sign-on) service. **NOTE** The solution version 2.2.4 is intended for our client, Unicus, and does not support the Android Legacy, iOS, and Knox VPN platforms or the Exchange and Connector functions.
2.2.5	2.2.5a	January 2020	• Added Android Enterprise profile policies. • Improved profile modification. • Improved EMM applications. • Improved E-FOTA Advanced. • Improved Network usage. • Improved Admin Portal UI/UX.
2.2.5.1	2.2.5b	March 2020	• Added DualDAR. • Improved Admin Portal UI/UX.

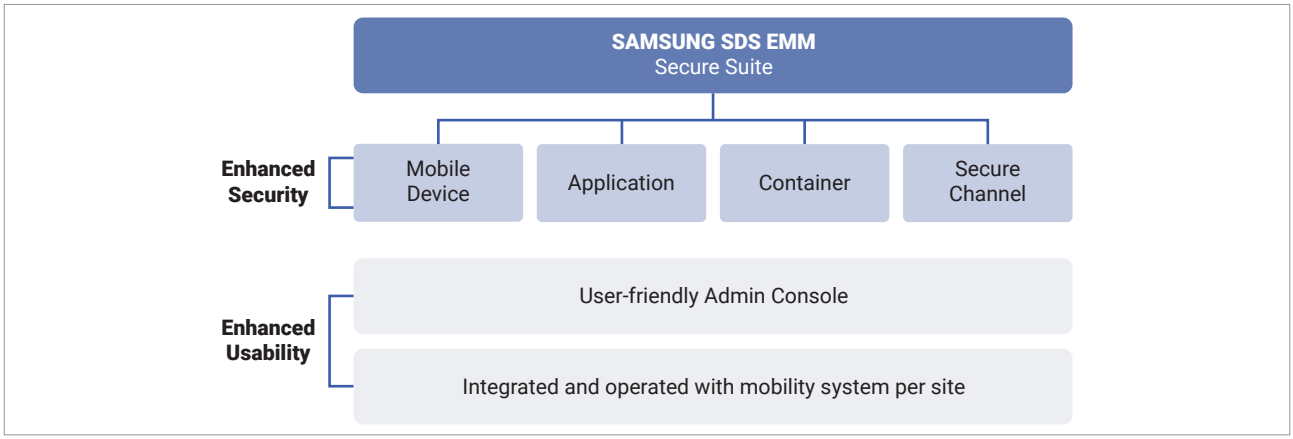
Solution version	Manual version	Manual revised date	Revised details
2.2.5.2	2.2.5c	December 2020	• Added multilicense. • Added social distance monitoring. • Improved terms and policies settings.
2.2.5.3	2.2.5d	March 2021	• Added Content Push. • Added Managed Configuration of Internal Apps. • Added CAC Sign-In.
2.2.5.4	2.2.5e	June 2021	• Dual DAR for Android Enterprise. • Work Profile on company-owned Support. • VPN Chaining.
2.2.5.5	2.2.5f	Nov 2021	• Support for XAPK type applications. • Support for Managed Google Play Web applications. • Support for iOS DEP users bulk assignment and usability improvement. • Improved iOS VPP applications assignment. • Support for new OS (Android 12, iOS 15)
2.2.5.6	2.2.5g	March 2022	• Support for Azure AD integration. • Support for controlling the number of devices for application installation. • Supporting iOS version changed.
2.2.5.7	2.2.5h	September 2022	• Google EMM API Deprecation • Support for new OS (Android 13)
2.2.5.8	2.2.5i	December 2022	• Support for Dual DAR Fully Managed • Support for certificate pre-installation

1

Introducing Samsung SDS EMM

Introducing Samsung SDS EMM

Samsung SDS EMM is an Enterprise Mobility Management solution which provides integrated management of mobile devices. Various policies can be customized for device management and assigned to mobile devices. Applications can be assigned to be only available to employees on their mobile devices while working. Once IT admin register the employees and their devices, the integrated management of mobile devices begins. Improve business efficiency and secure company data using EMM.



This chapter explains the following topics:

EMM strengths

Optimized Admin Portal

The user interface of the Admin Portal is designed to be administrator-centric. You can easily monitor the security status of activated devices and quickly collect information needed for prompt action.

Support of differentiated Samsung Knox

EMM supports the latest firmware of Samsung Knox, the mobile enterprise security platform embedded into Samsung devices. In addition, EMM fully guarantees fully supports for the latest Knox API.

Integrated management of Android Enterprise devices

EMM provides a full management service for any type of Android Enterprise device. You can save service support costs through the easy assignment of policies, applications, and the latest updates. For more information about the Android Enterprise type, see Activating Android Enterprise (AE) devices.

Bulk device activation and application assignment

EMM provides the means for the easy and quick activation of mobile devices through Knox Mobile Enrollment (KME) for Android devices or the Device Enrollment Program (DEP) for iOS devices. In the case of iOS devices, Apple's Volume Purchase Program (VPP) is also available to help conveniently assign the desired applications.

Optimal management of OS versions using E-FOTA

EMM enables wireless firmware management via an Enterprise Firmware-Over-The-Air (E-FOTA) service (for both Cloud and on-premise systems). E-FOTA helps resolve security risks for vulnerable OS versions and guarantees compatibility between software developed in the company and any new OS versions.

Dual DAR encryption

The Dual DAR solution provides dual encryption through two layers of encryption. EMM fully protects data in Dual DAR Workspace with Dual DAR on Android Legacy or Android Enterprise (Fully Managed or Work Profile on company-owned) devices that support Samsung Knox 3.3 or higher and Android File Based Encryption (FBE). Dual DAR requires the Dual DAR licenses and settings to be registered in the Admin Portal. For more information, see Setting the Dual DAR and https://docs.samsungknox.com/whitepapers/knox-platform/DualDAR.htm.

Detects and get rid of viruses, spyware, trojan, worms and other dangerous files using Anti-Malware

EMM provides protection against malware. With Anti-Malware, devices can stay free from any virus or malware. Only the V3 application provided by AhnLab is available for Anti-Malware.

The EMM Guardian feature protects devices safely even when they are factory reset

Generally, EMM solutions are not equipped with security policies because EMM is also deleted when a device is factory reset. Samsung SDS EMM provides the Guardian feature to detect EMM deletion when the device is factory reset, automatically controls the device's I/O, and induces EMM reinstallation to prevent malicious data leakage due to theft or loss of the device.

- Device I/O controls: Camera, External memory, USB connection, Bluetooth, Tethering, Screen capture

Storage of device analysis data

In addition to monitoring devices in real time, EMM also provides audits. You can check events that occur in the system, applied policies, tampering and compliance violations, etc., and take appropriate actions against them.

Provides highly secure and reliable two-way push service with Samsung SDS Push

EMM not only supports both major mobile devices platforms; Android and iOS and Windows 10 Mobile, but also capable of flexibly extending service even with an increase in devices. By overcoming the limits of public push service, Samsung SDS Push provides high quality two-way push with a 100% delivery rate, guaranteed message ordering, and duplicate delivery prevention. It securely protects both the packets and data delivered during communication due to the secured communication channels.

- Supports multiple platforms (Android, iOS, Windows 10 Mobile) and multiple applications
- Supports safe and reliable high-quality two-way push services
- Supports high quality two-way push with a 100% transfer rate, guaranteed message ordering, and duplicate delivery prevention

Provides content push service

Send files such as images, files, texts, and videos that are added to the EMM Admin Portal to mobile devices through the content push service. EMM delivers content files stored on the EMM server to Android and iOS devices quickly and safely via the Mobile Content Management (MCM) feature.

Easy creation of launcher applications with Kiosk Wizard

EMM provides Kiosk Wizard that helps you set up devices to display only specific applications, widgets, and notifications. You can configure Kiosk devices to perfectly fit your work and service.

Provides Secure Browser

Public access web browsers, such as IE and Chrome, do not provide adequate security for businesses. When an unsecured web browser is used for business purposes, features such as copy text and screenshot may lead to a high risk of information leakage. Attacks from viruses due to accessing harmful websites and illegal downloads are also critical security threats. EMM's Secure Browser lowers the risk for information leaks and virus attacks that arise from using an unsecured mobile web browser.

- Blocks corporate information leakage with Secure Browser, the enterprise mobile security web browser.
- Troubleshoots virus infection due to harmful website access and illegal file downloads
- Security policy enforcement prevents text copy and screen capture

Direct Boot enabled

EMM supports Direct Boot on Android 7 and higher (Samsung S10 and higher) devices. EMM is executed after the user reboots the device and before the device is unlocked. The commands that can be executed before unlocking are limited to the following.

- Available commands in the Direct Boot locked status: Unenroll (AE Only), Update Profile, Event (Trigger), Factory Reset & Reset SD Card, Factory Reset, Reset Knox Password, Uninstall Knox (Legacy Only).

> **NOTE** Reset Knox Password:
>
> The "Reset Knox Password device command" sent to the device from EMM does not show the Temporary Password pop-up window on the user device in Direct Boot mode due to Android restrictions. The administrator should check the temporary password in the device details page in the Device menu of the EMM Admin Portal and deliver it to the user.

Supports the first stand-alone Tizen Wearable in the IT industry

EMM provides support in the Tizen Wearable devices of SAMSUNG Electronics. EMM manages the Tizen Wearable devices and makes the installation of business applications more convenient on the EMM Admin Portal. Controlling device functions enhances battery efficiency by up to 30%.

- Remotely distributes and manages applications in stand-alone mode without pairing with a smart phone.
- Protects data when a device is lost due to device lock or factory reset
- Controls device policies: Wi-Fi, Bluetooth, NFC, GPS, Cellular data

Supporting the collection of Dual SIM information

EMM supports the collection of Dual SIM information from the Fully Managed and Work Profile devices of Android Enterprise and Samsung Android Legacy devices (only partial information, such as the phone number, is collectible from non-Samsung devices) that use KPE licenses from v2.5.5 version. You can check the phone number or IMEI information of the device equipped with Dual SIM in the Device, Group, Application, or Content menus.

Guaranteed secure communication channel without any additional investment using the Samsung SDS AppTunnel

The Samsung SDS AppTunnel secures stable communication channels without any additional installation of hardware. It protects both stored and transmitted data. Samsung SDS AppTunnel provides a more secure communication channel by creating channels for each application. EMM replaces VPN with AppTunnel, because VPN spends a lot of time loading and exposes the entire communication history while AppTunnel limits the security problem within the corresponding app only.

- Adopted Samsung SDS App Tunnel to replace the VPN, which has lots of loading in between processes
- Software-based secure communication channel for applications

Strong data protection

EMM has incorporated top-level security requirements since the initial design process in order to protect corporate data from possible data security threats:

- All data between the server and mobile device is encrypted with FIPS 140-2 (FIPS: US Federal Information Processing Standards).
- Two-factor authentication is supported through applications and communication based on security certificates.
- Highly secured communication channel based on TLS 1.2
- Data encryption with US Federal Information Processing Standards FIPS 140-2 authentication modules

EMM meets the Federal government-grade security requirements (MDMPP 1.1) as well as the U.S. Federal Information Processing Standards (FIPS 140-2). Also, EMM is the first solution to be listed in the Commercial Solutions for Classified Program of the U.S. National Security Administration from among its competitors in the EMM industry. EMM has been re-certified with MDMPP 2.0 and has been awarded CC certification as the industry's first iOS platform.

Common Criteria Evaluated Security Functions

Communication between the EMM Agent and EMM Server are secured through TLS channels by default. The communication path from the Admin Portal to the EMM server channels also creates an encrypted communication channel by supporting HTTPS (over TLS). The communication path from the EMM to its certificate authority (MC ADCS), supporting MS SQL and Syslog Server are protected using Windows Server provided IPsec – instructions can be found in Samsung SDS EMM Configuration Guide for IPsec settings in Microsoft Windows Server 2016/2019 for Common Criteria Evaluation.

Please refer to Samsung SDS Co. Ltd. EMM and EMM Agent for Android Security Target for the details of security functions that have been subject to Common Criteria evaluation.
Please refer to the EMM system architecture diagrams below. Note that the ports identified in the following figures are only examples – the actual ports can be configured during installation. Note also that while the diagrams identify the MS ADCS, MS SQL and Syslog Server connections as HTTPS or TLS, in the evaluated configuration they are protected using IPsec as identified above.

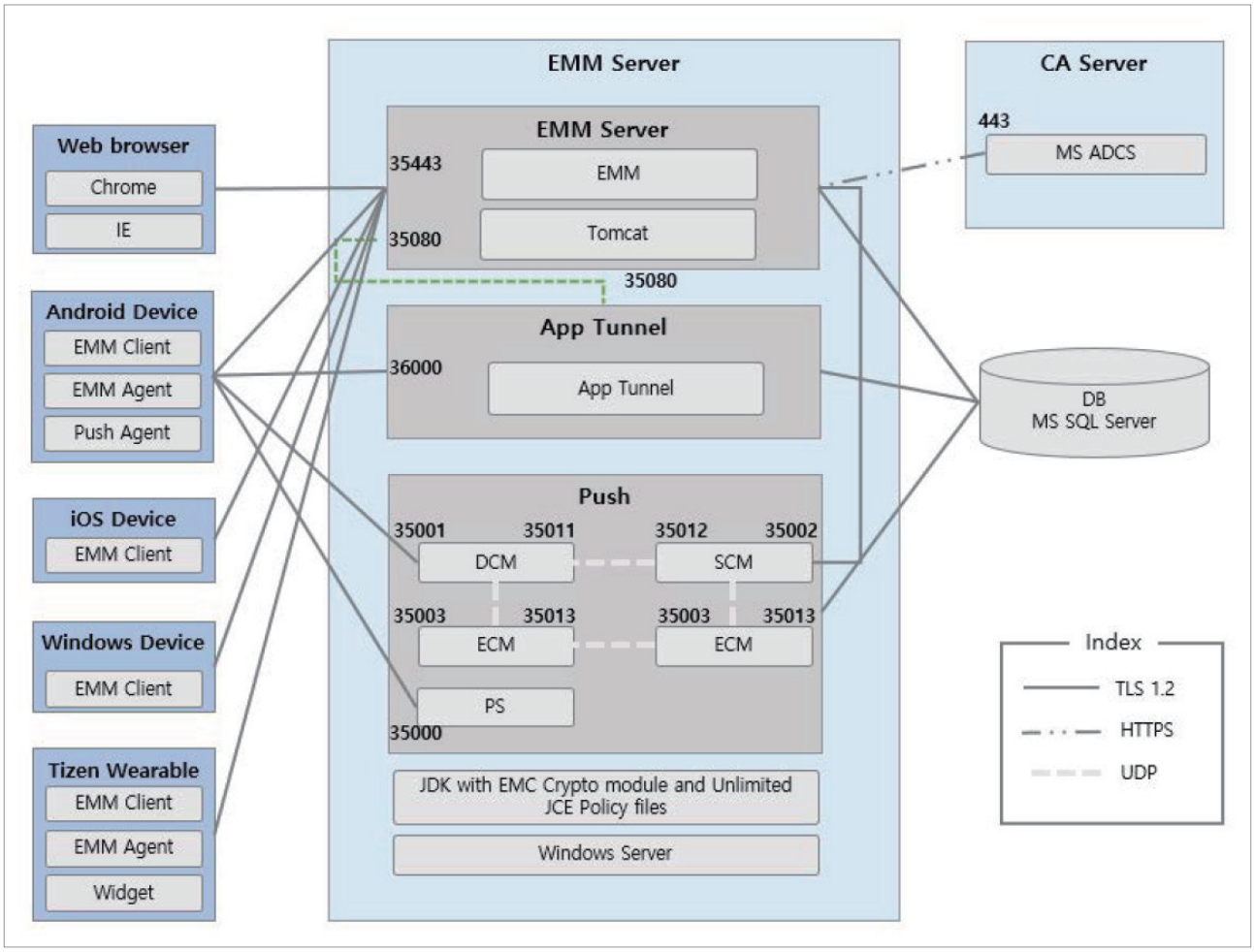


Figure 1-1. Samsung SDS EMM operation architecture - Single server

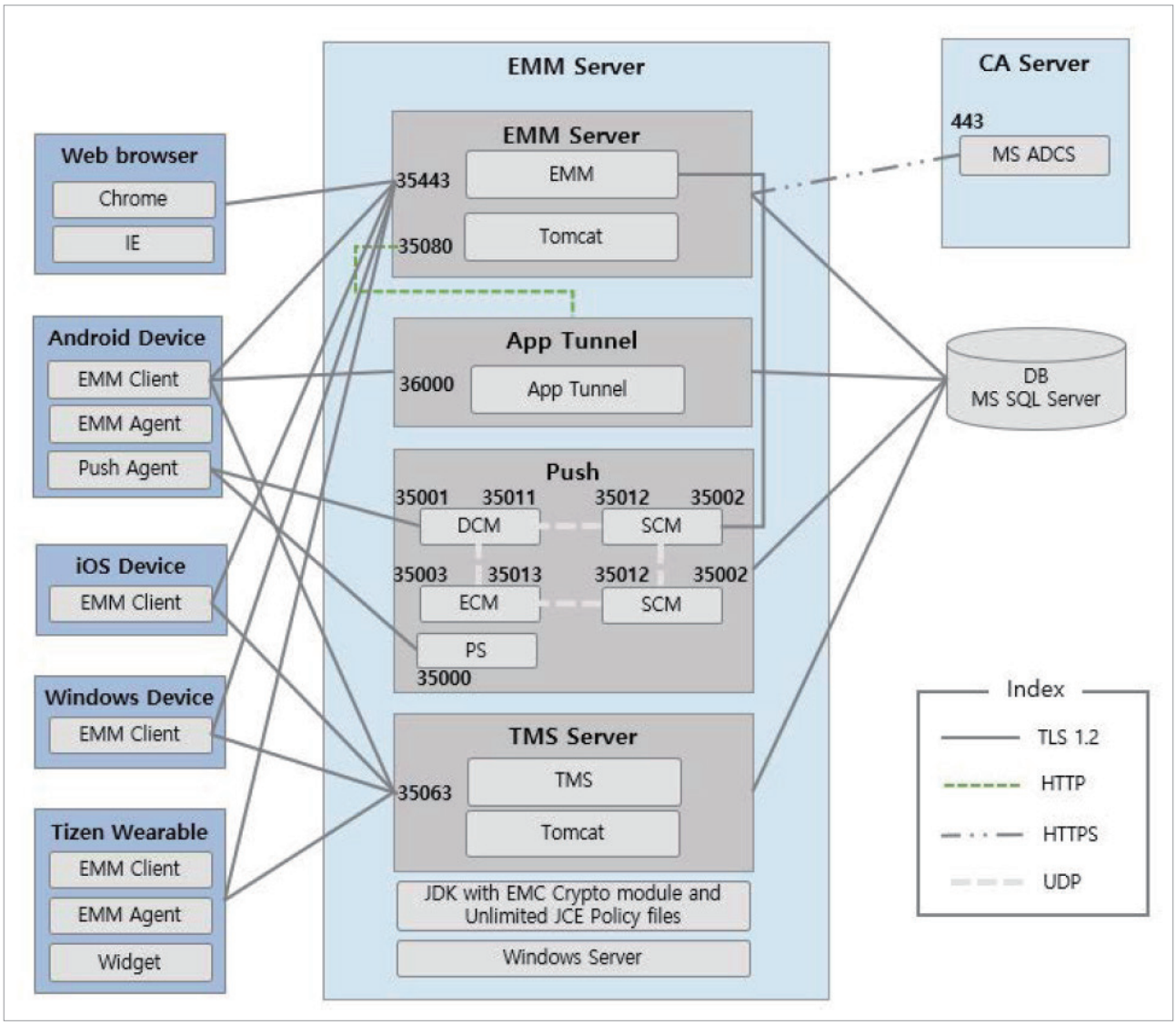


Figure 1-2. Samsung SDS EMM operation architecture - Single server with TMS

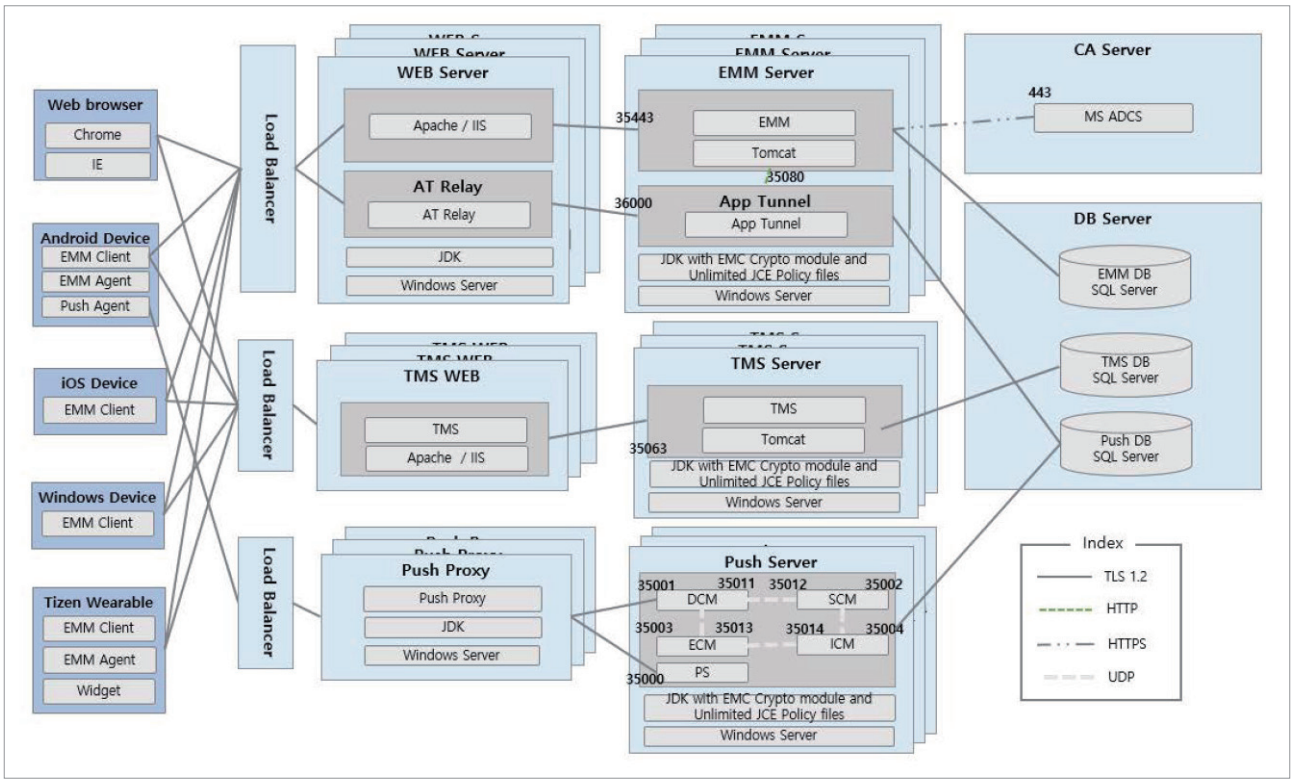


Figure 1-3. Samsung SDS EMM operation architecture - Multiple servers

EMM system requirements

Meet the requirements listed below to ensure the efficient operation of EMM:

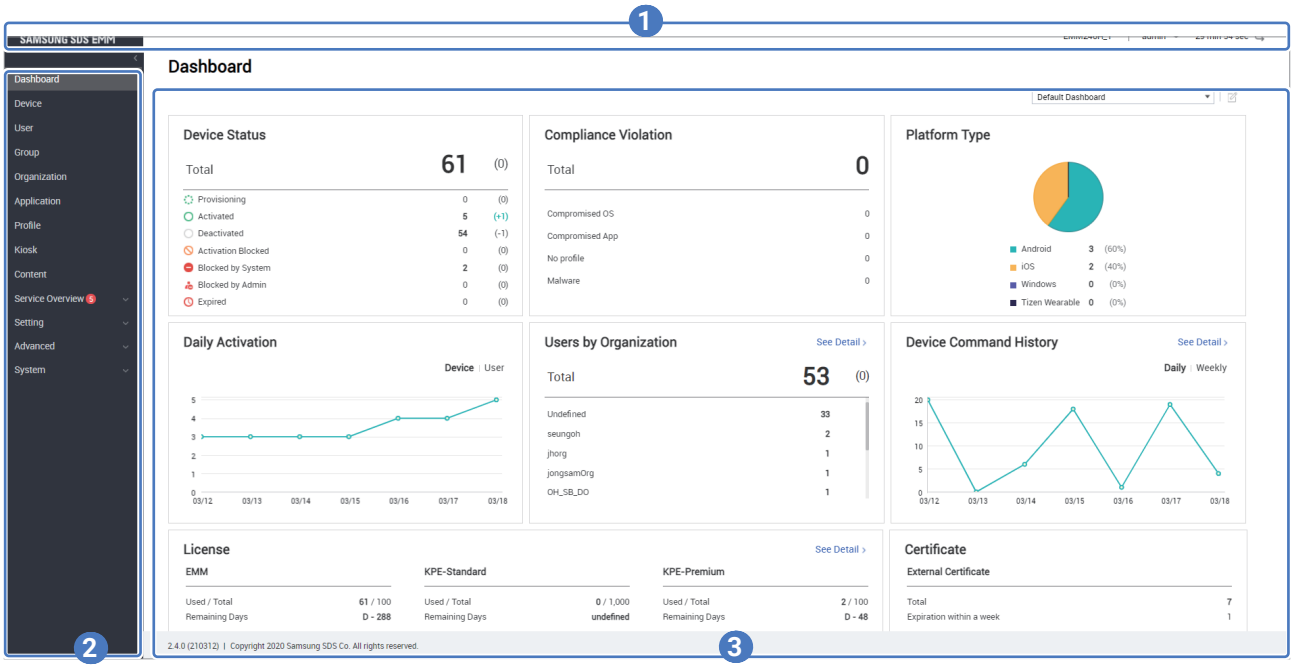
Item		Requirement
EMM server	CPU	x86 quad-core processor or faster
	Memory	16 GB or more
	Disk space	300 GB or more
	OS	Microsoft Windows 2008 Enterprise server (64 bit) or higher. Windows Server 2012, 2016 is the evaluated platform in the CC evaluation4.
	DBMS	Microsoft SQL Server 2008 (64 bit), 2016, 2019. Refer to Microsoft's website for the detailed specifications of the installation of hardware and software.
IT admin’s PC	OS	Microsoft Windows XP or higher
	Browser	• Google Chrome version 41 or higher • Mozilla Firefox version 37 or higher • Microsoft Internet Explorer 11
	Resolution	1920 x 1080 (px)
User’s device	Android Enterprise	Android 6.0 (Marshmallow) or higher (Samsung devices only supported)
	Android Legacy	Android 6.0 (Marshmallow) or higher (Samsung devices only supported)
	iOS	iOS 11.0 or higher
	Windows	A desktop computer on which Microsoft Windows 10 Version 1703 or higher has been installed (Pro/Enterprise/ Home)
	Tizen wearable	Tizen 2.3.2 or higher
Supported language	Admin Portal	English, Chinese, Portuguese, Spanish, French, German, Italian, Korean
	EMM Agent	Any of the above languages set in the device language settings • If the selected language in EMM Agent is not supported on the mobile device, EMM Agent will be displayed in English.

NOTE In accordance with the GDPR (General Data Protection Regulation) and the privacy policy, your organization must follow following standards:

- Your organization must get the users consent for collection of personal data from all employees using EMM solution in advance.
  - For EMM device users, the End User License Agreement (EULA) upon EMM agent installation can be used for privacy policy consent.
- In case of users or IT admin drop out, the withdrawal should be requested to your organization.
- For Korean users: In case of app customization, all accessibilities used by the app should be notified to users.

EMM Admin Portal

Get familiar with the Admin Portal's interface features before starting the Admin Portal.



No.	Name	Description
1	Header	Appears on every page. The logo, tenant ID, account ID, and the session time reset are provided. Click  next to the account ID to view more menus. For more information, see Header.
2	Main menu	Appears on every page. The EMM features are listed by type. For more information, see Main menu.
3	Content page	Displays a list of information for the selected Main menu or the details about the selected resource. For more information, see List. The privacy policy, EMM version, and copyright information appear at the bottom of the content pages. Click **Privacy Policy** to navigate to the detail page. When you enter a value on this page, you must fill out any input field with an asterisk (*).

Header

Find out more about the elements in the header.

No.	Name	Description
1	Logo	Click the logo to go to the main page. You can change the logo and color theme. For more information, see Setting the logo.
2	Tenant ID, Account ID	The tenant ID appears when the EMM is operated as a multi-tenant. Click next to the account ID to view more menus. • **Change Password**: Change your account password. • **Set Session Timeout**: Change the session time limit. • **Enable high contrast theme**: Apply a high contrast theme to the Admin Portal to help people with poor vision. • **Change Language**: Change the display language. • **Logout**: Sign out of the Admin Portal.
3	Session time	View the remaining session time. Click to refresh it.

Main menu

The Admin Portal's Main menus help you perform any required tasks that you need to perform as a IT admin. Find out what you can do in each menu.

Menu	Description
Device	Manage the mobile devices activated in EMM. Check the details of each device and send commands to the devices.
User	Manage the users enrolled in EMM. Check the details for each user including the group or organization they belong to and their devices.
Group	Manage the user or device groups enrolled in EMM. Assign and apply profiles or send commands to desired groups.
Organization	Manage the user organizations enrolled in EMM. Create or delete sub-organizations. Assign and apply profiles to desired organizations.
Application	Manage internal or public applications in EMM. Assign applications to groups or organizations.

Menu	Description
Profile	Create new profiles and set policies in them for device management. Assign and apply profiles to mobile devices in groups or organizations. Edit or delete the existing profiles.
Kiosk	Upload a single Kiosk application or use the Kiosk Wizard to create a Multi App Kiosk. Set new Kiosk applications to profiles for assignment. Control the enrolled Kiosk applications.
Content	Deploy files such as images, files, texts, and videos that are added to the Admin Portal to mobile devices through the content push service.
Service Overview	Monitor and manage the Admin Portal. Track events in the Admin Portal through the audit, log, and history. Set alerts to notify device users of important events. Send general notices to users.
Setting	Configure the EMM server, EMM applications, and EMM Agent policies. Change the settings for the Android and iOS device environments, the Admin Portal environment, and the Keepalive feature. Schedule for profile updates. Manage licenses for using EMM.
Advanced	Configure the settings for the E-FOTA service and the anti-malware scanning service. Monitor the network usage of enrolled devices. Manage any external systems that will be synchronized or integrated, issue certificates from the external certificate authority, and Open API.
System	Integrate EMM with the back-end systems of your company, such as company database, etc., and configure their connectors. Set CSP and PPKG files for Windows 10.

List

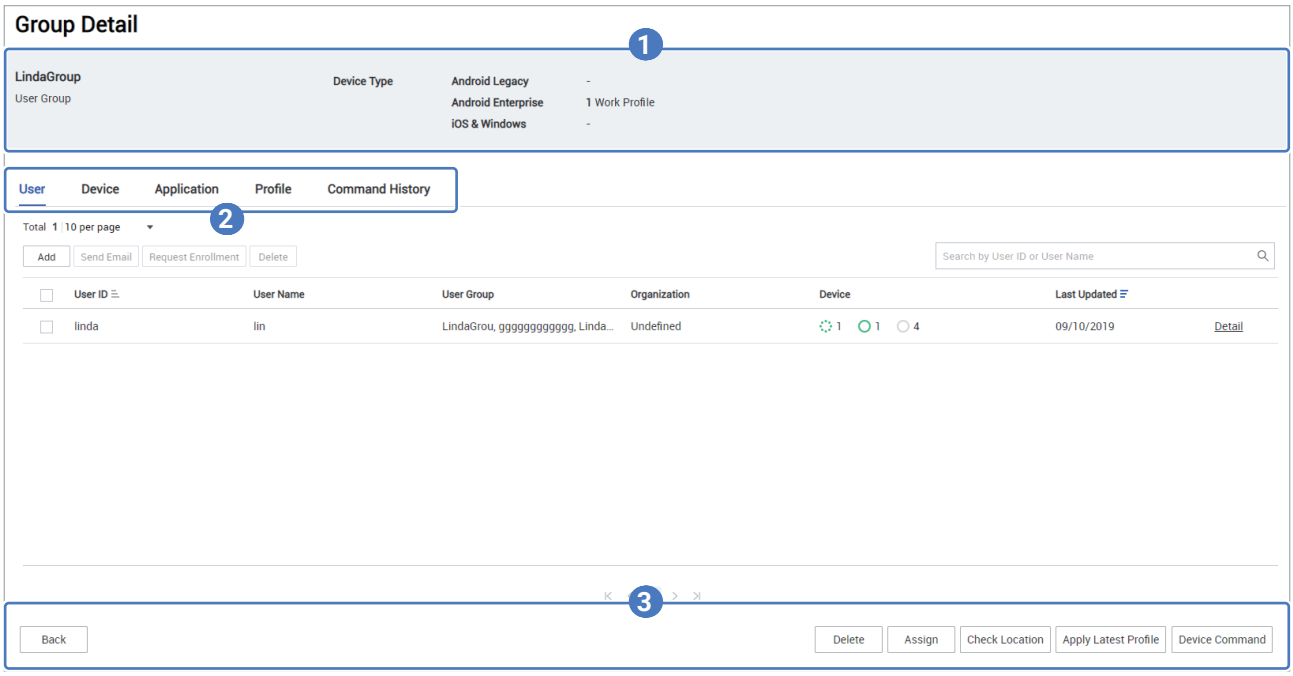
When you click one of the Main menus, the initial information is displayed as a list on the content page.

The following are the attributes of lists:

- Rearrange the list by clicking (ascending order) or (descending order) next to the column headers.
- Filter the list by clicking next to the column headers when there are more than two types of value.
- Adjust the length of the columns by putting the mouse pointer between the columns and dragging it when the mouse pointer changes to .
- Rearrange the column order by placing the mouse pointer over the column header you want to move and dragging it when mouse pointer changes to . While dragging the column header, will appear next to the column header. If it changes to , you can drop it in a place where appears.

Detail page

When you click one of the items on the list, detailed information about the selected item is displayed on the detail page. The detail page is organized as follows.



No.	Name	Description
1	Summary	Displays the basic information.
2	Tabs	Displays the detailed data and information of the selected item in categories. Function buttons are provided for using various functions in the selected tab.
3	Function buttons in the footer	The buttons for the available functions related to the selected item

Function icon

When you click the following icons, various actions are performed in the Admin Portal.

Icon	Description
Save	Click to save changes.
Sync	Synchronize an item. Select the sync target type and confirm the synchronization.
Restore	Select an item to restore and click . Confirm the restoration.
/// Tooltip	Click /// to open a brief guide, detail, or alert about an item.
Download	Click to download an item.
Upload	Click and select a file to upload.
Search	Input a keyword and click to search for an item.
Text Clear	Click to clear the words entered in the search field.
Preview	Click to preview the result.
Expand	Click to view a hidden area.
Collapse	Click to hide an expanded area.
Order Up	Click to move an item up on the list.
Order Down	Click to move an item down on the list.
Reference Items	Click to add reference items that will be replaced with actual values.

Alert pop-up

The alert pop-up appears after signing in. The pop-up informs you of the followings while also providing the possibility to take action:

Item	Description
License expiration	Click the displayed number of the devices to renew them. For more information, see Managing licenses.
APNs certificate expiration	Click the displayed number of the certificate to renew them. For more information, see Setting a APNs certificate (iOS only).
Apple DEP token expiration	Click the link provided for new token issuance. For more information, see Issuing a DEP token.
Apple VPP token expiration	Click the link provided for new token issuance. For more information, see Downloading the VPP token from the VPP website.
Policy assignment error	Click any item to view the detailed information and take appropriate action. For more information about alerts, see Managing alerts.

Available services by device type and OS

Supported services in EMM differ by device type and OS. Look at the following table and discover the available services depending on the user's device.

Service	Android Enterprise	Android Legacy	iOS	Windows
Knox Workspace		v		
E-FOTA	v	v		
Kiosk	v	v		
Volume Purchase Program (VPP)			v	
Knox Mobile Enrollment (KME)	v	v		
Device Enrollment Program (DEP)			v	
Anti-Malware	v			
Dual DAR	v (Fully Managed or Work Profile on company-owned)	v		

2

Starting up

Starting up

To begin using EMM, you will need to create an account and purchase the necessary licenses. Once you are registered and signed into the Admin Portal, you can configure initial settings for using mobile devices with EMM.

This chapter explains the following topics:

Signing in to EMM

EMM services can be utilized through the Admin Portal. Sign in to the Admin Portal to start EMM. To sign in to the Admin Portal, complete the following steps:

1. Navigate to the EMM Admin Portal login page.
2. Select a language and enter your corporate domain, admin ID, password and then click **Sign in**.
    - Accounts are locked for ten minutes after five or more login failures.
3. If two-factor authentication is enabled for security, enter the single-use password you received via text message or emai in the “OTP Authentication” window and click **OK**.
    - To use OTP authentication, you must set the **Two-Factor Authentication** to **TRUE** in **Setting > Server > Configuration** on the Admin Portal and you have to register your mobile phone number or email address during registration.

NOTE

- The login method may differ depending on the EMM operating mode.
  - In Single-Tenant mode, a corporate domain (tenant ID) is not required.
  - In Multi-Tenant mode, the corporate domain (tenant ID) is managed by the TMS administrator. Contact the TMS administrator for the corporate domain that you need to enter. For more information about Multi-Tenant Mode, see Samsung SDS TMS Administrator's Guide.
- If you click the checkbox next to **Save ID**, a pop-up window asking for consent to the collection of cookie information by the site will appear when saving login information.
- If there is content that the IT admin needs to be notified of, a notification message pop-up window will appear. For information on how to create a notification message that requires IT admin notification, see Setting the logo.
- When the password expires, the password change window will appear when logging in. For information on how to enter a new password in the password change window and set the password validity period, see Configuring the environment.
- To find your login ID and password, click **Find ID / Password** and enter the email or company ID and user ID you entered when signing up.
- To log in to EMM with SSO, click **SSO Login** and enter your tenant ID. You can sign in to EMM using the SSO service. To use SSO, you must configure the SSO settings and integrate EMM with ADFS. For more information, see Configuring SSO.
- To log in to EMM with CAC smart card security authentication, insert a CAC smart card into the reader, click **CAC Sign-In**, and enter your tenant ID in the "Tenant ID Setting" pop-up window. When the certificate selection pop-up appears, select a certificate and enter a certification PIN number. If the EMM server operates in Single-Tenant mode, the tenant ID input pop-up does not appear. For more information about CAC smart card authentication, see Setting the CAC Sign-In and CAC Sign-In of the Appendix.
- A pop-up window asking for consent to the terms and policies will appear when there are terms and policies to be accepted. For information on how to create the terms and policies, see Setting Terms and Policies.

Managing licenses

EMM manages licenses collectively. When a license expires, the use of EMM is restricted and a monitoring notification with the license expiration date will appear in the EMM Admin Portal. The composition of menus and policies on the EMM Admin Portal may differ depending on the license. For more information about licenses, please contact the Samsung SDS EMM Support Team.

License types

Licenses managed by EMM are classified as follows, and the menus and policies on the EMM Admin Portal may differ depending on the license.

When purchasing, EMM, ELM, Backwards Compatible, and KPE-Standard licenses are provided by default, and KPE-Standard can be upgraded to KPE-Premium licenses. However, a KPE-Premium license cannot be downgraded to a KPE-Standard license.

Type	Description
EMM	This license key is necessary for using EMM. • The EMM license is managed in TMS when EMM is operated as a multi-tenant, so you can only check the EMM license in the EMM Admin Portal.
ELM	The Enterprise License Manager (ELM) license is a license key that is necessary for using Samsung Knox SDK.
Backwards Compatible	This is a license key to support customers using existing licenses. • The ELM key provided by Samsung will end service on December 31, 2020, so this license key is needed to support Samsung Knox SDK on mobile devices with Knox 2.7.1 or lower.
E-FOTA	This is a license key for using E-FOTA. For information about E-FOTA license registration, see Managing Enterprise-Firmware Over The Air (E-FOTA). • Registering the E-FOTA license activates the **Advanced> E-FOTA** menu.
KPE-Standard	The KPE (Knox Platform for Enterprise) license is a license that provides standard and premium services for Samsung Knox SDK on the Android platform, and is supported only on Samsung devices with Android 8.x (Oreo) or higher. For more information about Knox licenses, see the Samsung Knox website (https://docs.samsungknox.com/dev/common/knox-licenses.htm). • KPE-Standard is a license that provides permission to call APIs that manage functions, such as network connection, user account, location, data encryption, and security restrictions.

Type	Description
KPE-Premium	KPE-Premium is a multi-registration license key, and only the devices that has the license activated can lock the devices. When KPE-Premium expires, Knox Workspace will be unavailable. • KPE-Premium is a license that provides permissions to call APIs that manage advanced security features, such as Knox Workspace, VPN, and certificates, in addition to the permissions provided by KPE-Standard.
KPE-Dual DAR	This is a paid license key for using Dual DAR. When Dual DAR expires, Knox Workspace will be unavailable. For information about Dual DAR license registration, see Setting the Dual DAR.
Tizen Wearable ELM	This is a license key for using Samsung Knox SDK on Tizen Wearable devices.
Tizen Wearable KPE-Standard	This is a license key for the KPE-Standard services on Tizen Wearable devices.
Tizen Wearable KPE-Premium	This is a license key for the KPE-Premium services on Tizen Wearable devices.

NOTE

- The KPE Premium license is necessary for updating the EMM Agent on Work Profile type Samsung devices to the 2.4.1 version. Therefore, the license upgrade must be preceded by using the device command to update the EMM Agent to the latest version on Work Profile, Fully Managed with Work Profile, and Work Profile with Company-owned type devices activated with the KPE Standard license. For non-Samsung devices, the EMM Agent update is not supported, so you must install the latest EMM Agent manually. In this case, the application's installation policy for untrusted sources must be set to allow.
- When upgrading EMM from v2.3.5 version or lower, the following tasks must be performed for KPE and Backward Compatible licenses to register new devices normally. When the following tasks are completed, send the **Update License** device command to activate expired devices.
  - 1) **Update the KPE-Premium license**: The type and license key are automatically updated, and Total Quantity, Start Date, and Expiration Date need to be newly entered based on the update information.
  - 2) **Deleting the Backwards Compatible license and registering a new one**
  - 3) **Deleting the KPE-Standard license and registering a new one**: If the information does not exist on the EMM server after deleting the KPE-Standard license, you must request and add a KPE-Standard license key. Contact the Samsung SDS EMM Support Team for more information.
- Restrictions on the number of licenses used: From v2.3.5, the number of licenses used is measured at the time of device activation, so the number of licenses activated in the previous versions is not displayed. That is, when modifying a license, enter the **Total quantity**, considering the number of licenses from the previous versions.
- EMM supports the collection of Dual SIM information from the Fully Managed and Work Profile devices of Android Enterprise and Samsung Android Legacy devices (only partial information, such as the phone number, is collectible from non-Samsung devices) that use KPE licenses from v2.5.5 version. You can check the phone number or IMEI information of the device equipped with Dual SIM in the Device, Group, Application, or Content menus.

Registering a license

To operate Samsung SDS EME properly, you must register a valid license to the EMM Admin Portal. If you use the demonstration license, the use of some features for the EMM Admin Portal are limited. You can register a license for either EMM operation mode as follows:

- Multi-Tenant: Register a license in the License menu on the TMS Admin Portal. For more information about the TMS server, see Samsung SDS TMS Administrator's Guide.
- Single-Tenant: Register a license in the EMM Admin Portal.

Licenses managed by EMM can only be deleted, and additional information such as license quantity and expiration date can be modified. For licenses, an automatic batch job that checks the licenses every day at 01:00 will be operated on the server, and after checking valid licenses for expired devices, update device command will be sent to the devices.
In addition, if you replace the KPE-Premium key or upgrade to a KPE-Premium license from KPE-Standard, you can upgrade the license with device command, or update for renewal due to the expiration of the Dual DAR or KPE-Premium license. For more information, see Sending device commands to devices.

To register the license in EMM, complete the following steps:

1. Navigate to **Setting** > **License**.
2. Click **Add** to register a license.
3. On the "Add License" page, enter the following items. Items displayed may differ depending on the license type.
   - **Type**: Select the type of license you want to register. KPE-Standard, Backwards Compatible Licenses are provided by default and do not appear under Type.
     - KPE-Premium: This is a multi-register license. Enter the license to use the KPE Premium service.
     - KPE-Dual DAR: For more information about Dual DAR license registration, see Setting the Dual DAR.
     - E-FOTA: For more information about E-FOTA license registration, see Managing Enterprise-Firmware Over The Air (E-FOTA).
     - Tizen Wearable KPE-Premium: To use the KPE Premium service on Tizen Wearable devices, enter the license.
   - **Product Key**: Enter the product key of the selected type.
   - **License Key**: Enter the license key of the selected type.
   - **License File**: Click ⬆ and register a license file.
   - Enter the **Total Quantity**, **Start Date**, and **Expiration Date** of the license.

4. Click **Save**.

NOTE

- The EMM license is registered in TMS when operating as a multi-tenant and does not appear under Type.
- When the KPE-Premium (formerly KLM) license expires, Android Enterprise devices are locked by the KLM Agent, so you must renew the license before the license expires. If a device is locked due to license expiration, device command for the license update is not applied when the device is rebooted.

Managing KPE-Premium licenses

When you register the KPE-Premium license in the license menu, you can select the license usage method for Android Legacy or Android Enterprise devices.

To select the license usage method, complete the following steps:

1. Navigate to **Setting** > **License**.
2. In the top-right corner of the “License” page, click **Manage License Usage**.
3. In Android Enterprise or Android Legacy, select whether to use the KPE-Premium license key and when to activate the license, and click **Save**.
   - **Android Enterprise**: Select whether to use the KPE-Premium license key or not during device initial activation.
   - **Android Legacy**: Select whether to use the KPE-Premium license key during device initial activation or when applying the Knox Workspace profile.

Checking license information

To check the license information, complete the following steps:

1. Navigate to **Setting** > **License** and click the license you want to check the details for.
2. The license details are displayed at the top of the “License Detail” page, and the device information using the license is displayed at the bottom. The license details may differ depending on the license type.

Item	Description
Company Name	Displays the tenant ID.
License Version	Displays the version of the license.
Security Level	Displays the security level (Enterprise or High security version).
Access Period	Displays the validity period of the license.
Single Product	• PUSH: Samsung SDS Push • APPTUNNEL: Samsung SDS AppTunnel
Connector	Displays the types of the connectors that can be connected with EMM.
Maximum number of devices	The maximum number of devices that can use the EMM service is displayed (number of activated devices). • The number of devices is counted as the sum of all the device platforms that can be activated, and devices cannot be registered beyond the maximum number of devices.
Maximum number of API Client	Displays the maximum number of the API Clients for developing EMM.
SecuCamera Count	Displays as unlimited or displays the number of SecuCameras registered under the license.
Knox Portal for Mobile	Displays whether to use the EMM Admin Portal on the device.
Samsung Group	Displays whether to use a Samsung Group license.

NOTE There must be a license to use SecuCamera. The SecuCamera licenses are managed in **Management > Tenant** on the TMS Admin Portal. If the SecuCamera license is set to unlimited in **Setting > Server > Configuration** on the EMM Admin Portal, there are no restrictions for using SecuCamera, and you can activate SecuCamera during user registration. For more information, see Creating user accounts and the Samsung SDS TMS Admin Guide.

Setting the Dual DAR

Set Dual DAR to use dual encrypted Dual DAR Workspace on Android Legacy or Android Enterprise (Fully Managed or Work Profile on company-owned) devices.

When the Dual DAR license is registered, the Dual DAR Workspace is enabled. You can set the Dual DAR when creating a profile for Android Legacy devices or when adding users or organizations for Android Enterprise (Fully Managed or Work Profile on company-owned) devices, and deploy Dual DAR with QR code or KME. For more information about Dual DAR, see https://docs.samsungknox.com/whitepapers/knox-platform/DualDAR.htm.

The necessary preparations for using Dual DAR and the method for creating a Dual DAR Workspace are as follows.

- Necessary preparations
  - Dual DAR license (paid)
  - Supported platform: An Android Legacy or Android Enterprise Fully Managed or Work Profile on company-owned devices (Samsung S10, Note10 or higher) that supports FBE (Android File Based Encryption), Samsung Knox Version 3.3 or higher
  - Supported devices: Android 12 or higher for Fully Managed Dual DAR, Android 11 or higher for Work Profile on company-owned Dual DAR

- Creating a Dual DAR Workspace
  - Using the Admin Portal: For the Android Legacy type, set and apply the Dual DAR policies when creating a profile. For more information, see Creating a new profile.
    For Android Enterprise (Fully Managed or Work Profile on company-owned) devices, set Dual DAR when adding users or organizations and deploy the profile with the Dual DAR policies applied. For more information, see Registering a single user account and Adding an organization.
  - Using the Knox Mobile Enrollment (KME) service: Set Dual DAR on Knox Mobile Enrollment (KME) and activate devices. For more information, see Configuring Android Enterprise Policies.

Registering the Dual DAR

To set the Dual DAR, complete the following steps:

1. Navigate to **Setting** > **License**.
2. Click **Add** to register the Dual DAR license.
3. On the “License” page, enter the following items.
   - **Type**: Select KPE-Dual DAR in Type.
   - **License Key**: Enter the Dual DAR license key.
   - Enter the **Total Quantity**, **Start Date**, and **Expiration Date** of the Dual DAR license.
   - **Dual DAR Client Type**: Select the Dual DAR registration type.
     If you selected Third Party app or Preload app, enter the corresponding app, package, and any additional information.
     - **Android Default**: Uses the default Android encryption method to use Dual DAR.
     - **Third Party Application**: Register third party application and enter the application name to use Dual DAR. Third party applications should be installed on the device before creating a Dual DAR Workspace.
       Register a third party application and enter the application name. When the registration is complete, the application version, package name, app signature, and Android Enterprise (Work Profile on company-owned) signature is automatically entered.
     - **Preload Application**: Register preloaded applications to use Dual DAR. Enter the package name. For app signature, use a Keytool and enter the value in the SHA-256 format.
4. Click **Save**.

NOTE If there is at least one device with Dual DAR Workspace activated using Dual DAR, it is impossible to change Dual DAR setting and also to change the package name and signature of the Dual DAR Client Type.

Configuring basic environments

Configure how device users are verified when they sign in to EMM. You can also configure the required environments to use the EMM server and certain types of devices.

Setting the user authentication method

Set up the authentication method for when device users sign in to EMM on their mobile devices.

Type	Description
Automatic	This is the default authentication method provided by EMM that authenticates the user with the user ID and password registered in the Admin Portal. Synchronized users will be verified via their user IDs and passwords that were imported by AD/LDAP synchronization.
Manual	Customizes the authentication method by user type.

To set the authentication method to **Automatic**, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. On the “Configuration” page, click **Authentication Setting** to open the “Authentication Setting” window.
3. In the “User Authentication Settings” section, click **Automatic**.
4. Click **Save**.

To set the authentication method to **Manual**, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. On the “Configuration” page, click **Authentication Setting** to open the “Authentication Setting” window.
3. In the “User Authentication Settings” section, click **Manual**.
4. In the “Sync User Authentication Settings” section, select the authentication method for synchronized users.

Item	Description
Authenticator	• **globalEmmAuthenticator**: Verifies the device users via the user ID and password saved in the EMM server. • **globalLdapAuthenticator**: Verifies the device users via the user ID and password imported by AD/LDAP synchronization. • **globalLdapServiceAuthenticator**: Verifies the device users via the user ID saved in the EMM server and the password imported from the AD/LDAP server accessed by a directory service.
LDAP Service ID	If you selected **globalLdapServiceAuthenticator**, enter the directory service ID to use for accessing the AD/LDAP server.

5. In the “Local User Authentication Settings” section, select the authentication method for locally registered users.

Item	Description
Set identical to the Sync User Authentication Settings	Uses the same authentication method as set in the “Sync User Authentication Settings” section.
Authenticator	• **globalEmmAuthenticator**: Verifies the device users via the user ID and password saved in the EMM server. • **globalLdapAuthenticator**: Verifies the device users via the user ID and password imported by AD/LDAP synchronization. • **globalLdapServiceAuthenticator**: Verifies the device users via the user ID saved in the EMM server and the password imported from the AD/LDAP server accessed by a directory service.
LDAP Service ID	If you selected **globalLdapServiceAuthenticator**, enter the directory service ID to use for accessing the AD/LDAP server.

6. In the “Smart Key Authentication Settings” section, authenticate users for vehicle control.

Item	Description
Authenticator	Select **sampleSmartKeyAuthenticator**.

7. Click **Save**.

Configuring Android Enterprise environments

This setting is for Android Enterprise. Select Managed Google Play as the application distribution method in the Android Enterprise menu. You register Samsung SDS EMM as the EMM provider in the Google Play Console and configure the Managed Google Play environment.

If EMM is operated on a closed network that restricts Internet access, select to use the EMM App Store provided by Samsung SDS EMM for application distribution. If you do not register your Managed Google Play account after selecting the EMM App Store, external applications provided by Managed Google Play may be restricted for use.

NOTE The application distribution method for Android Enterprise can be changed to Managed Google Play or EMM App Store. However, note that the existing settings are reset when changing the application distribution method. If there are activated Android Enterprise devices, you cannot change the application distribution method.

To configure the Android Enterprise environments, complete the following steps:

1. Navigate to **Setting** > **Android** > **Android Enterprise**.
2. On the “Android Enterprise” page, set the application distribution method of Android Enterprise as **Managed Google Play**.
   - For closed networks with limited Internet access, choose the **EMM App Store**.
3. Click **Register EMM**.
   - The Google Play Console will appear.
4. Sign in to the Google Play Console using your Google account.
5. Create a Managed Google Play account and register Samsung SDS EMM as the EMM provider.
   - When registration is finished, the Managed Google Play account information and Google API settings will appear on the Admin Portal’s “Android Enterprise” page.
6. Click **Save**.

NOTE Starting from EMM v2.5.3, the application update method is supported in **Auto Update Mode** when assigning applications. The Auto Update Apps setting provided in the existing Android Enterprise menu is no longer supported.

Resetting the Managed Google Play Store Layout

Starting from EMM v2.5.3, Managed Google Play (Store, Private, Web) applications can be classified and managed with Collection, the Organize Apps function of Managed Google Play. The applications configured with Collection can be viewed in the Play Store on the device, and, by setting the Basic Store Layout, applications can be listed and viewed in the existing method without Collection.

To reset the Collection classified by the Organize Apps function of Managed Google Play to the Basic Store Layout, complete the following steps:

1. Navigate to **Setting > Android > Android Enterprise**.
2. On the "Android Enterprise" page, click **Reset** in Managed Google Play Store Setting, Reset to Basic Store Layout.
3. In the "Reset to Basic Store Layout" pop-up window, click **OK**.
    - When resetting to the Basic Store Layout, any Collection of Managed Google Play (Store, Private, Web) applications created on the device is deleted, and the Collection can be reconfigured with the Organize Apps function. For more information, see Managing applications with Collection.

Deleting EMM provider information

To delete the registered EMM provider information from EMM, complete the following steps:

1. Navigate to **Setting** > **Android** > **Android Enterprise**.
2. On the "Android Enterprise" page, click **Unregister EMM**.
    - The information registered on the Google Play Console will be deleted, and the user will no longer be able to use the device as an Android Enterprise device.
    - Deleted information can be restored by re-registering it within 30 days.

Permanently deleting EMM provider information

To delete the registered EMM provider information permanently, complete the following steps:

1. Sign in to the Google Play Console (https://developer.android.com/distribute/console).
2. Click **Delete Enterprise**.
    - All the information registered regarding EMM providers will be deleted within 24 hours and cannot be restored.

Setting public push servers

You can set up Public Push (FCM, APNs, WNS, Tizen Wearable) provided by Google, Apple, Windows, and Tizen Wearable respectively. The Public Push information that is provided is as follows:

- FCM: This is the Google Cloud Push server to send notification messages between the Android device application and the application server. It provides a push notification service for sending notification messages to Android devices.
- APNs: This is the Apple's Push server for sending notification messages to iOS devices. It provides the Apple Push Notification Service when a certificate or token is registered in the EMM Admin Portal.
- WNS: This is the Windows Push server to send notification messages to devices for use on PC, tablet, and mobile devices where Windows 10 is installed.
- Tizen Wearable: This is Tizen's Push server to send notification messages to Tizen Wearable devices. It provides the push notification service for sending notification messages to Tizen Wearable devices.

To set up Public Push, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Public Push** on the top of the window.
3. The following is a description of the Public Push settings for **FCM**, **APNs**, **WNS**, and **Tizen Wearable**. Click the tab to see the content.
   - **FCM**: The sender ID and APK KEY are the information stored on the application server. The Client and Agent use the same Sender ID. When FCM information has changed, the activated devices should be rebooted to use the FCM service.
     - **Sender ID**: This is a digit string issued for FCM use as a transfer ID for Push.
     - **API KEY**: This is an authentication key value required to use Google services.

     NOTE Google has deprecated GCM as of April, 2018, and replaced the service with FCM. The existing GCM settings remain unchanged. The Sender ID doesn't change, even if an API key is issued for the new FCM service.

   - **APNs**: For information about how to register a certificate or token for use with APNs service, see Setting a APNs certificate (iOS only). If a APNs certificate has already been registered, the currently registered certificate information and the expiration date appear at the top of the window.

- **WNS**: You need an authentication ID and password for sending push notification messages. For more information, visit https://developer.microsoft.com, and navigate to **Windows Developer Center** > **Dashboard** to check the Client ID, Client Secret, and PFN value in the app related menu.
  - **Client ID**: An ID for authentication when sending notification messages.
  - **Client Secret**: A password for authentication when sending notification messages.
  - **PFN (Package Family Name)**: Enter the Package Family name.
- **Tizen Wearable**: To use Tizen Push, Tizen Agent must be registered at **Setting** > **EMM Application and Policy** > **EMM Application**, and the package name should be "com.sds.emm.wearable." Also, the Application ID and Application Key are required to send a notification message to a wearable device via the Tizen Push service.
  - **App ID**: Application ID for using Tizen Push service.
  - **APP Secret**: Application Key value for using Tizen Push service.
    The key value of the App Secret can be downloaded at the following **URL**. Enter the **Package ID**, **Application name** and email address, and click **Submit**. The App Secret key value will be sent via email.
    - **URL**: https://developer.tizen.org/webform/request-permission-tizen-push-service
    - **Package ID**: com.sds.emm.wearable
    - **Application name**: EMM Client

4. Click **Save**.

Setting a APNs certificate (iOS only)

Set up Apple Push Notification Service (APNs) for iOS device use or control. To use the APNs service, register an Apple-signed certificate or token on the EMM Admin Portal. A APNs certificate is valid for one year. To view the details of the registered APNs certificate, navigate to **Advanced** > **Certificates** > **External Certificates**. If the certificate is expired, you cannot send device commands to iOS devices. For more information about APNs, see https://developer.apple.com/library/content/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html.

NOTE From November 2020, the APNs authentication method will be changed to HTTP/2 protocol token-based authentication. For new authentication, get a token instead of a certificate. If a certificate has already been issued, authentication is possible with an existing certificate. You need to upgrade to Tomcat 8.5 or higher that supports HTTP/2.

Using EMM on iOS devices

To use EMM on iOS devices, certificates and the registration procedure are necessary. The previous procedure was complicated because the iOS related certificates had to be issued and registered through the client certificates, but starting from SDS EMM v2.4.1, the procedure became simplified by providing the SDS build certificates. For a detailed procedure for the earlier versions, see “Using EMM on iOS” in the Samsung SDS EMM Installation’s Guide.

NOTE Restrictions on iOS Generic Clients

To modify applications or share data with the client’s other work app, you must build and deploy iOS applications using the client’s build certificate as was done before. No update is available if the build certificate is different.

The SDS ADEP certificate is valid for two years, and expired iOS applications cannot be deployed and installed. Update iOS applications to the latest version before expiration. The expiration date of the SDS ADEP certificate is February 8, 2023.

- Registration procedure
  - Building iOS Clients
  - Creating and registering the APNs Client certificate
  - Creating and registering the APNs Agent certificate
  - Creating and registering the profile signature certificate

- Certificate
  - App Push certificate: A certificate to use App APNs, which sends push messages from the EMM server to the EMM applications. The certificate can be created by the client certificate.
  - MDM APNs certificate: A certificate to use MDM APNs, which sends push messages from the EMM server to the iOS EMM module. The certificate can be created by the agent certificate.

Registering a APNs certificate

To register a APNs certificate, complete the following steps. The procedure for certificate registration may be different depending on the EMM version. In EMM v2.4.1, the APNs Client token and the profile signature certificate are automatically registered, so only perform creation and registration of the MDM APNs certificate (APNs Agent certificate), which is step 4, 6, and 7.

1. Navigate to **Setting** > **Server** > **Configuration**.
2. On the “Configuration” page, click **Public Push**.
3. In the “Public Push” window, click **APNs**.
4. Select **Certificate** for the authentication type and click **Generate Request** in both the Client and Agent areas.
   - 1) An App CSR file from the Client area and an MDM CSR file from the Agent area will be downloaded to your PC.
   - 2) The MDM CSR file downloaded by the Agent area does not have a vender signature. Send the CSR file to the Samsung SDS EMM support team and receive the CSR file with the signature added.
5. Create the App APNs certificate.
   Create the certificate by uploading CSR file downloaded in 1). For more information about how to create the certificate, see the Samsung SDS EMM Installation Guide.
   - You need to sign up for the Apple Developer Enterprise Program (ADEP) to create the App APNs certificate. For more information about ADEP, see https://developer.apple.com/programs/enterprise/.
6. To create the MDM APNs certificate.
   Register the CSR file received in 2) to Apple Push Certificate Portal (https://identity.apple.com/pushcert).
   - You visit the Apple website (https://appleid.apple.com) and create your account. It is recommended to create a new account for business use because the account will be continuously used for renewing the APNs certificate.
   - On the Apple Push Certificate Portal, click **Create a Certificate**. On the “Create a New Push Certificate” page, click **Choose File** and select the downloaded CSR file and click **Upload**.
   - On the “Confirmation” page, click **Download**. The APNs certificate will be downloaded to your PC as a PEM file.
7. In the “Public Push” window of the EMM Admin Portal, click **Upload Cert** in the Agent area.
8. Click **Browse** and select the downloaded PEM file and click **OK**.
9. Click **Save** when the certificate registration is complete.

NOTE
- You can download a registered APNs certificate by clicking **Download Cert**.
- If you have issued a APNs certificate with an external CSR file, you can import the certificate by clicking **Import Cert**.

Renewing a APNs certificate

The existing APNs certificate can be renewed before the expiration date. The renewal process is same as the process for new registration. When renewing an existing APNs certificate, you must use the same Apple ID that you used to create the certificate.

Registering a APNs token

To register a token for APNs authentication, complete the following steps.

1. Navigate to **Setting** > **Server** > **Configuration**.
2. On the “Configuration” page, click **Public Push**.
3. In the “Public Push” window, click **APNs**.
4. Select **Token** in the authentication type and click in the Client area to register the token file(p8).
   - When the token file is registered, the Key ID and Team ID information are displayed.
   - The token authentication method is only supported by EMM Client. For the EMM Agent area, see Registering a APNs certificate, the existing certificate registration method.
5. Click **Save** when token registration is complete.

Setting up the email server

You can send the EMM registration information and service information via email after setting up the email server. Also, email can be transferred when an email address is registered in the user information in **User**. Use the message templates for email registered in **Setting** > **Message Template**.

To set up the email server, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Mail Server** on the top of the window.
   - **Sender email**: Enter the sender's email address.
   - **Sender Name**: Enter the sender's name.
   - **SMTP Host**: Enter the SMTP host address.
   - **Encryption**: Select the encryption status for outgoing email (None/SSL).
   - **SMTP Port**: Enter the SMTP port number.
     - If no **encryption** is selected, the SMTP port is set to the default value of 25.
   - **Timeout (sec)**: Set the time-out of the email server. (5 - 120 seconds).
     - The default value is 30 seconds.
   - **Authentication**: Select the authentication. Enter the following when Authentication's Need is selected.
     - **User Name**: Enter the user name for encryption.
     - **Password**: Enter the user password for encryption.
3. Check whether the email server runs normally by clicking **Connection Test**.
4. Click **Save**.

Configuring the SMS settings

You can install Wearable EMM on a Tizen Wearable device or log in to the Tizen wearable by sending an SMS message. The installation information of Tizen Wearable needed to send to the device via SMS is provided in **Setting** > **Message Template**. To send an SMS message, you must enter the phone number to send an SMS in **Device**.

To set up SMS, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **SMS Settings** on the top of the window.
3. Enter the caller's telephone number and select a sender type.
   - **Caller's Number**: Enter the phone number of the sender you want to send an SMS to.
   - **Sender Type**: Select the Sender that provides the SMS service. If you select **twilioSMSSender**, you can use the twilio SMS service via account registration on www.twilio.com. Also, if you select **sampleSMSSender** or **baseSMSSender**, additional development work is required for linking with the SMS service.
     - **sampleSMSSender**: This is a method to send SMS messages by developing a transmission module from an external site. Additional development work is required. For more information, see the Samsung EMM Developer's Guide.
     - **baseSMSSender**: This is a method to store messages to be sent in the SMS Queue table using the Open API provided by EMM, and to obtain necessary data from the external SMS system for sending SMS messages. For more information about Open API, which stores messages in the SMS Queue table, see the Samsung EMM Developer's Guide.
     - **amazonSMSSender**: This is a method for using the Amazon system for sending SMS messages. When you sign up on the Amazon website (https://www.amazon.com), the Access Key and the Secret Key are sent to your new account. For more information about using the SMS service via Amazon, visit the Amazon website (https://www.amazon.com).
       - **Access Key**: Enter the Access Key received from Amazon.
       - **Secret Key**: Enter the Secret Key received from Amazon.
     - **twilioSMSSender**: This is a method for using the twilio system for sending SMS messages. When you sign up on https://www.twilio.com, you will receive information that includes an Account SID and Authentication Token value sent to your new account. For more information about using the SMS service via twilio, visit https://www.twilio.com.
       - **Account SID**: Enter the Account SID you have received from twilio.
       - **Authentication Token**: Enter the Authentication Token value received from twilio.
4. Click **Save**.

Setting Terms and Policies

Set up terms and policies to create the EMM Terms of Use and Privacy Policy and End User License Agreement (EULA).

To configure the Terms and Policies, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Terms & Policies** on the top of the window.
3. In the “Terms & Policies” window, select the language you want to write, then enter the terms of use, privacy policy and end user license agreement for using the EMM.
4. Choose whether to enable or disable and to include EU countries.
    - If you select an EU country as an example, the privacy policy will be changed to a mandatory registration item.
5. Click **Save**.
    - When logging in to the EMM for the first time from a device or the Admin Portal, there will be a procedure to obtain user or administrator consent. If the consent is not checked, logging in to the EMM will be disabled.
    - When modifying the terms and policies, a notification to confirm the user’s consent is sent to the device. If the consent is not checked, the use of EMM will be disabled. (Android, iOS only)
    - When modifying the terms and policies, there will be a procedure to reconfirm administrator consent. If the consent is not checked, logging in to the EMM will be disabled.

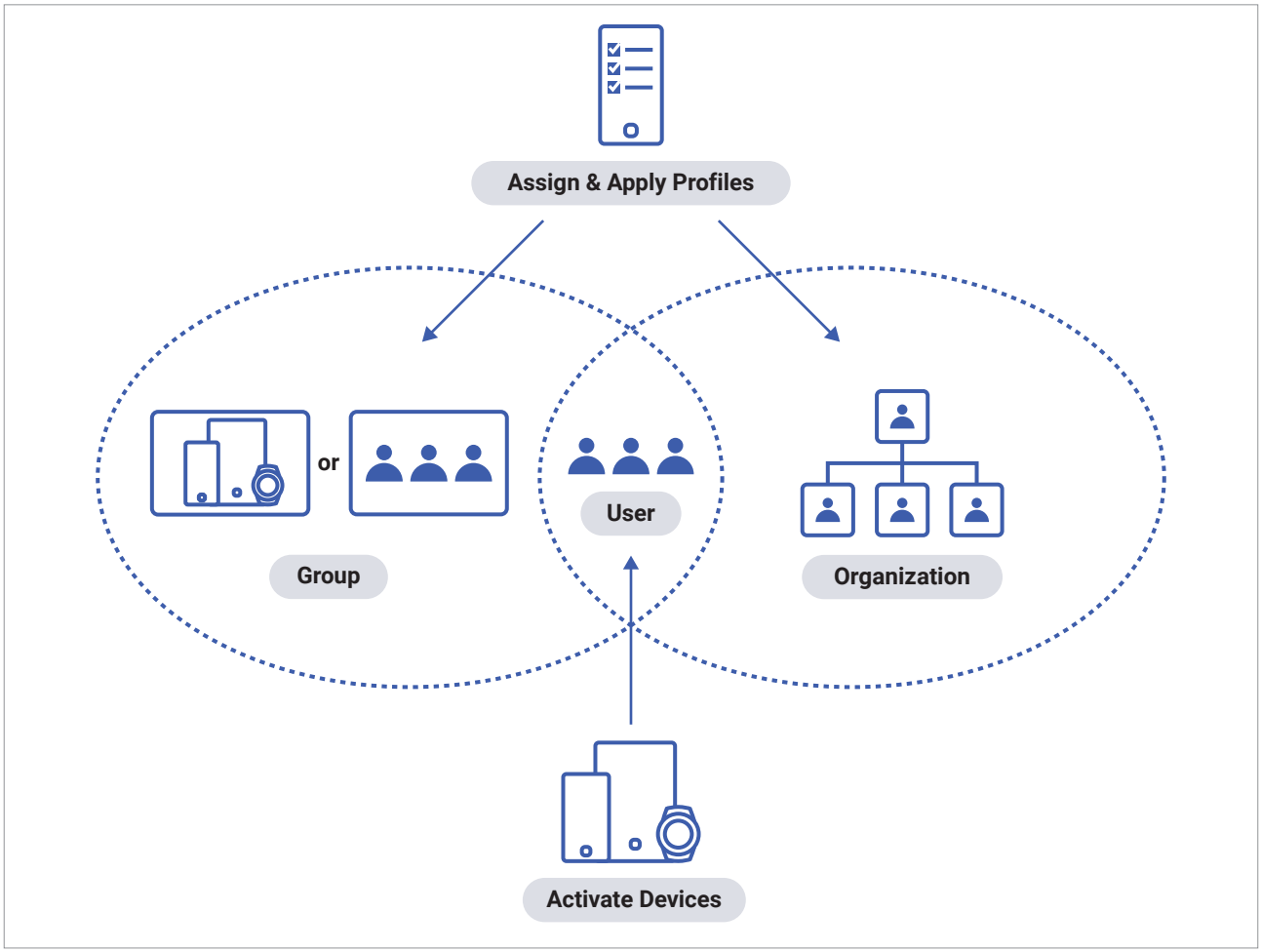
3

User/Group/ Organization

User/Group/ Organization

Create user accounts in the Admin Portal directly or add them from existing employee information by synchronizing it with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system. To activate devices, a user account must be created in advance. After creating a user account, the user can register their devices to the Admin Portal and activate their devices to be controlled by EMM.

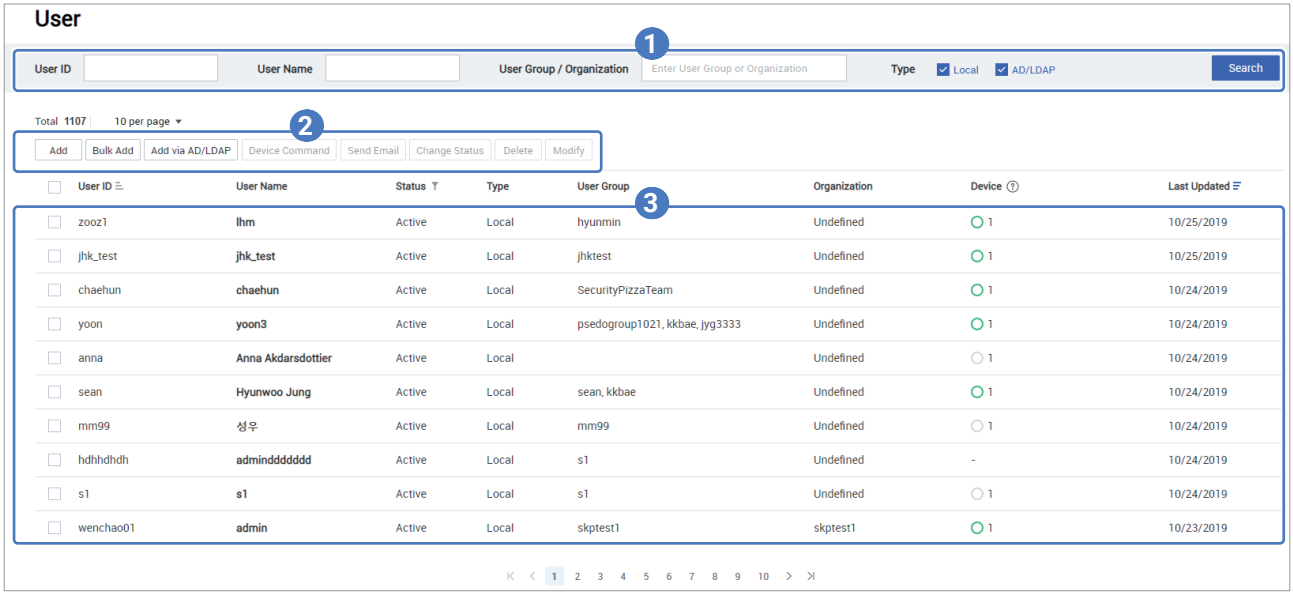
Also, users must belong to a group or an organization to be assigned profiles and have them applied. You can create a group of users or devices to manage simultaneously, and you can also manage users by organizations, which can be added in the Admin Portal or synchronized from your corporate directory server.



This chapter explains the following topics:

Viewing the user list

Navigate to **User** to view all the user accounts registered in the Admin Portal on the “User” page. You can also perform specific functions to the selected user account among the list.



No.	Name		Description
1	Search field		Search for a desired user.
2	Function buttons	Add	Add a single user account. For more information, see Registering a single user account.
		Bulk Add	Add bulk user accounts using a template. For more information, see Registering bulk user accounts.
		Add via AD/ LDAP	Add a single AD/LDAP user account or multiple user accounts at a time. For more information, see Registering a single AD/ LDAP user account and Registering multiple AD/LDAP user accounts.
		SecuCamera	Assign the SecuCamera function to users. For more information, see Assigning the SecuCamera function to users. • It differs depending on the SecuCamera license restrictions in SecuCamera under **Setting > Server > Configuration**. If the SecuCamera license is set to unlimited, all users can use SecuCamera and the SecuCamera function button will not be displayed. For more information, see Creating user accounts.
		Device Command	Send device command requests to the user's activated devices. For more information, see Sending device commands to users.
		Send Email	Send templates or user notifications registered in the Admin Portal to users via email. For more information, see Sending templates or user notifications to users via email.
		Send SMS	Send the "Tizen Wearable Installation" template to users via SMS. The mobile numbers of the users must be registered to their accounts.
		Change Status	Activate or inactivate the user account.
		Delete	Delete the selected user accounts. For more information, see Deleting user accounts.
		Modify	Modify the selected user account details. For more information, see Modifying user account details.
3	User list		View the brief information of the user accounts on the list.

Viewing the user details

View each user's details by clicking a user name on the user list. You can view the detailed information on the selected user account.

The following function buttons are available:

Function button	Description
Change Password	Enter a new password between 8 and 30 characters and confirm it. For more information, see Changing the user account password.
Reset Password	Reset the password. A temporary password will be sent to the user via email.
Change Status	Activate or inactivate the user account. For more information, see User/Group/Organization.
Send Email	Send templates or user notifications registered in the Admin Portal to the selected user via email. For more information, see Sending templates or user notifications to users via email.
Send SMS	Send the "Tizen Wearable Installation" template to users via SMS. The mobile numbers of the users must be registered to their accounts.

- **User Group / Organization**: Displays a list of groups or organizations to which the user belongs.
- **Exceptional Profile**: Displays a list of exceptional profiles assigned to the user.

Function button	Description
Manage Priority	Change the priority of exceptional profiles. For more information, see Changing priority of Exceptional Profile.
Manage Expired Profile	Unassign the expired exceptional profiles. For more information, see Unassign the expired exceptional profile.

- **Device**: Displays a list of all devices registered to the user.

Function buttons in the footer

You can perform specific functions to the selected user using the function buttons in the footer. The following function buttons are available:

Function button	Description
Back	Return to the user list.
Delete	Delete the selected user account.
Modify	Modify the selected user account information.
Sync	Synchronize the selected user account information with the AD / LDAP service.

Creating user accounts

Create a single user account directly in the Admin Portal or bulk users at a time using a template. You can also create user accounts from existing employee information by synchronizing it with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system.

You can also allow users' devices to use SecuCamera which allows users to use a camera and store the picture files on the server for security. To grant permissions for SecuCamera, register its license information on the Tenant Management System (TMS) and register the number of users.

NOTE In accordance with each country or region's privacy policies, be sure to notify the administrator or obtain consent before registering.

Registering a single user account

To register a single user account directly in the Admin Portal, complete the following steps:

1. Navigate to **User**.
2. On the "User" page, click **Add**.
3. On the "Add User" page, enter the following user information:
   - **User ID**: Enter a user ID to log in to EMM with for device activation.
   - **Password**: Enter a password between 8 and 30 characters.
     - If you set the **User Password Strength Setting** as **TRUE** (**Setting** > **Server** > **Configuration**), the password must contain letters, numbers and symbols between 8 and 30 characters.
     - Click the checkbox next to **Reset after sign-in** to allow users to change their password when they first logged in.

     NOTE If you use the AD/LDAP directory services for user authentication, you cannot change the password after the first login. Navigate to **Setting** > **Server** > **Configuration** > **Authentication Setting**, select **Manual** for **User Authentication Settings**, and select **globalLdapAuthenticator** or **globalLdapServiceAUthenticator** for the Authenticator to use the AD/LDAP directory services for user authentication. For more information about the user authentication settings, see Setting the user authentication method.

   - **Confirm Password**: Repeat the password.
   - **User Name**: Enter the user's full name.
   - **Email**: Enter the user's email address.

- **Mobile Number**: Select the country number and enter the user's mobile number. The country number is entered by default as the value in the Default Country Code in Admin under **Setting** > **Server** > **Configuration**.
- **User Group / Organization**: Click **Select**, and in the "Select User Group / Organization" window, select the user group on the User Group tab and the organization on the Organization tab.

NOTE If you do not select an organization, the user will automatically belong to the "Undefined" organization.

- **Android Manage Type**: Between **Android Legacy**, **Android Enterprise**, and **Follow Organization Type**, select a platform and management type for Android devices.
  - **Android Legacy**: Activate the device based on the manufacturer. You can select a container or Dual DAR use when creating profiles.
  - **Android Enterprise**: Activate the device based on Google B2B service. You should set Dual DAR use in the item below.
    - **Dual DAR**: To use the Dual DAR, which features enhanced security, on the Fully Managed or Work Profile on company-owned devices of Android Enterprise, select "Yes." The policies for Dual DAR can be set in the Profile menu. For more information, see Creating a new profile.

      NOTE
      - Fully Managed Dual DAR supports devices with Android 12 or higher only, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.
      - Fully Managed Dual DAR supports models that are S22, Tab S8 and above only.

    - **Work Profile on company-owned**: To activate Android Enterprise devices as the Work Profile on company-owned type, which features the enhanced work area, select "Yes." This type is supported only on devices running Android 11 or higher, and the Work Profile is automatically created on devices. EMM can manage both the personal area and the work area via policies or device commands.
  - **Follow Organization Type**: The Android Manage Type of organization you selected at **User Group/Organization** will be applied.

NOTE The user's Android manage type takes a higher priority than the organization's Android manage type. Even if you move the user to a different organization, the Android manage type set for the users still applies to the users.

- **AD/LDAP Sync**: This menu is displayed as disabled because the user account was created manually and not synchronized with the AD/LDAP system.
- **SecuCamera**: Enable or disable the SecuCamera function.
  - If the SecuCamera license is set to unlimited in SecuCamera in **Setting > Server > Configuration**, users can enable and use SecuCamera.
  - If the SecuCamera license is set to limited, to enable this function, navigate to **Setting > License**, click EMM License, and check if **SecuCamera Count** is registered on the "License Detail" page.

- **Tag**: Click **Add**, and in the “Add Tag” window, enter new tags to add.
- **Additional Information**: Enter the following additional information for the user.
  - **Employee No.**: Enter the employee number.
  - **First / Middle / Last Name**: Enter the first, middle, and last names.
  - **Display Name**: Enter the desired name to be displayed on EMM.
  - **Department**: Enter the department name.
  - **Administrator DN**: Enter the administrator DN.
  - **Email User Name**: Enter the user’s email name.
  - **Phone**: Enter the phone number.
  - **UPN**: Enter the user principal name (UPN).
  - **Position**: Enter the job position.
  - **Site**: Enter the site name.
  - **Security Level**: Enter the security level.
  - **User-Defined 1–3**: Enter the desired user-defined parameter.

4. Click **Save & Add Device**.
   - Click **Save** to create a user account only.
5. In the “Save & Add Device” window, click **OK** to create a user account. The “Add Device” page will appear. For more information on entering device information, see Viewing the device details.

Registering bulk user accounts

To register bulk user accounts at a time, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click **Bulk Add**.
3. In the “Bulk Add Users” window, follow the guideline to download and fill out the Excel file template.

   NOTE If you set the **User Password Strength Setting** as **TRUE (Setting > Server > Configuration)**, the password must contain letters, numbers and symbols between 8 and 30 characters.

4. Click  , and then select the complete Excel file template filled with the user information.
5. Click **Open**.
6. In the “Save User” window, click **OK**.

Registering a single AD/LDAP user account

To register a single AD/LDAP user account, complete the following steps:

NOTE Before registering AD/LDAP user accounts, you must connect AD/LDAP directory services with EMM and add a sync service. For more information about adding a sync service, see Adding sync services.

1. Navigate to **User**.
2. On the "User" page, click **Add via AD/LDAP**.
3. In the "Select AD/LDAP Sync Type" window, select **Single User Sync**, and then click **OK**.
4. On the "Add User" page, enter the AD/LDAP user information:
   - **Sync target**: Click **Select** to open the "Select Sync Target" window, select a sync service, and then search for users by user name. Select a user to add, and then click **OK**.
   - **User ID**: The ID of the user that you selected as Sync target will appear here.
   - **DN**: The unique Distinguished Name of the AD/LDAP object will be entered automatically.
   - **Password**: Enter a password between 8 and 30 characters.
     - If you set the **User Password Strength Setting** as **TRUE** (**Setting** > **Server** > **Configuration**), the password must contain letters, numbers and symbols between 8 and 30 characters.
     - Click the checkbox next to **Reset after sign-in** to allow users to change their password when they first logged in.

NOTE If you use the AD/LDAP directory services for user authentication, you cannot change the password after the first login.

Navigate to **Setting** > **Server** > **Configuration** > **Authentication Setting**, select **Manual** for **User Authentication Settings**, and select **globalLdapAuthenticator** or **globalLdapServiceAUthenticator** for the Authenticator to use the AD/LDAP directory services for user authentication. For more information about the user authentication settings, see Setting the user authentication method.

   - **Confirm Password**: Repeat the password.
   - **User Name**: Enter the user's full name.
   - **Email**: Enter the user's email address.
   - **Mobile Number**: Select the country number and enter the user's mobile number to send the URL address for device enrollment via SMS. The country number is entered by default as the value in the Default Country Code in Admin under **Setting** > **Server** > **Configuration**.
   - **User Group / Organization**: Click **Select**, and in the "Select User Group / Organization" window, select the user group on the User Group tab and the organization on the Organization tab.

- In the User Groups tab, select a group. You can also create a new user group by clicking **Add User Group** at the bottom. For more information, see Registering a group.
- In the Organizations tab, select an organization. You can also create a new organization by clicking **Add Organization** at the bottom. For more information, see Adding an organization.

NOTE If you do not select an organization, the user will automatically belong to the "Undefined" organization.

- **Android Manage Type**: Between **Android Legacy**, **Android Enterprise**, and **Follow Organization Type**, select a platform and management type for Android devices.
  - **Android Legacy**: Activate the device based on the manufacturer. You can select a container or Dual DAR use when creating profiles.
  - **Android Enterprise**: Activate the device based on Google B2B service. You should set Dual DAR use in the item below.
    - **Dual DAR**: To use the Dual DAR, which features enhanced security, on the Fully Managed or Work Profile on company-owned devices of Android Enterprise, select "Yes." The policies for Dual DAR can be set in the Profile menu. For more information, see Creating a new profile.

      NOTE
      - Fully Managed Dual DAR supports devices with Android 12 or higher only, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.
      - Fully Managed Dual DAR supports models that are S22, Tab S8 and above only.

    - **Work Profile on company-owned**: To activate Android Enterprise devices as the Work Profile on company-owned type, which features the enhanced work area, select "Yes." This type is supported only on devices running Android 11 or higher, and the Work Profile is automatically created on devices. EMM can manage both the personal area and the work area via policies or device commands.
  - **Follow Organization Type**: The Android Manage Type of organization you selected at **User Group/Organization** will be applied.

NOTE The user's Android manage type takes a higher priority than the organization's Android manage type. Even if you move the user to a different organization, the Android manage type set for the users still applies to the users.

- **AD/LDAP Sync**: This menu is displayed as enabled because the user account was created by synchronizing from the AD/LDAP system. If AD/LDAP Sync is selected, the existing user information will be synchronized from the AD/LDAP system and registered to the Admin Portal.
- **SecuCamera**: Enable or disable the SecuCamera function.
  - If the SecuCamera license is set to unlimited in SecuCamera in **Setting > Server > Configuration**, users can enable and use SecuCamera.
  - If the SecuCamera license is set to limited, to enable this function, navigate to **Setting > License**, click EMM License, and check if **SecuCamera Count** is registered on the "License Detail" page.

- **Tag**: Click Add, and in the "Add Tag" window, enter new tags to add.
- **Additional Information**: Enter the following additional information for the user.
  - **Employee No.**: Enter the employee number.
  - **First / Middle / Last Name**: Enter the first, middle, and last names.
  - **Display Name**: Enter the desired name to be displayed on EMM.
  - **Department**: Enter the department name.
  - **Administrator DN**: Enter the administrator DN.
  - **Email User Name**: Enter the user's email name.
  - **Phone**: Enter the phone number.
  - **UPN**: Enter the user principal name (UPN).
  - **Position**: Enter the job position.
  - **Site**: Enter the site name.
  - **Security Level**: Enter the security level.
  - **User-Defined 1–3**: Enter the desired user-defined parameter.

5. Click **Save & Add Device**.
   - Click **Save** to create a user account only.
6. In the "Save & Add Device" window, click **OK** to create a user account. The "Add Device" page will appear. For more information on entering device information, see Adding a single device.

Registering multiple AD/LDAP user accounts

To register AD/LDAP user accounts at a time, complete the following steps:

NOTE Before registering AD/LDAP user accounts, you must connect AD/LDAP directory services with EMM and add a sync service. For more information about adding a sync service, see Adding sync services.

1. Navigate to **User**.
2. On the "User" page, click **Add via AD/LDAP**.
3. In the "Select AD/LDAP Sync Type" window, select **Multiple User Sync**, and then click **OK**.
4. In the "Select Sync Target" window, select a sync service, and then search for users with their names.
5. Click the checkboxes for users to add, and then click **OK**.
   - To delete the selected users on the selected users list, click 🗑.

Managing user accounts

You can view the detailed user account information, modify user account details, send activation guides or templates registered in the Admin Portal to users via email and/or SMS, and delete user accounts.

Modifying user account details

To modify the user account details, complete the following steps:

1. Navigate to **User**.
2. On the "User" page, click the checkbox next to the user ID to modify the account details, and then click **Modify**.
3. On the "Modify User" page, modify the following user information if necessary:
   - **User Name**: Modify the user's full name.
   - **Email**: Modify the user's email address.
   - **Mobile Number**: Modify the country number and the user's mobile number.
   - **User Group / Organization**: Click **Select** and then, in the "Select User Group / Organization" window, select the user group on the User Group tab and the organization in the Organization tab.
     - In the User Groups tab, select a group. You can also create a new user group by clicking **Add User Group** at the bottom. For more information, see Registering a group.
     - In the Organizations tab, select an organization. You can also create a new organization by clicking **Add Organization** at the bottom. For more information, see Adding an organization.
   - **Android Manage Type**: Between **Android Legacy**, **Android Enterprise**, and **Follow Organization Type**, select a platform and management type for Android devices.
     - **Android Legacy**: Activate the device based on the manufacturer. You can select a container or Dual DAR use when creating profiles.
     - **Android Enterprise**: Activate the device based on Google B2B service. You should set Dual DAR use in the item below.
       - **Dual DAR**: To use the Dual DAR, which features enhanced security, on the Fully Managed or Work Profile on company-owned devices of Android Enterprise, select "Yes." The policies for Dual DAR can be set in the Profile menu. For more information, see Creating a new profile.

         NOTE
         - Fully Managed Dual DAR supports devices with Android 12 or higher only, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.
         - Fully Managed Dual DAR supports models that are S22, Tab S8 and above only.

- **Work Profile on company-owned**: To activate Android Enterprise devices as the Work Profile on company-owned type, which features the enhanced work area, select "Yes." This type is supported only on devices running Android 11 or higher, and the Work Profile is automatically created on devices. EMM can manage both the personal area and the work area via policies or device commands.
- **Follow Organization Type**: The Android Manage Type of organization you selected at **User Group/Organization** will be applied.

> **NOTE** The user's Android manage type takes a higher priority than the organization's Android manage type. Even if you move the user to a different organization, the Android manage type set for the users still applies to the users.

- **AD/LDAP Sync**: Allows creating user accounts from the AD/LDAP system.
- **SecuCamera**: Enable or disable the SecuCamera function.
  - If the SecuCamera license is set to unlimited in SecuCamera in **Setting > Server > Configuration**, users can enable and use SecuCamera.
  - If the SecuCamera license is set to limited, to enable this function, navigate to **Setting > License**, click EMM License, and check if **SecuCamera Count** is registered on the "License Detail" page.
- **Tag**: Click **Add**, and in the "Add Tag" window, enter new tags to add.
- **Additional Information**: Modify the following additional information for the user.
  - **Employee No.**: Enter the employee number.
  - **First** / **Middle** / **Last Name**: Enter the first, middle, and last names.
  - **Display Name**: Enter the desired name to be displayed on EMM.
  - **Department**: Enter the department name.
  - **Administrator DN**: Enter the administrator DN.
  - **Email User Name**: Enter the user's email name.
  - **Phone**: Enter the phone number.
  - **UPN**: Enter the user principal name (UPN).
  - **Position**: Enter the job position.
  - **Site**: Enter the site name.
  - **Security Level**: Enter the security level.
  - **User-Defined 1–3**: Enter the desired user-defined parameter.

4. Click **Save** to save the modified user account information.
5. In the "Save Changes" window, click **OK**. Profiles and applications assigned to group or organization will be automatically assigned to the user.

Activating or inactivating user accounts

You can activate as many users as there are licenses in use. When a user account is added to the Admin Portal, the user account is activated automatically. If there are no remaining licenses, the newly added user account cannot be activated.

To activate or inactivate user accounts, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click a user name on the list.
3. On the “User Detail” page, click **Change Status** to activate or inactivate the user account. The status of the user account is displayed next to **Status**.

> **NOTE** To inactivated EMM, both user and device status must be changed to inactive.

Sending device commands to users

You can send device commands to the user’s activated devices. For more information on each device command, see Sending device commands to devices.

To send device commands, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click the checkbox next to the user ID to send a device command to.
3. Click **Device Command** and select the supported OS platform (activated device).
4. In the “Device Command” window, select a desired device command.
5. In the “Request Command” window, click **OK**.

Sending templates or user notifications to users via email

To send templates or user notifications registered in EMM to users via email, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click the checkbox next to the user ID you want to send activation guides to, and then click **Send Email**.
3. In the “Send Email” window, select a template file from the template list, and then click **Send**.

NOTE To activate a Tizen Wearable device, select the “Tizen Wearable Installation” template.

- Click to view a preview of the selected template.

NOTE For more information on templates, see Managing administrator accounts.

Changing the user account password

To change the user account password, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click a user name to change its password.
3. On the “User Detail” page, click **Change Password**.
4. In the “Change Password” window, enter the following user password information:
   - **New Password**: Enter a new password between 8 and 30 characters.
     When you set the User Password Strength Setting as TRUE (Setting > Server > Configuration), the password must contain letters, numbers and symbols between 8 and 30 characters.
   - **Confirm Password**: Repeat the new password.
5. Click **Save**.
   - Click the checkbox next to **Reset after sign-in** to allow the user to change the password when logged in first.

Resetting the user account password

To reset the user account password, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click a user name to reset its password.
3. On the “User Detail” page, click **Reset Password**.
4. In the “Reset Password” window, click **OK**.
   - A temporary user account password will be sent to the user via email.

Deleting user accounts

To delete user accounts, complete the following steps:

NOTE To delete a user account, the status of all the devices must be “Deactivated,” “Activation blocked,” “Blocked by System,” or “Blocked by Admin.”

1. Navigate to **User**.
2. On the “User” page, click the checkbox next to the user ID you want to delete, and then click **Delete**.
3. In the “Delete User” window, click **OK**.

Assigning the SecuCamera function to users

You can assign the SecuCamera function to activated users. This function can only be assigned to as many users as there are available licenses. Also, the assigned the SecuCamera function can be revoked.

To assign the SecuCamera function to users, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click **SecuCamera**.
3. In the “SecuCamera Users” window, click the checkboxes next to the user ID you want to assign the SecuCamera function to. If you have selected any users, the selected users are displayed on the Selected User tab.

- To select all of the users registered on EMM, click **Select All users**.
- The SecuCamera feature only supports Android Legacy (Knox Workspace) devices.

4. Click **Assign**.

Changing priority of Exceptional Profile

You can change the priority of profiles when users have been applied multiple exceptional profiles.

To change the priority, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click the **user name** to change priority.
3. On the “User Detail” page, click the **Manage Priority** next to Exceptional Profile.
4. In the “Manage Priority” window, click ↑ or ↓ to prioritize the selected profile.
   - Changing priority is only applicable when exception type is policy. The latest assigned exceptional profile has the lowest priority.
5. Click **Save**.
6. In the “Save Priority” window, click **OK**.

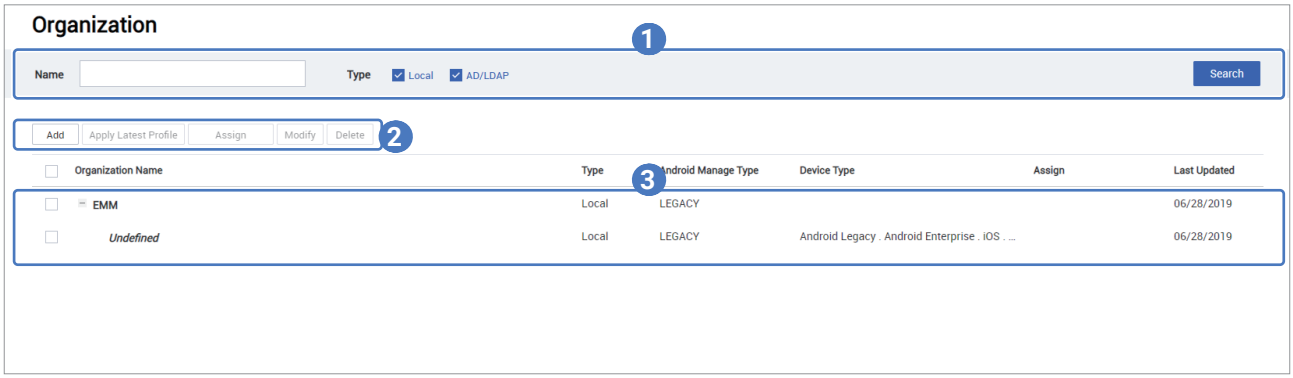
Unassign the expired exceptional profile

To unassign the exceptional profile which has been expired, complete the following steps:

1. Navigate to **User**.
2. On the “User” page, click the **user name** to change priority.
3. On the “User Detail” page, click **Manage Expired Profile**.
4. In the “Manage Expired Profile” window, check the box next to Exception Type.
   - Click **Unassign All** to unassign all profiles of the user.
5. Click **Unassign**.
6. In the “Unassign Profile” window, click **OK**.

Viewing the organization list

Navigate to **Organization** to view all the organizations registered in the Admin Portal on the “Organization” page. You can also perform specific functions to the selected organizations among the list.



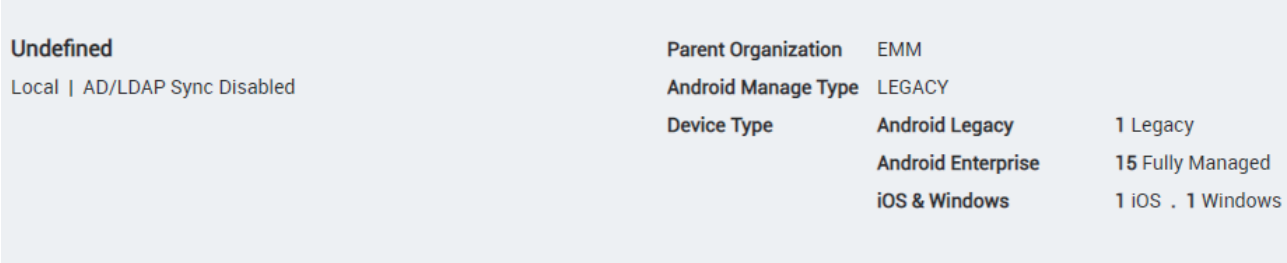
No.	Name		Description
1	Search field		Search for a desired organization.
2	Function buttons	Add	Add a sub-organization in the parent organizations individually, or add a sub-organization by synchronizing organizations with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system. For more information, see Adding an organization.
		Add Sub-Org	Add a sub-organization to the selected organization individually, or add a sub-organization by synchronizing organizations with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system.
		Apply Latest Profile	Apply the latest assigned profile to the selected organization. For more information, see Applying the latest profiles to organizations.
		Modify	Modify the selected organization details. For more information, see Modifying the organization details.
		Delete	Delete the selected organization. For more information, see Deleting the organizations.
		Application (Assign)	Assign applications to the selected organization. For more information, see Assigning applications to organizations.
		Profile (Assign)	Assign profiles to the selected organization. For more information, see Assigning and applying profiles to organizations.
		Content (Assign)	Assign contents to the selected organization. For more information, see Assigning and deploying content to organizations.
3	Organization list		View the brief information of the organizations on the list.

Viewing the organization details

View each organization's details by clicking an organization name on the organization list. For more information about each section of the detail page, see Detail page.

Summary area

The summary area contains the information about the selected organization such as organization settings, user's device types and detailed information.



Tab: User

The User tab shows the user account information in the organization.

- **Detail**: Move to the "User Detail" page for the selected user. For more information on the "User Detail" page, see Viewing the user details.

The following function buttons are available:

Function button	Description
Add	Add users to the selected organization.
Change Organization	Move the selected users to other existing organizations. For more information, see Changing user's organizations.
Send Email	Send templates or user notifications registered in the Admin Portal to users via email. For more information, see Sending templates or user notifications to users via email. **NOTE** To activate a Tizen Wearable device, select the "Tizen Wearable Installation" template.
Send SMS	Send the "Tizen Wearable Installation" template to users via SMS. The mobile numbers of the users must be registered to their accounts.
Delete User	Delete the selected users from the organization. If a user in the organization is deleted, the user will be moved to the "Undefined" organization.

Tab: Device

The Device tab shows the status of the devices that belong to the organization, the device names and tags, IMEI/MEID (the additional IMEI will be displayed if using Dual SIM), the Last Seen, Platform & Manage Type, and Last Updated.

- **Detail**: Move to the "Device Detail" page for the selected device. For more information on the "Device Detail" page, see Viewing the device details.

Function button	Description
Refresh	Update the list of devices.

Tab: Application

The Application tab shows the applications assigned to the organization. The following function buttons are available:

Function button	Description
Unassign	Unassign the application assigned to the organization. **NOTE** If **Uninstall if the app is unassigned** is selected in the selected application settings, the application will be removed from the devices. However, if the selected application is assigned to other groups or organizations, the application will not be removed even if you unassign it.
Modify Setting	Modify the settings for the selected application. For more information, see Modifying applications.

Tab: Profile

The Profile tab shows the profiles assigned or applied to the organization.

Function button	Description
Unassign	Unassign the profile assigned to the organization.

Tab: Content

The Content tab shows the content that has been assigned or deployed to the organization. The following function buttons are available:

Function button	Description
Unassign	Unassign the content assigned to the organization.
See Setting	View Download Type, Deployment Area, and Device Platform of the content assigned to deployment. For more information, see Assigning and deploying content.

Function buttons in the footer

You can perform specific functions to the organization using the function buttons in the footer.

The following function buttons are available:

Function button	Description
Back	Return to the organization list.
Delete	Delete the selected organization.
Modify	Modify the selected organization's details.
Assign	Assign applications, profiles or contents to the selected organizations.
Apply Latest Profile	Apply the latest assigned profiles to the selected organizations.

Managing organizations

Configure the hierarchy of organizations for users and apply various profiles to each organization. After configuring the organizations and assigning the users to each organization, you can view the information on user account, activated devices, applications, profiles and contents by organization.

Adding an organization

Create a sub-organization in the parent organizations individually, or add a sub-organization by synchronizing organizations with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system.

To add a sub-organization, complete the following steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click **Add**.
3. On the “Add Organization” page, enter the following user information:
    - **Parent Organization**: Select the parent organization to add a sub-organization to.
    - **Inheritable Profile**: Displays the profiles inherited with the parent organization. If there is no inheritable profiles, **None** is displayed. If a sub-organization was not assigned a profile and saved, the profile of the parent organization is inherited and applied.
    - **Code**: Enter a new organization code that complies with the organization format.

    NOTE Once the organization code is saved, you cannot change it.

    - **Name**: Enter a new organization name.
    - **AD/LDAP Sync**: Allow the creating of organizations from the AD/LDAP system. If **Enable** is selected, the existing organization information, including its sub-organizations, will be synchronized from the AD/LDAP system and registered to the Admin Portal.

    NOTE To create AD/LDAP organizations, you must connect AD/LDAP directory services with EMM and add a sync service. For more information about adding a sync services, see Adding sync services.

- **Android Manage Type**: Between **Android Legacy** and **Android Enterprise**, select a platform and management type for Android devices.
  - **Android Legacy**: Activate the device based on the manufacturer. You can select a container or Dual DAR use when creating profiles.
  - **Android Enterprise**: Activate the device based on Google B2B service. You should set Dual DAR use in the item below.
    - **Dual DAR**: To use the Dual DAR, which features enhanced security, on the Fully Managed or Work Profile on company-owned devices of Android Enterprise, select "Yes." The policies for Dual DAR can be set in the Profile menu. For more information, see Creating a new profile.

      NOTE
      - Fully Managed Dual DAR supports devices with Android 12 or higher only, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.
      - Fully Managed Dual DAR supports models that are S22, Tab S8 and above only.

    - **Work Profile on company-owned**: To activate Android Enterprise devices as the Work Profile on company-owned type, which features the enhanced work area, select "Yes." This type is supported only on devices running Android 11 or higher, and the Work Profile is automatically created on devices. EMM can manage both the personal area and the work area via policies or device commands.
- **Sub-Administrator**: Select the administrators to manage the organization. If you log in to the Admin Portal for the first time as a super administrator, there will be no subadministrators registered to the Admin Portal. For more information on creating subadministrators, see Adding an administrator.

4. Click **Save & Assign**, and in the "Save & Assign" window, click **Application**, **Profile** or **Content** to select what to assign to the organization.
   - **Application**: Select the applications to assign to the organization, and then modify the application settings.
   - **Profile**: Select the profiles to assign to the organization, and then view the selected profile details.
   - **Content**: Select the content assigned to the organization, and modify the settings for content assignment and deployment.
   - Click **Save** to register the organization.

Modifying the organization details

After you create an organization, you can modify the organization information.

To modify the organization information, complete the following steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to the desired organization to modify its details, and then click **Modify**. To expand or collapse the parent organization, click + or — next to the organization name. You can also double-click the row of the desired organization to expand or collapse it.
3. In the “Modify Organization” window, modify the following existing organization information:
   - **Code**: Displays the organization’s code.

     NOTE Once the organization code is saved, you cannot change it.

   - **Name**: Enter a new organization name.
   - **Parent Organization**: Select the parent organization to add a sub-organization.
   - **Inheritable Profile**: Displays the profiles inherited with the parent organization.
   - **AD/LDAP Sync**: Allow creating organizations from the AD/LDAP system.
   - **Android Manage Type**: Between **Android Legacy** and **Android Enterprise**, select a platform and management type for Android devices.
     - **Android Legacy**: Activate the device based on the manufacturer. You can select a container or Dual DAR use when creating profiles.
     - **Android Enterprise**: Activate the device based on Google B2B service. You should set Dual DAR use in the item below.
       - **Dual DAR**: To use the Dual DAR, which features enhanced security, on the Fully Managed or Work Profile on company-owned devices of Android Enterprise, select “Yes.” The policies for Dual DAR can be set in the Profile menu. For more information, see Creating a new profile.

         NOTE
         - Fully Managed Dual DAR supports devices with Android 12 or higher only, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.
         - Fully Managed Dual DAR supports models that are S22, Tab S8 and above only.

- **Work Profile on company-owned**: To activate Android Enterprise devices as the Work Profile on company-owned type, which features the enhanced work area, select “Yes.” This type is supported only on devices running Android 11 or higher, and the Work Profile is automatically created on devices. EMM can manage both the personal area and the work area via policies or device commands.

- **Sub-Administrator**: Click **Select** to add sub-administrators to the organization.

4. Click **Save**.

Changing user’s organizations

You can change a user’s organizations to the desired organizations.

To change a user’s organizations, complete the following steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click a specific organization name to move the user between organizations.

NOTE To expand or collapse the parent organization, click + or — next to the organization name. You can also double-click the row of the desired organization to expand or collapse it.

3. On the “Organization Detail” page, click the User tab.
4. On the User tab, click the checkboxes next to the user IDs, and then click **Change Organization**.
5. In the “Select Organization” window, click the desired organization in the tenant tree, and then click **OK**.

Assigning applications to organizations

After applications are registered to the Admin Portal, you can assign them to specific organizations.

To assign applications to organizations, complete the followings steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to the organization name you want to assign the application to, and then click **Application** next to **Assign**.
3. In the “Select Application” window, click the checkboxes next to the applications to assign, and then click **Assign**.

4. On the “Assign Application” page, configure the assignment settings, and then click **Assign**.

NOTE

- The application settings vary depending on the platform, source, assigning device platform, and management type. For more information, see Assigning applications.
- The application assigned to the parent organization is not inherited, so it must be additionally assigned to the sub-organizations.

5. In the “Assign Application” window, click **OK**.

Assigning and applying profiles to organizations

After profiles are registered to the Admin Portal, you can assign and apply them to specific organizations.

To assign and apply profiles to organizations, complete the followings steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to an organization name you want to assign and apply the profile to, and then click **Profile** next to **Assign**.
3. In the “Select Profile” window, select the profile to assign, and then click **Assign**.

NOTE

- For more information on assigning and applying profiles, see Assigning to organizations.
- When a profile is assigned to a parent organization, its sub-organizations inherit the profile.

4. On the “Assign Profile” page, click **Assign & Apply**.
   - Click **Assign** to assign the profile to the selected organizations and to not apply the profile now.
5. In the “Apply Profile” window, click **OK**. The profile will be assigned and applied to the selected organizations at the same time.

Assigning and deploying content to organizations

After adding content to Admin Portal, assign and deploy that content to specific organizations.

To assign and deploy content to organizations, complete the followings steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to an organization name you want to assign and apply the content to, and then click **Content** next to **Assign**.
3. In the “Select Content” window, select the assigned content, and then click **Assign & Deploy**.
   - Click **Assign** to only assign content to an organization. In the “Assign & Deploy Content” window, check Download Type, Target Organization, Content Name, and Deployment Area, and then click **OK**.

NOTE

- For more information about assigning and deploying content, see Assigning and deploying content.
- The content assigned to the parent organization is not inherited, so it must be additionally assigned to the sub-organizations.

4. In the “Assign & Deploy Content” window, check Download Type, Target Organization, Content Name, and Deployment Area, and then click **OK**.
   - Download Type: Select a download type. If you select Automatic, the content will be downloaded to the device automatically at the same time as deployment. If you select Manual, the user must download the content manually.

Applying the latest profiles to organizations

Apply the latest assigned profile to an organization.

To apply an assigned profile to an organization, complete the following steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to the organization name you want to apply the latest profile to, and then click **Apply Latest Profile**.
3. In the “Apply Profile” window, click **OK**.

Deleting the organizations

To delete organizations, complete the following steps:

1. Navigate to **Organization**.
2. On the “Organization” page, click the checkbox next to the organization name you want to delete, and then click **Delete**.

NOTE If you delete a parent organization that has sub-organizations, the sub-organizations will become parent organizations.

3. In the “Delete Organization” window, click **OK**.

Viewing the group list

Navigate to **Group** to view all the groups registered in the Admin Portal on the “Group” page. You can also perform specific functions to the selected groups among the list.

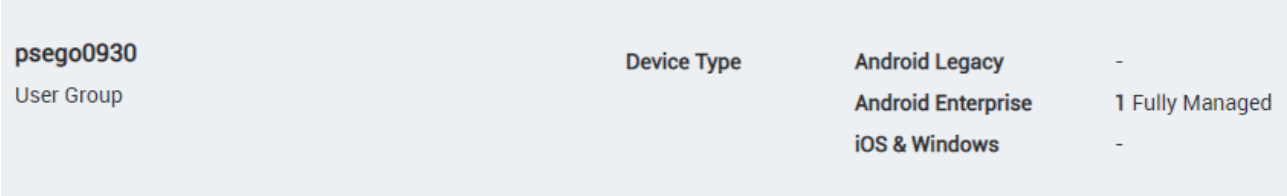
No.	Name		Description
1	Search field		Search for a desired group.
2	Function buttons	Add	Add a group of users or devices. For more information, see Registering a group.
		Add via AD/ LDAP	Add a group from existing employee information by synchronizing it with the AD/LDAP system. For more information, see Registering an AD/LDAP sync group.
		Device Command	Send device command requests to the activated devices in the group. For more information, see Sending device command requests to groups.
		Delete	Delete the selected group. For more information, see Deleting the groups.
		Application (Assign)	Assign applications to the selected groups. For more information, see Assigning applications to groups.
		Profile (Assign)	Assign profiles to the selected groups. For more information, see Assigning and applying profiles to groups.
		Content (Assign)	Assign contents to the selected groups. For more information, see Assigning and deploying content to groups.
3	Group list		View the brief information of the groups on the list.

Viewing the group details

View each group's details by clicking a group name on the group list. For more information about each section of the detail page, see Detail page.

Summary area

The summary area contains the information about the selected group such as group and user's device types.



Tab: User (For user or AD/LDAP groups)

The User tab for user or AD/LDAP groups shows the information of the user accounts in the group.

- **Detail**: Move to the "User Detail" page for the selected user. For more information on the "User Detail" page, see Viewing the user details.

The following function buttons are available:

Function button	Description
Add	Add a user to the group from the user list. For more information, see Adding users to user groups.
Send Email	Send templates or user notifications registered in the Admin Portal to users via email. For more information, see Sending templates or user notifications to users via email.
Send SMS	Send the "Tizen Wearable Installation" template to users via SMS. The mobile numbers of the users must be registered to their accounts.
Delete User	Delete the selected user from the group. **NOTE** You cannot delete users from the AD/LDAP group.

Tab: User (For device groups)

The User tab for device groups shows the information of the user's devices and user accounts in the group.

- **Detail**: Move to the "User Detail" page for the selected user. For more information on the "User Detail" page, see Viewing the user details.

The following function buttons are available:

Function button	Description
Send Email	Send templates or user notifications registered in the Admin Portal to users via email. For more information, see Sending templates or user notifications to users via email.
Send SMS	Send the "Tizen Wearable Installation" template to users via SMS. The mobile numbers of the users must be registered to their accounts.

Tab: Device (For user or AD/LDAP groups)

The Device tab for user or AD/LDAP groups shows the status of the devices in the group, the device names and tags, IMEI/MEID (the additional IMEI will be displayed if using Dual SIM), the Last Seen, Platform & Manage Type, and Last Updated.

- **Detail**: Move to the "Device Detail" page for the selected user's device. For more information on the "Device Detail" page, see Viewing the device details.

Function button	Description
Refresh	Update the list of devices.

Tab: Device (For device groups)

The Device tab for device groups shows the status of the devices in the group, the device names and tags, IMEI/MEID (the additional IMEI will be displayed if using Dual SIM), the Last Seen, Platform & Manage Type, and Last Updated.

- **Detail**: Move to the "Device Detail" page for the selected device. For more information on the "Device Detail" page, see Viewing the device details.

Function button	Description
Refresh	Update the list of devices.
Add	Add a device from the device list to the group. For more information, see Adding devices to device groups.
Delete Device	Delete the selected device from the group.

Tab: Application

The Application tab shows the applications assigned to the group. The following function buttons are available:

Function button	Description
Unassign	Unassign the applications assigned to the group. **NOTE** If **Uninstall if the app is unassigned** is selected in the selected application settings, the application will be removed from the devices. However, if the selected application is assigned to other groups or organizations, the application will not be removed even if you unassign it.
Modify Setting	Modify the settings for the selected application. For more information, see Managing applications.

Tab: Profile

The Profile tab shows the profiles assigned to the group. The following function buttons are available:

Function button	Description
Unassign	Unassign the profiles assigned to the group.

Tab: Content

The Content tab shows the content that has been assigned or deployed to the group. The following function buttons are available:

Function button	Description
Unassign	Unassign the content assigned to the group.
See Setting	View Download Type, Deployment Area, and Device Platform of the content assigned to deployment. For more information, see Assigning and deploying content.

Tab: Command History

The Command History tab shows the command histories of the group.

- **Detail**: Move to the “Device Detail” page for the selected user’s device. For more information, see Viewing the device details.

Function buttons in the footer

You can perform specific functions to the group using the function buttons in the footer.

The following function buttons are available:

Function button	Description
Back	Return to the group list.
Delete	Delete the selected group.
Assign	Assign applications profiles or contents to the selected group.
Apply Latest Profile	Apply the latest assigned profiles to the selected group.
Device Command	Select a device command and send it to the activated devices in the selected group.

Creating groups of users or devices

A group can be composed either of users or devices. Once a group is created, you can assign and apply applications, profiles and contents to the group of users or devices. Create a group directly in the Admin Portal or from existing employee information by synchronizing it with the Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) system.

Registering a group

To create a group of users or devices, complete the following steps:

1. Navigate to **Group**.
2. On the “Group” page, click **Add**.
3. On the “Add Group” page, enter the following user information:
   - **Name**: Enter a group name.
   - **Type**: Select one of the following group types.
     - **User**: A group composed of user accounts only
     - **Device**: A group composed of devices only
4. On the user or device list, click the checkboxes next to the user IDs or device names to include them in the group. After the users or devices are selected, they will be displayed on the selected user or selected device list.
   - You can also search for and select devices using filters. In the “Selected Device” area, click **Select via Filter**, and then click the checkboxes for the filters you want to apply, such as user status, position, and security level. Filtered devices will be added to the selected device list.
5. Click **Save & Assign**, and in the “Save & Assign” window, click **Application**, **Profile** or **Content** to select what to assign to the group.
   - **Application**: Select the applications to assign to the group, and then modify the application settings.
   - **Profile**: Select the profiles to assign to the group, and then view the selected profile details.
   - **Content**: Select the content assigned to the group, and modify the settings for content assignment and deployment.
   - Click **Save** to create a group only.

Registering an AD/LDAP sync group

To create a group from existing employee information by synchronizing it with the AD/LDAP system, complete the following steps:

1. Navigate to **Group**.
2. On the “Group” page, click **Add via AD/LDAP**.
3. In the “Select Sync Target” window, enter the AD/LDAP group information:
   - **Sync Target**: Select a synchronization service to search for groups. If you have selected a synchronization service, the relevant filter is automatically entered.
   - **Keyword Search**: Enter a keyword to search for groups within the selected range, and then click **Search**.
4. Select a group from the search result, and then click **OK**.
5. On the “Add AD/LDAP Group” page, enter the following group information:
   - **Sync target**: Click **Select** to open the “Select Sync Target” window. For more information, see step 3.
   - **Group Name**: Enter a group name.
   - **Profile/App Auto Apply**: Select when to apply a profile or application to a group member automatically. (**When Adding a User**, **When Deleting a User**, **When Deleting a Group**)
   - **Sync Group Member**: Select whether sync all users or only the selected users of the group.
     - **Sync All**: Sync all members of the group.
     - **Sync Selected Only**: Sync only the selected members of the group.
6. Click **Save & Assign**, and in the “Save & Assign” window, click **Application**, **Profile** or **Content** to select what to assign to the group.
   - **Application**: Select the applications to assign to the group, and then modify the application settings.
   - **Profile**: Select the profiles to assign to the group, and then view the selected profile details.
   - **Content**: Select the content assigned to the group, and modify the settings for content assignment and deployment.
   - Click **Save** to create a group only.

Managing groups

After configuring the groups of users or devices, apply various profiles to each group. You can also view the detailed information of the user account, devices, device locations, applications, and profiles by group.

Adding users to user groups

After creating a user group, you can add users to it.

To add users to a user group, complete the following steps:

1. Navigate to **Group**.
2. On the “Group” page, click a specific user group name to add users to.

NOTE The group type must be **User**.

3. On the “Group Detail” page, click the User tab.
4. On the User tab, click **Add**.
5. In the “Select User” window, click the checkboxes next to the user ID to select users to add and then, click **Add**. To delete the selected users on the selected user list, click 🗑.
6. In the “Add User” window, click **OK**.

NOTE After changing users (add/delete) in user groups, click **Yes** to apply the profiles and apps to the groups.

Adding devices to device groups

After creating a device group, if required, you can add devices to the desired device group.

To add devices to a device group, complete the following steps:

1. Navigate to **Groups**.
2. On the “Group” page, click a specific device group name to add devices to.

NOTE The group type must be **Device**.

3. On the “Group Detail” page, click the Device tab.
4. On the Device tab, click **Add**.
5. In the “Select Device” window, click the checkboxes next to the device name to select devices to add, and then click **Add**. To delete the selected devices on the selected device list, click 🗑.
   - You can also search for and select devices using filters. In the “Selected Device” area, click **Select via Filter**, and then click the checkboxes for the filters you want to apply, such as user status, position, and security level. Filtered devices will be added to the selected device list.
6. In the “Add Device” window, click **OK**.

NOTE After changing devices (add/delete) in device groups, click **Yes** to apply the profiles and apps to the groups.

Assigning applications to groups

After applications are registered to the Admin Portal, you can assign them to specific groups.

To assign applications to groups, complete the followings steps:

1. Navigate to **Group**.
2. On the “Group” page, click the checkbox next to the group name you want to assign the application to, and then click **Application** next to **Assign**.
3. In the “Select Application” window, click the checkboxes next to the applications to assign, and then click **Assign**.
4. On the “Assign Application” page, configure the assignment settings, and then click **Assign**.

NOTE The application settings vary depending on the platform, source, assigning device platform, and management type. For more information, see Assigning applications.

5. In the “Assign Application” window, click **OK**.

Assigning and applying profiles to groups

After profiles are registered to the Admin Portal, you can assign and apply them to specific groups.

To assign and apply profiles to groups, complete the followings steps:

1. Navigate to **Group**.
2. On the “Group” page, click the checkbox next to the group name you want to assign and apply the profile to, and then click **Profile** next to **Assign**.
3. In the “Select Profile” window, select the profile to assign, and then click **Assign**.

NOTE For more information on assigning and applying profiles, see Assigning to groups.

4. On the “Assign Profile” page, click **Assign & Apply** to assign and apply the profile to the selected groups at the same time.
   - Click **Assign** to assign the profile to the selected groups and not to apply the profile now.

Assigning and deploying content to groups

After adding content to Admin Portal, assign and deploy that content to specific groups.

To assign and deploy content to groups, complete the followings steps:

1. Navigate to **Group**.
2. On the “Group” page, click the checkbox next to a group name you want to assign and apply the content to, and then click **Content** next to **Assign**.
3. In the “Select Content” windows, select the assigned content, and then click **Assign & Deploy**.
   - Click **Assign** to only assign content to a group. In the “Assign & Deploy Content” window, check Download Type, Target Group, Content Name, and Deployment Area, and then click **OK**.

NOTE For more information about assigning and deploying content, see Assigning and deploying content.

4. In the “Assign & Deploy Content” window, check Download Type, Target Group, Content Name, and Deployment Area, and then click **OK**.
   - Download Type: Select a download type. If you select Automatic, the content will be downloaded to the device automatically at the same time as deployment. If you select Manual, the user must download the content manually.

Sending device command requests to groups

You can send device command requests to the user's activated devices. For more information on each device command, see Sending device commands to devices.

To send device command requests, complete the following steps:

1. Navigate to **Group**.
2. On the "Group" page, click the checkbox next to the group name to send a device command request to.
3. Click **Device Command** and select the supported OS platform (activated device).
4. In the "Device Command" window, select a desired device command.
5. In the "Request Command" window, click **OK**.

Deleting the groups

To delete groups, complete the following steps:

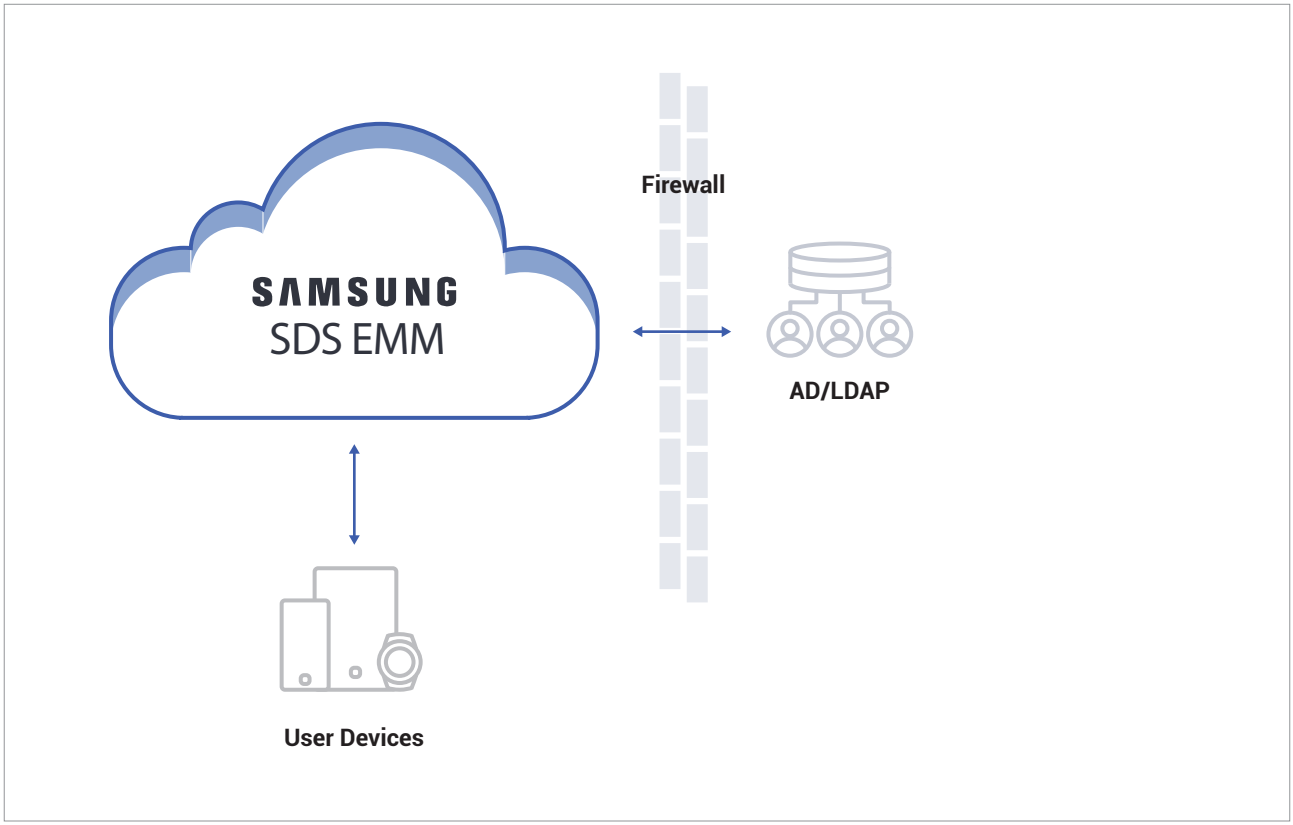
1. Navigate to **Group**.
2. On the "Group" page, click the checkbox next to the group name you want to delete, and then click **Delete**.
3. In the "Delete Group" window, click **Yes**.

NOTE To maintain the assigned applications and profiles of this group for the user, select **No**. To unassign the applications and profiles of this group from the user, select **Yes**.

Syncing user information with AD/LDAP

Add information about users, groups, and organizations to the EMM server through the Active Directory (AD) service that is built upon the industry-standard Lightweight Directory Access Protocol (LDAP). This service enables you to keep user, organizational, and group information synchronized across multiple sites throughout the enterprise and update information on demand or automatically at specified intervals.

The AD/LDAP service provided by EMM includes filtered search capabilities for viewing user information and historical data about sync services.



Adding sync services

Add AD/LDAP directory services in EMM to synchronize user, organizational, and group information. Once added, you can sync through the corresponding menus in **User**, **Group**, and **Organization**.

To add a sync service, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. On the “Sync Service” page, click  .
3. In the “Add Sync Service” window, click the Preferences tab.
4. Enter information required for specifying the basic information about a sync service.
   - **Sync Service ID**: Enter the sync service ID (up to 25 characters consisting of letters, numbers, and special characters (- or _ only). It will be used to distinguish each sync service and also used when selecting sync services in **User**, **Group**, and **Organization**.
   - **Auto Sync Setup**: Click the checkbox next to **Auto Sync Setup** to use automatic synchronization and enter the schedule and iteration cycle in the pop-up window:
     - **Target Server**: Click the drop-down menu and select the target server address to use for the automatic synchronization.
     - **Time Zone**: Click the drop-down menu and select the time zone to use for the automatic synchronization.
     - **Sync Interval**: Click the drop-down menu and select a sync service interval: **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Advanced Settings**. If you select the advanced settings, set a regular interval in month, week, day, or hour format using cron expressions.
     - **Sync Schedule**: Set the **Start Date** and **Start Time** for the sync service.
   - **Target**: Click the checkbox next to **User**, **Group**, or **Organization** as the target information to retrieve from the directory through the sync service.
5. Enter information required for specifying the LDAP server information.
   - **Directory Type**: Select a directory. Select **Other** when connecting to other directory servers except the Microsoft Active Directory.
   - **IP/Host**: Enter the IP or host address of the directory.
   - **Port**: Enter the TCP port number for communicating with the directory server. The default port number used for unencrypted communication with the directory server is 389.
   - **Encryption Type**: Select **None** (No encryption), **SSL** (Secured Socket Layer), or **TLS** (Transport Layer Security) as the encryption method for the internet communication protocol used for communicating with the directory server.

- **Auth Type**: Select **None**, **Simple**, **DIGEST-MD5(SASL)**, **CRAM-MD5(SASL)**, or **GSSAPI(Kerberos)** as the authentication method used when establishing a connection with the directory server. After selecting DIGEST-MD5(SASL), CRAM-MD5(SASL), or GSSAPI(Kerberos), fill out the Authentication details field for the chosen Auth Type as follows:

Auth Type	Description
DIGESTMD5(SASL)/ CRAMMD5(SASL)	Enter the following information for configuring the settings for Simple Authentication and security layer (SASL), which is a telnet-based protocol. • **SASL Realm**: Enter the realm value of the SASL server in domain format (e.g., sample.com). • **Quality of Protection**: Select the quality of the data protection from the followings. - **Authentication Only**: Protect data only upon authentication. - **Authentication with integrity**: Ensure integrity of all the data exchanged, as well as authentication. - **Authentication with integrity and privacy**: Ensure integrity of all data exchanges, as well as authentication through data encryption. • **Protection Strength**: Select a data protection level, and determine whether or not mutual authentication should be performed when exchanging data. - **High**: Use 128-bit encryption. - **Medium**: Use 56-bit encryption. - **Low**: Use 40-bit encryption. - **Mutual authentication**: Click the checkbox to ensure data validity by inserting the key into the data exchanged between the client and server.
GSSAPI(Kerberos)	Enter the following information for GSSAPI (Kerberos) authentication. • **Kerberos Credential Configuration**: Select how to obtain a Kerberos ticket. - **Use native TGT**: Select when you already have a ticket issued in EMM. - **Obtain TCT from KDC (provide user name and password)**: Select to issue a new ticket using the default user ID and password. • **Kerberos Configuration**: Select how to configure the Kerberos server. - **Use native system configuration**: Use Kerberos server information defined in the Java properties. - **Use following configuration**: Enter the Kerberos server information manually. - **Kerberos Realm**: Enter the realm of the Kerberos server. - **KDC Host**: Enter the Kerberos key distribution center (KDC) Host or IP address. - **KDC Port**: Enter the KDC Port number.

- **User ID**: Enter the administrator information of the directory server in the following forms:
  - domain/administrator ID,
  - administrator ID @ domain,
  - or CN = administrator ID, CN = Users, DC = domain, and DC = com.
- **Password**: Enter the user ID's password.

6. Click the User, Group, or Organization tab according to your selection in Target in the Preferences tab, and then enter the following information:
   - For more information on the User tab, see Customizing user information.
   - For more information on the Group tab, see Customizing group information.
   - For more information on the Organization tab, see Customizing organization information.
7. Click **Test** to validate the data you entered.
8. Click **Save**.
9. In the "Save Sync Service" window, click **OK**.

Customizing user information

Customize user information on the User tab in the "Add Sync Service" window.

To customize the user information when adding the sync service, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. On the "Sync Service" page, click  .
3. In the "Add Sync Service" window, click the Preferences tab, and then enter the information. For more information, see Adding sync services.

NOTE When entering the information in the "Add Sync Service" window, you must select **User** for the sync service target.

4. Click the User tab, and then enter the following information:
   - **Base DN**: Click  to open the "Select the Base DN" window and select a starting location for searches in the directory server. Entering a Base DN value can reduce the time required to search for data by limiting searches to a specific location.

- **Filter**: Click  to open the "Select Object Class" window and select an Object Class and attributes for the LDAP Syntax string that will be used to filter search results. For more information about setting filters, see Integration Services.
- **Auto Sync**: Click the checkbox next to **Auto Sync** to sync service automatically on the schedule specified in the Auto Sync Setup field in the Preferences tab.
- **Auto Deploy**: Click the checkbox next to **Auto Deploy** to automatically apply the profile to user devices when members of an organization change.
- **Permanent Delete**: Select how to process users who have been deleted from the directory server in EMM.
  - **Keep**: Select to keep the user's data in EMM.
  - **Delete**: Select to clear the user's data from EMM. Deleted users are then added to the list of Sync exceptions. To view this list, navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception** and view **Exception Type** with a value of **Deleted (Source)**.

5. Enter information for mapping the user attributes of the directory server and the user attributes entered when registering user accounts in EMM. The most common values of a directory server are entered automatically, but you can change them according to the directory server.
   - **User ID**: Enter a user ID up to 220 characters.
   - **UPN (User Principal Name)**: Enter the user's login name that will be used for the Windows domain. Enter the UPN in "User's login name@domain_name" format.
   - **DN (Distinguished Name)**: Enter the unique name of the LDAP object.
   - **Object identifier**: Enter the ID used to distinguish the synced user.
   - **Use SecuCamera**: Enter "1" to enable the SecuCamera function or enter "0" to disable it.
   - **Organization Code**: Enter the organization code.
   - **Security Level**: Select a security level for the user.
6. Click **Test** to validate the data you entered.
7. Click **Save**.
8. In the "Save Sync Service" window, click **OK**.

NOTE

- Click  to the right of each item to search for the attributes defined in the directory server.
- Click  to the right of each item to reset the saved values back to the default values.
- Click the checkbox next to **User input value** to delete the default mapped values and to allow you to enter values manually.

Customizing group information

Customize group information on the Group tab in the “Add Sync Service” window.

To customize the group information when adding the sync service, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. On the “Sync Service” page, click +.
3. In the “Add Sync Service” window, click the Preferences tab, and then enter the information. For more information, see Adding sync services.

NOTE When entering the information in the “Add Sync Service” window, you must select the sync service target as **Group**.

4. In the “Add Sync Service” window, click the Group tab, and then enter the following information:
   - **Base DN**: Click 🔍 to open the “Select the Base DN” window and select a starting location for searches on the directory server. Entering a Base DN value can reduce the time required to search for data by limiting searches to a specific location.
   - **Filter**: Click 🔍 to open the “Select Object Class” window and select an Object Class and attributes for the LDAP Syntax string that will be used to filter search results. For more information about setting filters, see Integration Services.
   - **Auto Sync**: Click the checkbox next to **Auto Sync** to sync service automatically on the schedule specified in the Auto Sync Setup field in the Preferences tab.
   - **Sync Group Member**: Click the checkbox next to **Sync Group Member** to sync group members automatically with EMM.
   - **Permanent Delete**: Select how to process groups which have been deleted from the directory server in EMM.
     - **Keep**: Select to keep the group’s data in EMM.
     - **Delete**: Select to clear the group’s data from EMM. Deleted groups are then added to the list of Sync exceptions. To view this list, navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception** and view **Exception Type** with a value of **Deleted (Source)**.
5. Enter information for mapping the group attributes of the directory server and the group attributes entered when registering groups in EMM. The most common values of a directory server are entered automatically, but you can change them according to the directory server.
   - **Organization**: Select the organization to which the group belongs. If left unspecified, the group will not belong to any organization.
   - **DN (Distinguished Name)**: Enter the unique name of the LDAP object.
   - **Object Identifier**: Enter the ID used to distinguish the synced group.

6. Click **Test** to validate the data you entered.
7. Click **Save**.
8. In the “Save Sync Service” window, click **OK**.

NOTE

- Click to the right of each item to search for the attributes defined in the directory server.
- Click to the right of each item to reset the saved values back to the default values.
- Click the checkbox next to **User input value** to delete the default mapped values and to allow you to enter values manually.

Customizing organization information

Customize organization information on the Organization tab in the “Add Sync Service” window.

To customize the organization information when adding the sync service, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. On the “Sync Service” page, click .
3. In the “Add Sync Service” window, click the Preferences tab, and then enter the information. For more information, see Adding sync services.

NOTE When entering the information in the “Add Sync Service” window, you must select the sync service target as **Organization**.

4. In the “Add Sync Service” window, click the Organization tab, and then enter the following information:
   - **Base DN**: Click to open the “Select the Base DN” window and select a starting location for searches on the directory server. Entering a Base DN value can reduce the time required to search for data by limiting searches to a specific location.
   - **Filter**: Click to open the “Select Object Class” window and select an Object Class and attributes for the LDAP Syntax string that will be used to filter search results. For more information about setting filters, see Integration Services.
   - **Auto Sync**: Click the checkbox next to **Auto Sync** to sync service automatically on the schedule specified in the Auto Sync Setup field in the Preferences tab.

- **Permanent Delete**: Select how to process organizations which have been deleted from the directory server in EMM.
  - **Keep**: Select to keep the organization's data in EMM.
  - **Delete**: Select to clear the organization's data from EMM. Deleted organizations are then added to the list of Sync exceptions. To view this list, navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception** and view **Exception Type** with a value of **Deleted (Source)**.

5. Enter information for mapping the organization attributes of the directory server and the organization attributes entered when registering organizations in EMM. The most common values of a directory server are entered automatically, but you can change them according to the directory server.
   - **Upper Organization Code**: Enter the code for an organization in a higher tier than the organization to which the user belongs. It allows synchronizing the organization by maintaining the hierarchical relationships in the organization chart.
6. Click **Test** to validate the data you entered.
7. Click **Save**.
8. In the "Save Sync Service" window, click **OK**.

NOTE

- Click  to the right of each item to search for the attributes defined in the directory server.
- Click  to the right of each item to reset the saved values back to the default values.
- Click the checkbox next to **User input value** to delete the default mapped values and to allow you to enter values manually.

Viewing a list of sync services

After adding sync services, you can view the available sync services in a list.

From the Sync Services list, view the following information of each sync service ID:

NOTE You can manage the Azure AD service linked to EMM on the sync service list. For more information about linking the Azure AD service, see Syncing user information with Azure AD.

- **Target**: Check the target to be retrieved from the directory server.
- **Sync Service ID**: Click to view the preferences, entered users, and organizational and group information of the sync service.
- **Auto Sync**: Click to change the sync status to on or off.
- **Sync Status**: Check the status of the sync service. If the sync service is in progress, “In Progress” appears, and if the sync service is scheduled to sync at a specific time, “Waiting” appears.
- **Start Date**
- **Sync Interval**
- **Last Updated**

From the Sync Services list, click  to synchronize data immediately. For more information, see Running a sync service on demand.

You can also view the detailed sync result of the sync service. Click the empty area next to the sync service ID and click **Sync Result** that will appear at the bottom of the screen. The sync start and end date, the sync result and log messages will appear. If the sync service has a history, click to view the previous sync log. For more information about Sync history, see Viewing sync history.

Running sync services

Synchronization occurs automatically according to the schedule specified. The Sync Interval value can be set while adding a sync service (see Adding sync services). You can also perform on-demand synchronization at any time and can also add additional targets while doing so. The pop-up window that appears when running an on-demand sync service shows the expected number of targets, which helps you determine whether or not to run the synchronization.

Running a sync service automatically

Synchronize data automatically on the schedule specified. When adding or modifying sync services, click the checkbox next to **Auto Sync Setup** in the Preference tab and specify schedules for automatic synchronization. For more details, see Adding sync services.

- The history of the sync service can be viewed in **Advanced** > **AD/LDAP Sync** > **Sync History**.

Running a sync service on demand

Synchronize data on demand at any point in time by choose to synchronize the targets already specified for a service or adding, modifying, or deleting targets as needed.

To run a sync service on demand, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. On the “Sync Service” page, click  .
3. In the “Sync Now” window, select a sync target type and click **OK**.
4. In the “Sync Now” window, select a sync type.
   - **Automatic**: Select to run the sync service with the current sync service settings.
   - **Add Sync Target User/Group/Organization**: Select to add specific targets that are not already specified as targets for the sync service and then click **Next**.
     - Select **Direct select (Recommended)** or **All user in config**, and then click **OK**. When selecting **Direct select (Recommended)**, click the desired target in the “Users/Group/Organization select” window and click **Save**.
   - **Manual**: Select to manually select a Sync method and target, and then click **Next**.
     - **Sync method**: Select **All** to synchronize all information or **Changed only** to synchronize changed information only.
     - **Sync target**: Click the checkbox next to **Add**, **Modify**, or **Delete** users, groups, or organizations in EMM after comparing them with what is stored in the directory server.
5. In the “Expected Sync Results” window, check the expected synced targets and click **OK**.

NOTE Navigate to **Advanced** > **AD/LDAP Sync** > **Sync History** to view the history of the sync service.

Activating or deactivating auto sync services

To activate or deactivate sync services, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Service**.
2. Click ◌ in the Auto Sync column to activate the sync service.
   - Once activated, the sync service will run at the set sync interval.

   Click ○ in the Auto Sync column to deactivate the sync service.
   - Once deactivated, the sync service will not run even at the set sync interval.
3. In the “Change Status” window, click **OK**.

Viewing sync exceptions

Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception** to view all the list of users, organizations and groups that are excluded from the sync service on the “Sync Exception” page.

The sync exceptions list is sorted and managed according to the Exception Type.

- **Deleted (EMM)**: Targets that are deleted manually by the IT admin.
- **Deleted (Source)**: Targets that have been deleted from the directory server and, therefore, also deleted in EMM. This exception applies when you set the **Permanent Delete** option to **Delete** in the User, Group, or Organization tab in the “Add Sync Service” window.
- **Deleted (Synchronized Group)**: Target groups that have been deleted from the directory server and, therefore, also deleted in EMM. This exception applies when you click the checkbox next to **Sync Group Members** in the Group tab in “Add Sync Service” window.
- **Duplicated**: A user, group, or organization with the same ID exists in EMM.
- **Rejected**: A group or organization has been specifically excluded from synchronization in EMM, because the **AD/LDAP Sync** checkbox is not checked in the group and organization information in **Group** or **Organization**.
- **Inappropriate**: Targets whose registered information in the directory server is not appropriate for EMM’s architecture.

Restoring sync exceptions

View exceptions by Exception Type and restore them. When restoring exceptions for a target, synchronization begins immediately. Once synchronized, the target appears in the list of synchronized targets.

To restore a sync exception, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception**.
2. On the "Sync Exception" page, enter a target ID, integration system ID, or sync service ID and click  .
   - **Target ID**: The Sync exception ID, such as user ID, group, ID, or organization name.
   - **Integration System ID**: The base DN of the directory server set for the sync service.
   - **Sync Service ID**: The sync service ID used to distinguish each sync service.
3. Select the checkbox next to the target to be restored and click  . If the target cannot be restored, an error pop-up window appears.
4. In the "Restore" window, click **OK**.

Deleting sync exceptions

Targets that have been removed from the list of Sync exceptions are added to the list of sync targets for the relevant sync service again. They will be synchronized automatically according to the schedule or when you set to synchronize them on demand.

To delete a sync exception, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync Exception**.
2. On the "Sync Exception" page, enter a target ID, integration system ID, or sync service ID and click .
   - **Target ID**: The Sync exception ID such as user ID, group, ID, or organization name.
   - **Integration System ID**: The base DN of the directory server set for the sync service.
   - **Sync Service ID**: The sync service ID used to distinguish each sync service.
3. Click the checkbox next to the target and click  .
4. In the "Delete" window, click **OK**.

Once an exception is deleted, the target is added to the list of sync targets for the relevant sync service again, and will be synced automatically according to the schedule. For more information on running the sync service immediately, see Running a sync service on demand.

Viewing sync history

You can search for a history of previously-run sync services by sync type or period.

NOTE If the **Database Retention Period (Days)** and **Log File Retention Period (Days)** of the **LOG** classification in **Setting** > **Server** > **Configuration** are set, the synchronization history that has passed the storage period will not be searched. For more information, see LOG.

To search for a sync history, complete the following steps:

1. Navigate to **Advanced** > **AD/LDAP Sync** > **Sync History**.
2. On the "Sync History" page, enter a target ID, integration system ID, or sync service ID and click .
3. Click on the left of the relevant service to view additional details. You can view details about Add, Modify, Error, Delete, Ignore User, and Log Messages.

Viewing sync results

Navigate to **User**, **Organization**, or **Group** to view users, organizations, or groups added to EMM after running a sync service.

- **User**: On the "User" page, view the targets set to **AD/LDAP** under **Type**.
- **Organization**: On the "Organization" page, view the targets set to **AD/LDAP** under **Type**.
- **Group**: On the "Group" page, view the targets set to **AD/LDAP** under Type.

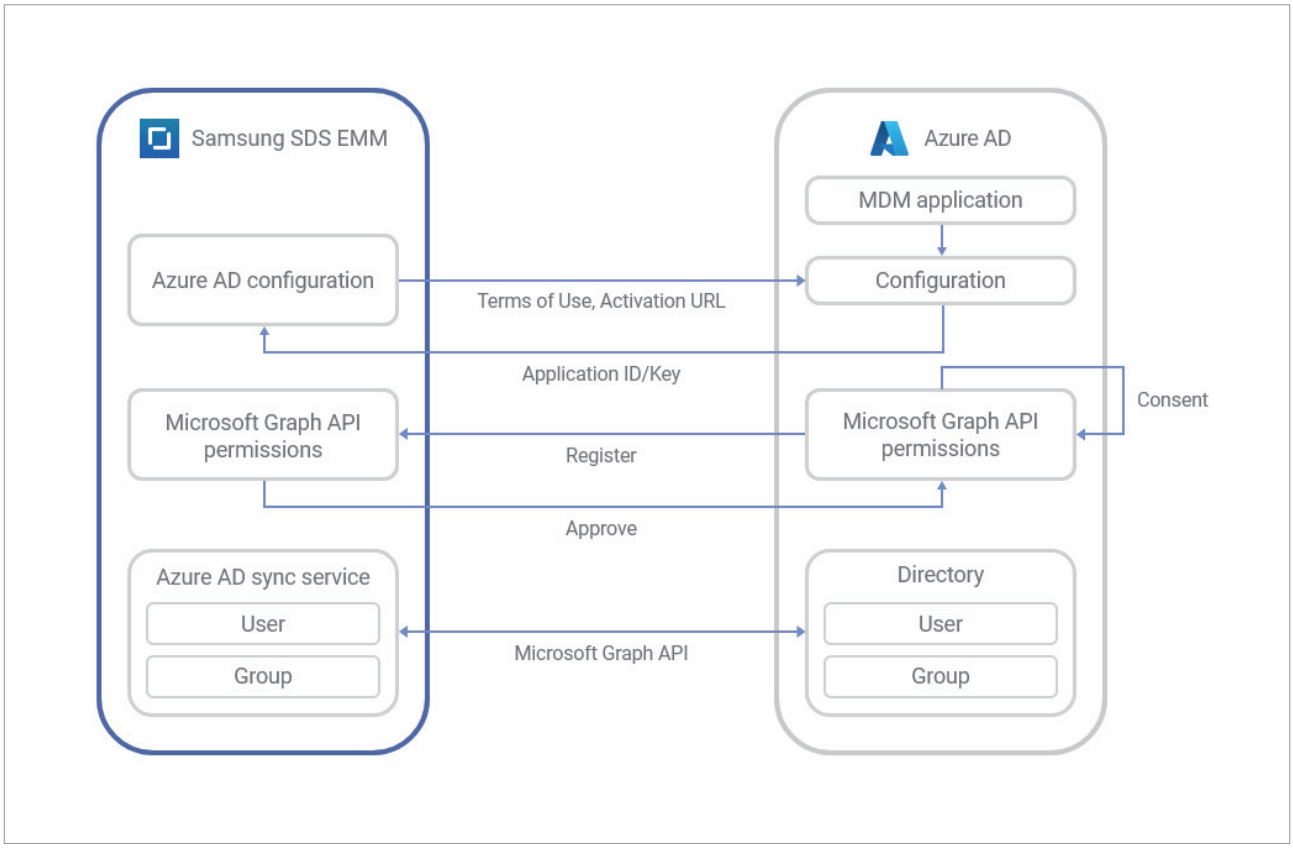
Syncing user information with Azure AD

EMM can be linked to the Microsoft Azure AD service through the Microsoft Graph API. When linking EMM to Microsoft Azure AD through the Microsoft Graph API, AD user accounts and group information will be provided to EMM through the LDAP protocol. Also, you can view the sync service history and user information on the EMM Admin Portal.

NOTE

- The sync service through the EMM and Azure AD connection is supported only for user and group synchronization.
- For more information on Microsoft Graph API, see https://docs.microsoft.com/en-us/azure/active-directory/develop/microsoft-graph-intro.

The following diagram provides the procedure to sync Azure AD with EMM through Microsoft Graph API.



Linking EMM to Azure AD

The procedure to link EMM to Azure AD through the Microsoft Graph API is as follows.

Complete the following tasks on the Azure Active Directory portal and EMM Admin Portal:

1. Add EMM as an MDM application on the Azure Active Directory portal
2. Add the EMM enrollment endpoints
3. Add the EMM redirect URI and allow public client flows
4. Enter the directory ID, application ID, and application key
5. Register the Microsoft Graph API permissions
6. Add Azure AD as a sync service on the EMM Admin Portal

Adding EMM as an MDM application

To add EMM as an MDM application on the Azure Active Directory portal, complete the following steps:

1. Visit the Azure Active Directory portal (https://aad.portal.azure.com/).
2. Navigate to **Azure Active Directory > Mobility (MDM and MAM)**.
3. On the "Mobility (MDM and MAM)" page, click **Add Application** at the top.
4. On the "Add an application" page, click **On-premises MDM application**.
5. On the "On-premises MDM application" page, enter **Samsung SDS EMM** in the "Name" field and click **Add**.

Adding the EMM enrollment endpoints

To add the EMM enrollment endpoints on the Azure Active Directory portal, complete the following steps:

1. Navigate to **Azure Active Directory > Mobility (MDM and MAM)**.
2. On the "Mobility (MDM and MAM)" page, select **Samsung SDS EMM**.
3. On the "Configure" page, enter the following information.
   The information can also be entered by copying the MDM terms of use and discover URL under **Advanced > Azure AD Integration** in the EMM Admin Portal:
   - MDM Terms of Use URL — e.g. https://emm.knoxemm.com:443/emm/termsofuse.do
   - MDM Discover URL — e.g. https://emm.knoxemm.com:443/emm/windows/azure/discovery

4. On the “Configure” page, click **Save** at the top.
5. Click **On-Premises MDM application settings** to navigate to the Samsung SDS EMM application configuration pages.

Adding the EMM redirect URI

To add the EMM redirect URI and allow public client flows on the Azure Active Directory portal, complete the following steps:

1. Navigate to **Azure Active Directory > Mobility (MDM and MAM)**.
2. On the “Mobility (MDM and MAM)” page, select **Samsung SDS EMM**. On the Samsung SDS EMM application configuration page, click **Authentication**.
3. On the “Platform configurations” page, click **Add a platform > Web**.
4. In the “Redirect URIs” field of the “Configure web” page, enter the following information.
   The information can also be entered by copying the Redirect URI under **Advanced > Azure AD Integration** in the EMM Admin Portal:
   - Redirect URI — e.g. https://emm.knoxemm.com:443/emm/permissions/stage/com
5. Enter the Redirect URI. Then, click **Configure** at the bottom of the “Configure web” page to save. You will be returned to the “Platform configurations” page.
6. In the **Advanced Settings > Allow public client flows > Enable the following mobile and desktop flows** of the “Platform configurations” page, click **Yes**.
7. Click **Save** at the top.

Entering the directory ID, application ID, and application key

To register the directory ID, application ID, and application key of the Samsung SDS EMM application on the EMM Admin Portal by copying them from the Azure Active Directory portal, complete the following steps:

1. Navigate to **Azure Active Directory > Mobility (MDM and MAM)**.
2. On the “Mobility (MDM and MAM)” page, select **Samsung SDS EMM**. On the Samsung SDS EMM application configuration page, click **Overview**.
3. Copy the **Directory (tenant ID)** and **Application (client) ID** fields, respectively.
4. On the EMM Admin Portal, navigate to **Advanced > Azure AD Integration**.
5. On the “Azure AD Integration” page, paste the copied IDs into the **Directory ID** and **Application ID** fields in stage 4.

6. Navigate to the Samsung SDS EMM application configuration page on the Azure Active Directory portal. Click **Certificates & secrets > Client secrets > New client secret**.
   A client secret is a password string used to authenticate the ID when an application requests a token. It is also called the application password.

7. On the “Add a client secret” page, enter the following information.
   - Description — Enter a one-line summary for the client secret. (e.g. EMM secret)
   - Expires — Select a lifetime for the client secret. (e.g. 6 months)

8. Click **Add** at the bottom of the “Add a client secret” page.
   The information will be saved and you will be returned to the “Certificates & secrets” page.

9. At the bottom of the “Certificates & secrets” page, copy the client secret.

10. On the EMM Admin Portal, navigate to **Advanced > Azure AD Integration**.

11. On the “Azure AD Integration” page, paste the copied client secret into the **Application Key** field in stage 4, and select the expiry date in the **Application Key Expiration** field.

12. At the bottom of the “Azure AD Integration” page, click **Save**.

Registering the Microsoft Graph API permissions

EMM needs three permissions from the Microsoft Graph API in order to sync the Azure AD information.

Permission type	Permission name	Requires Azure admin consent
Delegate	User.Read	No
Application	Directory.Read.All	Yes
Application	Device.ReadWrite.All	Yes

To grant these permissions to EMM, complete the following steps:

1. On the Azure Active Directory portal, navigate to **Azure Active Directory > Mobility (MDM and MAM)**.

2. On the “Mobility (MDM and MAM)” page, select **Samsung SDS EMM**. On the Samsung SDS EMM application configuration page, click **API permissions**.

3. On the “API permissions” page, click **Add a permission**.

4. On the “Request API permissions” page, click **Microsoft APIs**. Then, from the list of commonly used Microsoft APIs, click **Microsoft Graph API**.

5. Among the Microsoft Graph permissions, click **Delegated permissions** or **Application permissions**. In the "Select permissions" window, search for the permission name. (e.g. Directory. Read.All)

6. Select desired permissions, and click **Add permissions** at the bottom of the "Request API permissions" page.

7. Repeat steps 3-6 for both types of permissions, based on the permissions listed in the preceding table.

8. To grant consent for the API permissions, click **Grant admin consent for tenant name**. In the "Grant admin consent confirmation" window, click **Yes**.

9. When the approval is completed on the Azure Active Directory portal, you can view the approval result on the EMM Admin Portal. If there are permissions that are not approved on the Azure Active Directory portal, you can request the approval on the EMM Admin Portal. You may need to wait 1-5 minutes for the permissions to sync with the EMM Admin Portal.
   a. On the EMM Admin Portal, navigate to **Advanced > Azure AD Integration**.
   b. In the **MS Graph API Permission Setting > Permission List** of the "Azure AD Integration" page, select all the API permissions, then click **Approve**.
   c. In the "Approve" window, click **OK**. You will be moved to the Azure AD administrator approval page.
   d. When the approval is completed, you can view the approval result on the EMM Admin Portal.

Adding Azure AD as a sync service

Once an Azure AD service is linked with EMM, you can add it to the EMM Admin Portal as a sync service to begin syncing user information.

To add Azure AD to the EMM Admin Portal as a sync service, complete the following steps:

1. On the EMM Admin Portal, navigate to **Advanced > Azure AD Integration**.

2. In the **Sync Service Setting** of the "Azure AD Integration" page, click **Add**.

3. Enter **Sync Service Name**, select **Sync Target**, and click **Save & Sync**.
   The added sync service can be viewed under **Advanced > AD/LDAP Sync > Sync Service**.

NOTE You cannot add Azure AD as a sync service under **Advanced > AD/LDAP Sync > Sync Service**.

Managing and viewing the Azure AD sync service

After you add Azure AD to the EMM Admin Portal as a sync service, you can manage the sync service and view its history.

- Navigate to **Advanced > AD/LDAP Sync > Sync Service** and manage the sync services. For more information, see Running sync services.
- Navigate to **Advanced > AD/LDAP Sync > Sync History** and view the sync history. For more information, see Viewing sync history.

4

Device

Device

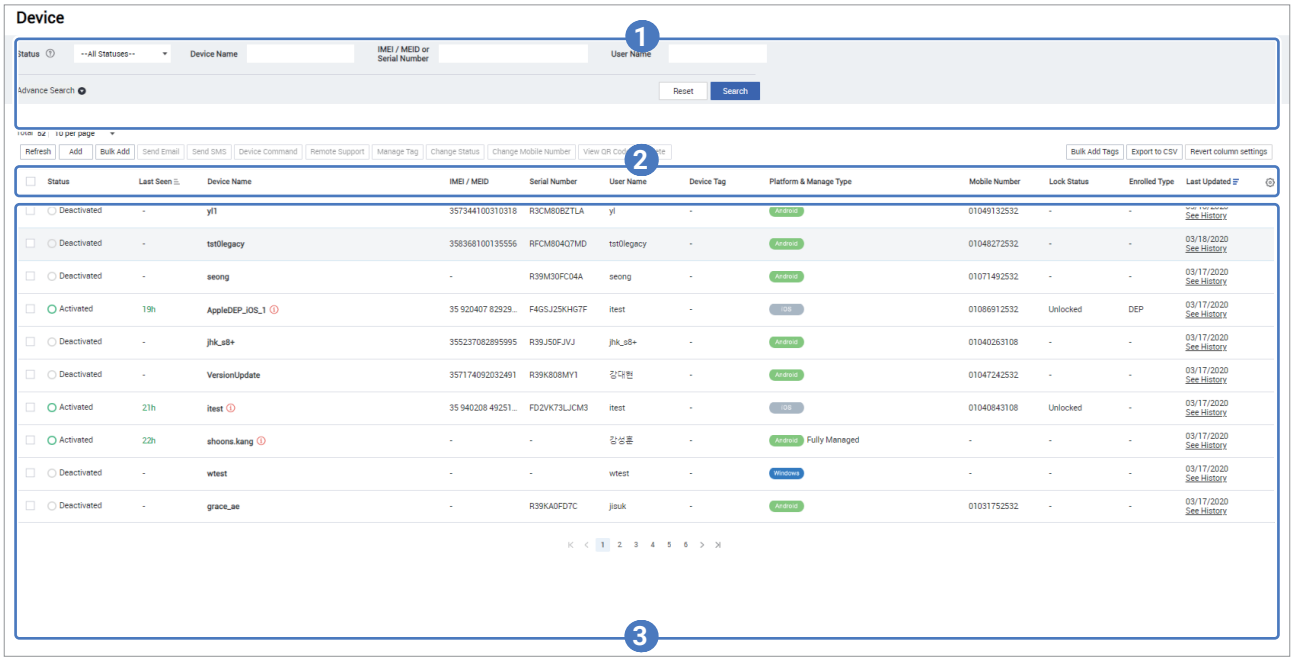
Samsung SDS EMM supports various device platforms, such as Android Legacy, Android Enterprise, iOS, Windows, and Tizen Wearable. Register the devices in the EMM Admin Portal as a single device or in bulk to manage them. When you add the devices, you need to select the user to use the device. If you need to create a new user account, see Creating user accounts.

Samsung SDS EMM also supports the Knox Mobile Enrollment (KME) service for Samsung devices and the Device Enrollment Program (DEP) service for Apple devices. For more information on KME and DEP, see Using Knox Mobile Enrollment (Samsung devices only) and Using the Apple Device Enrollment Program (iOS devices only). You can control the activated devices using device commands and view the detailed information for each activated device.

This chapter explains the following topics:

Viewing the device list

Navigate to **Device** to view all the devices registered in the Admin Portal on the “Device” page. You can also perform specific functions to the selected devices among the list. On the device list, the personalized settings of the columns will be saved. The saved settings will be retained before you delete the web browser’s cookies. You can also return the column settings to their default settings by clicking **Revert Column Settings**.



No.	Name	Description
1	Search field	Search for devices by device name, IMEI / MEID, user name, and status. You can also search for devices by device platform & manage type, enrolled type, issue only, KME ID, Gate Access etc and more by clicking **Advanced Search**. Click **Reset** to reset the search field. • Use KME ID to search KME devices registered individually or collectively in the EMM Admin Portal, and select **KME** as the **enrolled type** to search devices registered in the KME Portal. **NOTE** You can collect and search the respective IMEI/ MEID and mobile phone numbers of devices using Dual SIMs. For non-Samsung Android Legacy devices, only the mobile phone numbers are collected.

No.	Name		Description
2	Function	Refresh	Update the list of devices.
		Add	Add a device to the Admin Portal. For more information, see Adding a single device.
		Bulk Add	Add multiple devices at the same time to the Admin Portal. For more information, see Adding devices in bulk.
		Send Email	Send the “Tizen Wearable Installation” template via email. The email address of the users must be registered to their accounts.
		Send SMS	Send the “Tizen Wearable Installation” template via SMS. The mobile numbers of the users must be registered to their accounts.
		Device Command	Send the device commands to the selected device on the device list. For more information, see Sending device commands to devices.
		Remote Support	Remotely control the selected device with the RS Viewer from your computer. **NOTE** Remote Support is not available for the high security version.
		Manage Tag	Add or delete the tags of the selected devices in order to filter by specific information. Multiple tags can be also added to a device.
		Change Status	Change the device status. Depending on the current status, the available statuses to change may be different. For more information, see Changing the Device Status.

No.	Name		Description
2	Function	Change Mobile Number	Modify the mobile number of the selected device.
		View QR Code	Scan the QR code to activate the device as the Android Enterprise Fully Managed or Work Profile on company-owned type. To set this as the QR code, navigate to **Setting** > **Server** > **Configuration** and configure the QR Code setting. For more information, see Setting the QR code.
		Delete	Delete the selected deactivated devices from the device list.
		Bulk Add Tags	Add bulk device tags using a template.
		Export to CSV	Download a list of all the devices or KME devices as a CSV file.
		Revert Column Settings	Resets the column settings to the default settings.
3	Device list		View the brief information of the registered devices on the list. Information of the devices, such as model number, OS version, and MAC address, Gate Access can be viewed in the added columns. • For devices using Dual SIMs, IMEI/MEID and mobile phone numbers are displayed in two rows in the device list. • The result and application of the Gate Access event is displayed on the Gate Access column as “In” if a device comes in, “Out” if a device goes out, and “-” if the event is not applied.

Viewing the device details

View each device's details by clicking a device name (or tag) to on the device list. For more information about each section of the detail page, see Detail page.

Summary area

The summary area contains the information about the selected device such as device's status, and detailed information.

- **Detail**: View the detailed device's user information. For more information about the "User Detail" page, see Viewing the user details.
- **See History**: View the device history, license type, and license key history.

Tab: Security

The Security tab shows the detailed information about security, such as Lock Device, Password Policy, Compromised OS, and whether SD Card Encryption is set.

- **Detail**: Display additional device information at the bottom of the page.
- You can view the settings for Keepalive, the profile update scheduler, and the location interval.

Tab: Device Information

The Device Information tab shows the device's detailed information, Tag, OS Version, Last Location Scanned and License information. For devices using Dual SIMs, IMEI/MEID and mobile phone numbers are displayed.

- **Detail**: Display additional device information at the bottom of the page.
- Click the detail view next to Last Location Scanned to check the device location path. You can check it on the map only when a value is entered in **Setting** > **Server** > **Configuration** > **Google Maps API Key**. In the "Check Location" pop-up window, you can view the device's route history on a map for up to 30 days. If you click **Export to GPX**, you can download the location information (coordinate) in a GPX file.

Tab: Network

The Network tab shows the device's detailed network status such as Wi-Fi and SIM information.

NOTE Wi-Fi Transfer Data and Network Transfer Data do not appear on Android 10 (Q) devices.

Tab: Application

The Application tab shows the applications installed, assigned or controlled to the selected device. In the Application tab, the following tabs are additionally provided.

Application tab	Description
Installed Application	View the information of the installed applications to the device and Last Sync date. The following function buttons are available: • **Sync Installed App List**: Update the installed application list. • **Install or Update**: Select the application to install on the device or to update if it is already installed. • **Export to CSV**: Download a list of applications as a CSV file.
Assigned Application	View the information of the assigned applications to the device. • **See Setting**: Displays the Install Area, Install Type, whether to use Auto-run after Install, and the Use Deployment Scheduler of the applications.
Controlled Application	View the information of the applications that are controlled by specific policies, such as White/Black-listed apps or Battery Optimization Exception apps.

Tab: EMM Application

The EMM Application tab shows the policies applied to EMM applications on the device. The EMM Client policy also can be seen.

Tab: Profile

The Profile tab shows the detailed information on the profile and policies assigned to the selected device.

Tab: Content

The Content tab shows File Type, File size, Download Type, Last Assigned, and Download Date for the content assigned and deployed to the device.

Tab: Group / Organization

The Group / Organization tab shows the detailed information on the groups and organizations that the selected device belongs to.

- **Detail** (Group): Move to the “Group Detail” page for the selected group. For more information on the “Group Detail” page, see Viewing the group details.
- **Detail** (Organization): Move to the “Organization Detail” page for the selected organization. For more information on the “Organization Detail” page, see Viewing the organization details.

Tab: Command History

The Command History tab shows the history of device commands sent to the selected device. You can also view the detailed information on the audit events for each device command.

- **See Audit Event**: View in detail the audit events that occurred while completing a device command.

The following function buttons are available:

Function button	Description
Device Log	Download the device logs.
Re-Request	Re-request the requested device command on the list.

Function buttons in the footer

You can perform specific functions to the devices using the function buttons in the footer.

The following function buttons are available:

Adding devices to the Admin Portal

You should add devices to the Admin Portal before activating devices. You can add devices individually or in bulk.

Adding a single device

To add a single device to the Admin Portal, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click **Add**.
3. On the “Add Device” page, enter the following device information:
   - **Device Name**: Enter a device name.
   - **User**: Click **Select** and select a user on the list for the device.
   - **KME**: Select **Use** and enter the **KME ID**, if you want to register KME devices in the EMM Admin Portal.

     NOTE If you have registered KME devices in the EMM Admin Portal, you need to enter the device name in the Mobile ID when logging in to EMM. If you want to log in to EMM without entering the Mobile ID, register the device in the KME Portal. For more information about registering your device in the KME Portal, see Using Knox Mobile Enrollment (Samsung devices only).

   - **Platform**: Select the device’s platform type among **Android**, **iOS**, **Windows**, or **Tizen Wearable**.
   - **Mobile Number**: Enter the mobile phone number of a Tizen device.
   - **Type**: Select the device activation type between **BYOD** (Bring Your Own Device) or **COPE** (Company Owned Personally Enabled).
4. Click **Save**.

Adding devices in bulk

To register multiple devices at the same time to the Admin Portal, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click **Bulk Add**.
3. To register multiple devices at the same time in the “Bulk Add Devices” window, select **Bulk Add**. To register multiple KME devices at the same time, select **KME**.

> **NOTE** If you have registered KME devices in the EMM Admin Portal, you need to enter the device name in the Mobile ID when logging in to EMM. If you want to log in to EMM without entering the Mobile ID, register the device in the KME Portal. For more information about registering your device in the KME Portal, see Using Knox Mobile Enrollment (Samsung devices only).

5. Download the template of the device type to be registered, and enter the device information.
6. Click  , and then select the complete Excel file template filled with the device information.
7. Click **Save**.

Activating devices

After registering devices to the Admin Portal, the devices can be activated differently depending on the device platform. Also, users must install the following application delivered by the IT admin.

NOTE

- When you want to activate the device which has been activated, the device must be deactivated in advance and try the activation process. When you try a device reset or an activation with the same mobile name/user ID with the device which is not deactivated properly, the device status changes to Blocked by System.
- To use a multi-license, EMM Agent 2.3.5 version must be installed on the device. For more information, see Managing licenses.

- Android: EMM Agent
  - Users can also download the application from a public app store directly. Go to the Google Play Store and install **Samsung SDS EMM**.
  - Users who want to use Samsung SDS Push instead of the Google Push service should install the Push Agent delivered by the IT admin.
  - The Users who want to use or have already installed a version which separates the EMM Client from the EMM Agent should also install the EMM Client delivered by the IT admin.

NOTE

- In the version earlier than EMM v2.4.1, Samsung SDS Push is not available on Android Enterprise devices with the Work Profile type. For more information about Activating Android Enterprise, see Activating Android Enterprise (AE) devices.
- Starting from Android 13, the following have been changed regarding an agreement of the EMM application permission.
  - The user is optionally required for the location, camera, and SMS permission.
  - After device activation, the user is required to select permissions according to the policy set by the administrator (location policy in the profile, SMS Permission Control in Configuration).
  - The user must agree to the notification permission of the EMM application when activating the Android Legacy device.

- iOS and Windows: EMM Client
- Tizen Wearable: Wearable EMM

Activating general devices (Android Legacy, iOS and Windows)

Activate general devices to control them remotely. Users who want to use the Samsung SDS EMM on general devices must install the Samsung SDS EMM and log in with their user account. Then all profiles and applications assigned will be applied immediately.

NOTE

- Before activating devices, a user account must be created to log in to EMM. For more information on creating user accounts, see Creating user accounts.
- You need to register the EMM Extension app as an internal application to install the XAPK installation app. You need to install the XAPK installation app via the EMM Extension app, so install the EMM Extension app on devices first and acquire app permission.
- If you install an application from a XAPK installation app on Android Legacy 6.0 or higher devices, there are the following restrictions depending on the file type.
  - OBB (Android Opaque Binary Blob) file: A notification will appear for permission request during initial installation. After acquiring permission, the notification will not appear.
  - Splits file: A notification for permission request and a pop-up window whether to install the application will appear during initial installation. After acquiring permission, only the pop-up window will appear.
- For iOS devices, when the enrollment type and the type of the actually enrolled device do not match, you can view the unavailable devices on the device list by selecting **Incorrectly Activated** in the **Issue Only** field. Incorrect activation includes the following.
  - 1) When devices are activated as DEP devices in the Admin Portal but unassigned in the ABM portal
  - 2) When devices are activated as DEP devices in the Admin Portal but unassigned, factory-reset, and reactivated as general devices in EMM
  - 3) When general devices that have not been enrolled as DEP devices are activated as DEP devices

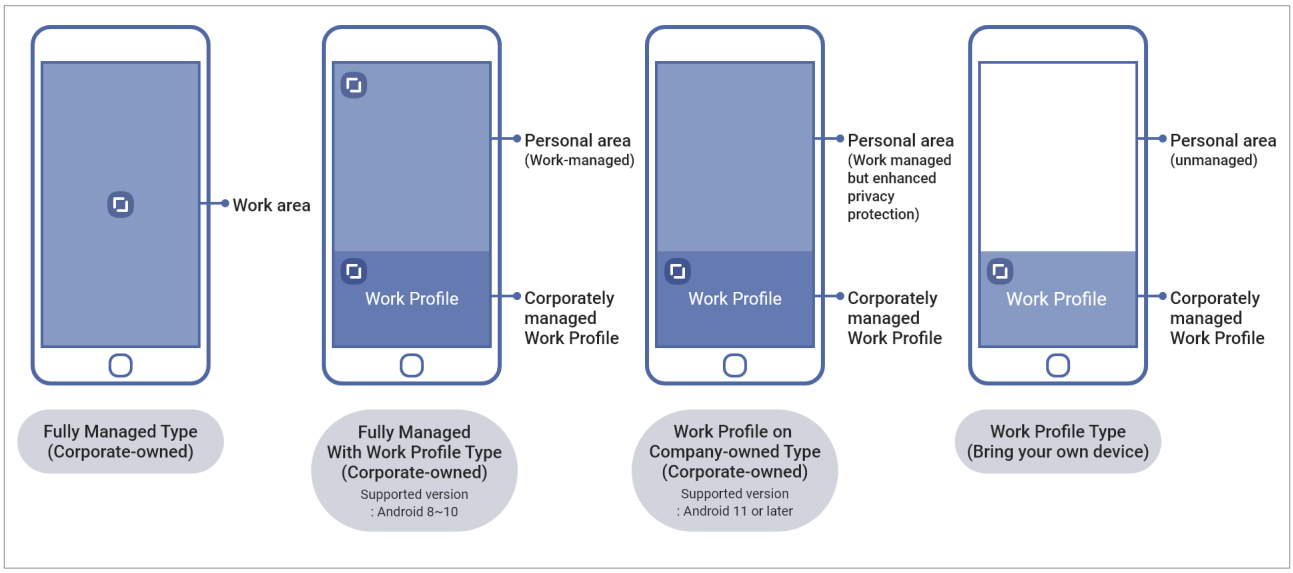
To activate general devices, complete the following steps:

1. Install the Samsung SDS EMM Agent delivered by the IT admin and launch it on the device.
   - For Android Legacy devices, users can directly download the application from the Google Play store. Search for **Samsung SDS EMM**.
2. On the log in screen, enter a user ID and password to sign in to EMM. If you log in to EMM successfully, the profiles, policies, and applications will be applied to the device. If an Android Legacy with Knox Workspace profile is applied, Knox Workspace will be automatically installed.
   - After registering the Dual DAR license in the EMM Admin Portal, set Dual DAR policies on Android Legacy devices deploy the profile. Knox Workspace (Dual DAR) will be automatically installed.

NOTE For Android Legacy with Knox Workspace devices running Android 10 (Q) or higher, tap the activation notification on the status bar to install the Knox Workspace manually.

Activating Android Enterprise (AE) devices

Samsung SDS EMM supports the following Android Enterprise (AE) manage types. Each manage type can be Activated differently.



- **Fully Managed type**: This type allows you to control the whole corporate owned device using EMM. To activate as a Fully Managed type, the device must be factory reset.
- **Fully Managed with Work Profile type**: This type, a combination of the Fully Managed and Work Profile types, allows you to control corporate owned devices. The Fully Managed with Work Profile type is supported on devices running Android 10 (Q) or lower. You can manage the device's personal area by sending device commands while controlling business applications and data within the separate Work Profile. Users can install and use personal applications on their device's personal area, and, in this case, EMM cannot control applications installed in the personal area or their data.
- **Work Profile on company-owned type**: This type, a combination of the Fully Managed and Work Profile types, allows you to control corporate owned devices with more enhanced privacy protection contrary to Fully Managed with Work Profile type. This Work Profile on company-owned type is supported on devices running Android 11 or higher. You can manage the device's personal area by sending device commands while controlling business applications and data within the separate Work Profile. Users can install and use personal applications on their device's personal area, and, in this case, EMM cannot control applications installed in the personal area or their data. Devices can be activated in the Work Profile on company-owned type only when you set "Work Profile on company-owned" when creating user accounts or adding an organization.

NOTE

- Devices that the administrator set to use the Dual DAR in Creating user accounts or Adding an organization after registering Dual DAR license in the EMM Admin Portal are activated as Fully Managed Dual DAR or Work Profile on company-owned Dual DAR.
- On Work Profile on company-owned devices, the device users cannot install the Google Play Store within the personal area. Also, the IT admin cannot add third party applications to the Application execution blacklist except system applications.
- You need to register the EMM Extension app as an internal application to install the XAPK installation app. You need to install the XAPK installation app via the EMM Extension app, so install the EMM Extension app on devices first and acquire app permission.
- If you install an application of a XAPK installation app on Android Enterprise devices, there are the following restrictions depending on the file type of applications and the management type of devices.
  1) Work Profile on company-owned and Work Profile devices
     - OBB (Android Opaque Binary Blob) file: A notification will appear for permission request during initial installation. After acquiring permission, the notification will not appear.
     - Splits file: A notification for permission request and a pop-up window whether to install the application will appear during initial installation. After acquiring permission, only the pop-up window will appear.
  2) Fully Managed and Fully Managed with Work Profile devices
     - OBB (Android Opaque Binary Blob) file: A notification will appear for permission request during initial installation. After acquiring permission, the notification will not appear.
     - Splits file: The application will be automatically installed.

- **Work Profile type**: This type allows you to control personal devices (BYOD). In this case, EMM only manages the Work Profile, which is the work area separated from the personal area, on the device.

For the Fully Managed type

Activate Android Enterprise (AE) devices as the Fully Managed type to control the whole area of the device. The device should be factory reset in advance. Select one of the following methods.

Method	Supported version
Using a token For more information, see Using a token.	Android 6.0 (Marshmallow) or higher
Using a QR code For more information, see Using a QR code.	Android 7.0 (Nougat) or higher
Using NFC For more information, see Using NFC.	Android 6.0 (Marshmallow) or higher

Installing CA certificates

You can install CA certificates on user devices for EMM server access on an EMM server operated on a closed network. You can only install CA certificates if you set **Pre-Installation** in the EMM Admin Portal.

You can install CA certificates before activating user devices. The installable device types and how to log in are as follows:

- Device types: Fully Managed or Work Profile on company-owned for Android Enterprise devices
- How to log in: Using the token, QR code

To pre-install CA certificates, complete the following steps:

1. Select how to install the certificates on the “Pre-Installation” screen.
    - **URL Address**: Enter the URL to download the CA certificates including http(s).
        - Access the web server with the HTTP protocol that does not require certificates or download the certificate by accessing the web server that requires certificates.
    - **USB**: Select the USB drive in the device explorer and select the CA certificate (.cer, .crt, .der) you want to install.
2. Tap **Install**. The CA certificate will be installed on the device.
    - Installed CA certificates will be stored in the EMM Agent Sandbox of the device.
3. Check the list of certificates that are installed on the device on the “Pre-Installation” screen.
    - Tap **Details** next to the certificate name and view the certificate details in the “Certificate Detail” window. You can also tap **UNINSTALL** to delete the certificate from your device.
4. Tap **<** (Back) on the “Pre-Installation” screen to move to a screen where you can enter the server information and Tenant ID. Tap Log in to activate your device.

Using a token

Enter the token (afw#SDSEMM) to activate the Android Enterprise (AE) devices as the Fully Managed or Fully Manage with Work Profile type. If the token is applied successfully, the Samsung SDS EMM Agent will be automatically installed on the device.

To activate using a token, complete the following steps:

1. Turn on the factory reset device, and then on the device screen, tap **START**.
2. On the “Connect to Wi-Fi” screen, select an available Wi-Fi network, and then tap **NEXT**.
3. On the “Agree to Terms and Conditions” screen, read the terms and conditions, and then tap the checkbox next to **“I have read and agree to all of the above”.** Then, tap **Agree**. The device will check for updates and the updated will be applied.

4. On the “Sign in” screen, enter “afw#SDSEMM” in the email or phone field, and then tap **Next**.
5. On the “Android Enterprise” screen, tap **Install** to download the Samsung SDS EMM Agent on the device. The Samsung SDS EMM Agent will be downloaded and launched automatically.
6. On the “Set up your device” screen of the Samsung SDS EMM Agent, read the privacy policy of EMM and Google, and then tap **Accept & continue**.
7. On “Sign in with your EMM Account” screen, tap **Pre-Installation** at the bottom to pre-install CA certificates on devices. For more information, see Installing CA certificates. Move to step 8 if you do not install certificates.
8. On the “Sign in with your EMM Account” screen, enter a user ID and password, and then tap **SIGN IN** to sign in to EMM. Depending on the profiles applied to the device, the device will be activated as the Fully Managed or Fully Managed with Work Profile type.

Using a QR code

Use a QR code to activate the devices as the Fully Managed, Fully Managed with Work Profile or Work Profile on company-owned type.

To activate using a QR code, complete the following steps:

1. Turn on the factory reset device, and then, on the welcome screen, tap the screen six times to launch QR code activation. The QR Reader app will be downloaded and the device camera will launch to scan the QR code automatically.
2. On the “Connect to Wi-Fi” screen, select an available Wi-Fi network, and then tap **NEXT**.
3. Select one of the two methods below and activate devices via QR code.
   - Send a QR code via email. For more information on sending a QR code, see Sending templates or user notifications to users via email.
   - On the Admin Portal, navigate to **Device**, click the checkbox next to the device you want to activate, and then click **View QR Code** to display the QR code.
4. Put the QR code in the square on the “Activate via QR Code” screen. The EMM URL and tenant information included in the QR code will be detected.
   - If the administrator sets to install CA certificates on the EMM Admin Portal, the “Pre-Installation” screen will appear automatically when users scan a QR code. For more information, see Installing CA certificates.
5. Tap Log in to activate your device.
6. On the “Agree to Terms and Conditions” screen, read the terms and conditions, and then tap the checkbox next to **“I have read and agree to all of the above.”** Then, tap **Agree**.

7. On the “Sign in with your EMM Account” screen, enter a user ID and password, and then tap **SIGN IN** to sign in to EMM. Depending on the profiles applied to the device, the device will be activated as the Fully Managed, Fully Managed with Work Profile or Work Profile on company-owned type.

Using NFC

You can activate multiple Android Enterprise devices through one parent device to activate them as the Fully Managed Device type. To activate devices using NFC, you need a parent device with the EMM Connect application installed.

To activate devices using NFC, complete the following steps:

1. Install the EMM Connect app on the parent device, and then launch the EMM Connect app.
2. On the activation and settings screen, enter the following information.
   - **Server Address**: Enter the EMM server address.
   - **Corporate Domain**: Enter the Tenant ID. The single tenant users do not need to enter the information.
   - **User ID**: Enter the EMM user ID.
   - **Mobile ID**: Enter the device ID that needs to log in.
   - **Password**: Enter the EMM user password. Once the user ID, mobile ID, and password have been entered, you can log in to EMM on the child devices automatically without an additional authentication process. If you activate the devices without the password, then the users need to enter the password on the login screen later.
   - **APK Download URL**: Enter the Samsung SDS EMM Agent download URL address.
   - **Time Zone**: Set the time zone for the devices being activated.
   - **Language**: Set the language for the devices being activated.
   - **Wi-Fi**: Enter the Wi-Fi network details. To activate the child devices using the EMM Connect application, you need to connect them to a Wi-Fi network.
   - **Encrypt Device**: Tap the checkbox to encrypt the child devices that have not been encrypted.
   - **Disable System Apps**: Tap the checkbox to disable the system applications on the device. Once activated as the Fully Managed Device type, only some of the preloaded applications are visible on the devices. If you disable this option, all preloaded applications will be visible to the users.
3. When the NFC standby screen appears on the device, perform an NFC bump between the factory reset child device and the parent device. It will send a provision request.
   - To activate multiple child devices, enter the user ID, mobile ID, and password again, and proceed with stage 2 with the other information retained.

4. When you hear a notification sound, tap the parent device's screen.

NOTE After performing an NFC bump, the "Cannot create work profile" error message will appear. Reconnect the child devices to a Wi-Fi network, check the time setting on the devices, and then try again.

5. Accept the User Agreement on each child device. Then, the devices will be automatically activated as the Fully Managed Device type and logged in to the EMM. If you did not enter the EMM password during the activation process, the login screen will appear.

For the Fully Managed with Work Profile type

Activate the Android Enterprise (AE) devices as the Fully Managed with Work Profile type to control the separate work and personal areas. The activation methods are the same as those for the Fully Managed type, but the applied profile should be set as **Create Work Profile on Fully Managed**. For more information, see Creating a new profile.

NOTE

- For devices running Android 10 (Q) or higher, tap the activation notification on the status bar to install the Work Profile manually.
- The Fully Managed with Work Profile type is supported on devices running Android 10 or lower. If the OS version of a Fully Managed with Work Profile device is upgraded to Android 11, the device will be automatically switched to the Work Profile on company-owned type. In this case, the EMM agent in the personal area will be deleted. Profile policies will be applied immediately in the personal and work area of Work Profile on company-owned devices, and you can send device commands.

Method	Supported version
Using a token For more information, see Using a token.	Android 6.0 (Marshmallow) or higher
Using a QR code For more information see Using a QR code.	Android 7.0 (Nougat) or higher
Using NFC For more information, see Using NFC.	Android 6.0 (Marshmallow) or higher

For Work Profile on company-owned type

You can control the work apps and data in the Work Profile area using device commands and policies by activating Android Enterprise (AE) devices as a Work Profile on company-owned type. This type is similar to the Fully Managed with Work Profile type but, is enhanced in aspect of privacy protection on personal area. Supported on devices running Android 11 or higher. To activate devices as a Work Profile on company-owned type, set the Android management type as “Work Profile on company-owned” when creating user accounts or adding organizations, and add devices as COPE (Company Owned Personally Enabled). For more information about the Work Profile on company-owned type, see Creating user accounts, Adding an organization, Adding a single device, and Creating a new profile.

NOTE

- For devices running Android 11 or higher, the Work Profile is automatically installed.
- Starting with Android 11, location permission for EMM app requires device users to select **Allow all the time** directly from the **Device Settings** not from the prompt on the enrollment step.
- If the Android management type set when creating user accounts and the device activation type are different, you can view the devices on the device list by selecting **Incorrectly Activated** in the **Issue Only** field.

Method	Supported version
Using a QR code For more information see Using a QR code.	Android 11 or higher

For the Work Profile type

To activate devices as the Work Profile type, install the Samsung SDS EMM Agent on the device.

To activate AE devices as the Work Profile type, complete the following steps:

1. Search for **Samsung SDS EMM** from the Google Play Store and download it on the device.
2. Install the Samsung SDS EMM Agent, and then launch the Samsung SDS EMM Agent on the device.
3. On the “Sign in with your EMM Account” screen, enter a user ID and password, and then tap **SIGN IN** to sign in to EMM.

NOTE For devices running Android 10 (Q) or higher, tap the activation notification on the status bar to install the Work Profile manually.

4. On the “Set up a work profile” screen, read the privacy policy of EMM, and then tap **Agree**. The work applications with the briefcase badge icons, which can be managed by EMM, will appear on the device.

Activating Tizen wearable devices

To activate Tizen Wearable devices, users must install the Wearable EMM application on their wearable devices and log in to the Wearable EMM app. When a user logs in to the Wearable EMM app successfully, the wearable device will be activated and the assigned policies and applications will be applied to the device. If you register an auto installation application, it will be installed automatically when a user logs in.

Sending installation information to wearable devices

To activate a Tizen Wearable device, you must send installation information to the device via SMS or email. The following installation information should be sent to a Tizen Wearable device:

- URL for EMM installation
- EMM/TMS service URL for EMM activation
- Device information, such as User ID, mobile ID, and tenant ID
- User authentication code and URL for generating authentication codes

Use the templates when sending installation information to devices. When sending information via SMS, use the Tizen Wearable information, Tizen Wearable installation, and Tizen Wearable code templates. You can find these templates in **Setting** > **Message Template**. For more information about the message templates, see Modifying message templates.

The Tizen Wearable user authentication code is automatically generated when registering a device. You can regenerate the authentication code when sending the installation information to a device via email or SMS. Also, users can receive an authentication code directly by accessing the authentication code generation URL. For more information, see the Samsung SDS EMM User's Guide.

Specify the configuration details for the Tizen Wearable device in Tizen Wearable classification in **Setting** > **Server** > **Configuration**. You can send the authentication code to an individual device or to multiple devices. If multiple devices are selected, the authentication code is sent only to available devices, and devices that fail to receive the code are reported in the audit log.

To send installation information to a Tizen Wearable device, complete the following steps:

1. Navigate to **Device**.
2. Click the checkbox next to the Tizen Wearable devices you want to activate, and then click **Send Email** or **Send SMS** to send installation information via email or SMS.
3. In the "Send email" or "Send SMS" window, select Tizen Wearable Installation template.
4. Click **OK**.

Installing and running the Wearable EMM application

To install and run the Wearable EMM application for device activation, complete the following steps:

1. Install the Wearable EMM application from the Tizen Wearable Installation URL sent via email or SMS from the Admin Portal.
2. Tap the EMM icon on the wearable device to run the Wearable EMM application, or register the EMM widget and tap the widget.
3. Select one of the following URL types for the connection and tap **NEXT**.
   - **Automatic input**: The Admin Portal sends the installation information to the wearable device via SMS. The received information is extracted and the EMM server address is automatically entered.
     - On the wearable device, check for the automatic input of the EMM/TMS service URL and click **Next** to log in to the Wearable EMM.
   - **Manual input**: If the SMS message is not received, check the information received via another method, such as email, and manually enter the server URL.
     - After selecting the service URL type, enter only the detailed address after the "/" symbol, or select **Manual** and enter the full URL address. e.g.) If the URL is https://bit.ly/2KPlQmS, select the URL type as **bit.ly**, and enter "2KPlQmS" in the URL info field.

NOTE New goo.gl short URLs cannot be created because Google has discontinued the service. Thus, only existing users can use the shortened URLs that already exist. If you have a goo.gl short URL, then select "goo.gl" as the **Service URL Type**, enter the relevant goo.gl URL, and then access it.

4. Enter the 8-digit authentication code received from the IT admin and tap **LOG IN**.
5. Read the End User License Agreement and tap ☑.
6. On the Licensing Guide page, scroll to the bottom, select **Agree**, and then tap **OK**.
   - During the license authentication process, the Wearable EMM app will automatically register the Samsung SDS Push service and communicate with a device to receive profiles and policies.

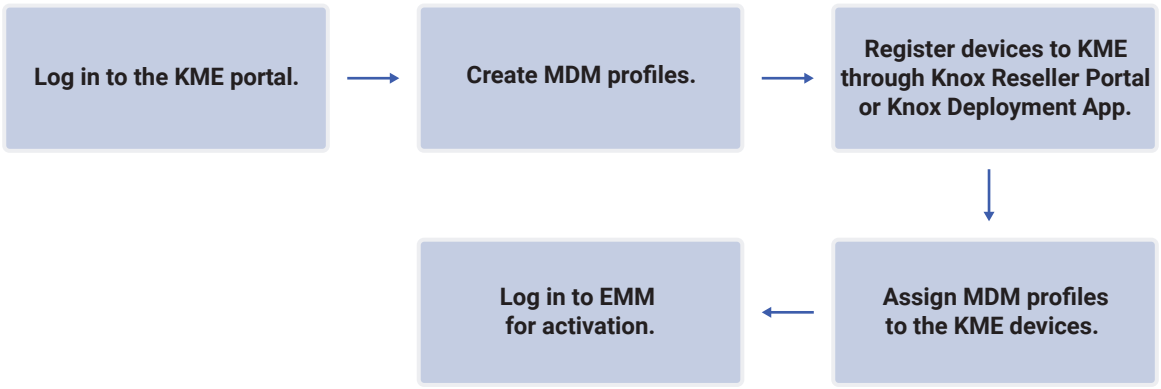
Using Knox Mobile Enrollment (Samsung devices only)

Samsung Knox Mobile Enrollment (KME) allows you to quickly and easily activate a large number of corporate-owned Samsung devices. The devices are automatically activated when users connect to the internet and log in to EMM. Even if you reset the devices activated by the KME service, the Samsung SDS EMM Agent is re-installed automatically and the devices are re-activated in to EMM. For more information about activating KME devices as general devices, see Deactivating KME devices.

KME provides the following advantages:

- Activate a large number of devices in bulk without having to manually activate each device.
- Allow the KME devices to automatically install the Samsung SDS EMM Agent when the KME devices are reset.

To activate devices using KME, the following procedures must be performed.



NOTE For more information about KME, refer to the KME Admin Guide (https://docs.samsungknox.com/KME-Getting-Started/Content/about-kme.htm).

Before using Knox Mobile Enrollment

To use Knox Mobile Enrollment (KME) properly, the followings must be prepared:

- See the list of available countries at the Samsung Knox website and check if KME is available in your country.
- Prepare a device from the following carrier or reseller to use KME:
  - A distributor approved by KME
  - A dealer sharing IMEI or serial numbers directly with the Samsung representative
- Make sure the devices are Samsung devices with Knox 2.4 or higher.
- Sign up for an account in the Samsung Knox Web Portal.
- To install the Samsung SDS EMM Agent, devices must have more than 50% of their battery charged.
- Before activating devices using Android Enterprise's Fully Managed Device, make sure the devices are running on Samsung S8 and Android 5.0 (Lollipop) or above. For more information about Android Enterprise, visit the Android website at https://www.android.com/enterprise/.

Logging in to the Knox Mobile Enrollment Portal

To use Knox Mobile Enrollment (KME), you should log in to the Knox Mobile Enrollment Portal.

To log in to the Knox Mobile Enrollment Portal, complete the following steps:

1. Visit the Knox Portal at https://www.samsungknox.com, and click **Sign in** in the upper right-corner of the screen.
2. Enter a Samsung account ID and password, and then click **SIGN IN**.
3. On the main Knox Portal page, navigate to **SOLUTIONS** > **Knox Mobile Enrollment**.
4. On the Knox Mobile Enrollment page, click **Get Started**.
5. Enter a work email address and click **APPLY FOR FREE**. If the application is approved, you will receive a welcome email with instructions on Knox Mobile Enrollment (KME).
6. On the My Knox solutions page, click **LAUNCH CONSOLE** on **Knox Mobile Enrollment**.

Creating MDM profiles

Before activating devices, create MDM profiles for Android (Legacy) and Android Enterprise through the Knox Mobile Enrollment Portal.

Samsung SDS EMM supports two types of KME activations for MDM profiles.

Profile type	Targeted device	Description
Device Admin	Android Legacy	MDM profile for Android Legacy devices
Device Owner	Android Enterprise	MDM Profile for Android Enterprise's fully managed devices

Creating MDM profiles for Android Legacy devices

To create MDM profiles for the Device Admin profile type, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **MDM Profiles**.
2. In the upper-right corner of the "MDM Profiles" page, click **CREATE PROFILE**.
3. On the "Select profile type" page, click **DEVICE ADMIN**.
4. On the "Device Admin profile details" page, enter the following basic information
   - **Profile Name**: Enter an appropriate profile name to distinguish it from others with similar attributes. Special characters are not permitted.
   - **Description**: Enter a profile description (200 characters maximum) to further differentiate this profile from others.
   - **MDM Server URI**: Enter the EMM server address.

     NOTE Once you have created an MDM profile, you cannot change the MDM server URI.

   - **Server URI is not required for my MDM**: Select this option if you either do not need to point to the MDM's enterprise installation or are unable due to connection restraints.
5. Click **CONTINUE**.
6. On the "Device Admin profile settings" page, set the following MDM configuration settings.
   - **MDM Agent APK**: Click **ADD MDM APPS** and enter the SDS EMM APK link for the Samsung SDS EMM Agent, and then click **SAVE**. The application will be automatically installed on the device when it connects to the internet.

NOTE For wearable devices, add Deep Link for the MDM application registered in the Tizen store.

- **Custom JSON Data (as defined by MDM)**: In the **Custom JSON data** field, enter data in the following JSON format: For more information about JSON, see http://json.org.
  - Enter the tenant information including the **TenantId** and **TenantType** in the java script object notation (JSON) format, as in `{"TenantId":"YOUR_TENANT", "TenantType":"M"}`. **TenantId** refers to the name of your EMM company account. It occurs after @ in your EMM Username. For example, if your login ID for EMM is sample@samsung.com, enter as follows:
    - Multi-Tenant: `{"TenantId":"samsung.com","TenantType":"M"}`
    - Single-Tenant: `{"TenantId":"EMM","TenantType":"S"}`

7. On the "Device Admin profile settings" page, set the following device settings.
   - **Enrollment settings**: Select the additional activation setting options.

     NOTE The Skip Setup Wizard option performs independently from the Allow device user to cancel activation, and both options can be enabled at the same time.

     - **Skip Setup Wizard**: Skips the setup wizard screen and allows you to start the activation process much faster.

       NOTE This option is not currently available on all AT&T devices.

     - **Allow the end user to cancel enrollment**: Permits device user to cancel activation on their devices.
   - **Privacy Policy, EULAs and Terms of Service**: Click **Samsung Knox Privacy Policy** to view the specific privacy policy text displayed to device users based on their geographic region.
   - **ADD LEGAL AGREEMENT**: Enter the agreement title and agreement text.
   - **Support contact details**: View the support contact details.
   - **EDIT**: Update the company name, company address, support phone number, and support email address displayed on the devices after successful activation. If required, click **Save as default support contact details** to use this same information as the default contact information.

     NOTE If the device owner (DO) support is enabled for the profile, then only the client name is editable, and the remaining fields are inactive.

   - **Associate a Knox license with this profile**: Pass the Knox license key directly to the intended device for easier Knox profile configuration.

8. Click **CREATE**. To view the created MDM profile, navigate to **MDM Profiles** on the Knox Mobile Enrollment Portal.

Creating MDM profiles for Android Enterprise devices

To create MDM profiles for the Device Owner profile type, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **Profiles**.
2. In the upper-right corner of the “Profiles” page, click **CREATE PROFILE**.
3. On the “Select profile type” page, click **ANDROID ENTERPRISE**.
   Register as Device Owner (DO) or set MDM to select either Device Owner (DO) or Profile Owner (PO).
4. On the “Android enterprise profile details” page, enter the following basic information for the device owner profile.
   - **Profile Name**: Enter an appropriate profile name to distinguish it from others with similar attributes. Special characters are not permitted.
   - **Description**: Enter a profile description (200 characters maximum) to further differentiate this profile from others.
5. On the “Android enterprise profile details” page, enter the following MDM information for the device owner profile.
   - Set MDM to register devices by selecting either Device Owner (DO) or Profile Owner (PO), or select to start compulsory creation as Device Owner (DO; Fully Managed).
   - **Pick your MDM**: Select **Samsung SDS EMM**.
   - **MDM Agent APK**: Enter the link where users can download the Samsung SDS EMM Agent. The application will be automatically installed on the device when it is connected to the internet.
   - **MDM Server URI**: Enter the EMM server address.

     NOTE Once you have created a MDM profile, you cannot change the MDM server URI.
6. Click **CONTINUE**.
7. On the “Android enterprise profile settings” page, set the following MDM configuration settings.
   - **Custom JSON Data (as defined by MDM)**: In the **Custom JSON data** field, enter data in the following JSON format: For more information about JSON, see http://json.org.
     - Enter the tenant information including the **TenantId** and **TenantType** in the java script object notation (JSON) format, as in `{”TenantId”:”YOUR_TENANT”, ”TenantType”:”M”}`. **TenantId** refers to the name of your EMM company account. It occurs after @ in your EMM Username. For example, if your login ID for EMM is sample@samsung.com, enter as follows:
       - Multi-Tenant: `{”TenantId”:”samsung.com”,”TenantType”:”M”}`
       - Single-Tenant: `{”TenantId”:”EMM”,”TenantType”:”S”}`

- To use Dual DAR on Android Enterprise (Fully Managed or Work Profile on company-owned) devices, make sure you uncheck **Double DAR > Dual DAR use** and enter the following Custom JSON data: Dual DAR platform is decided based on the Mode settings.
  - `{"TenantId":"EMM","TenantType":"M","Method":"KME","DualDAREnable":"true","Mode":", or DO or PO"}`
- If EMM is operated on a closed network, you can install CA certificates in advance for EMM server access before EMM activation. To install CA certificates when logging in to EMM, enter the following Custom JSON data:
  - `{"TenantId":"EMM","TenantType":"M","Method":"KME","PreInstall":"true or false"}`
- To log in to EMM without entering a Mobile ID on Android Enterprise (Fully Managed or Work Profile on company-owned) devices, enter the following Custom JSON data:
  You must select "True" for **Device Auto Registration** in **Setting > Server > Configuration** in the EMM Admin Portal.
  - `{"TenantId":"EMM","TenantType":"M","Method":"KME","ShowMobileId":"Hide"}`

- **Root/intermediate certificate**: Supported on devices running Android 9 or higher. Click **UPLOAD CERTIFICATE FILE** to upload a root or intermediate certificate to be installed on the devices. Only the .cer, .pem, .crt, .ca formats are supported.
- **QR code for enrollment**: Supported on devices running Android 10 or higher. Click **ADD A QR CODE** to enroll the profile using a QR code.
- **Dual DAR**: Select whether to use Dual DAR or not. You can either enter Dual DAR in the Custom JSON data field in the JSON data format or set Dual DAR as a third party crypto application.
  - **Enable Dual DAR**: If you need a third party crypto application, click **Dual DAR use**. Click the checkbox next to **Use 3rd party crypto application** and click **ADD PACKAGE INFORMATION** to enter the package signature for using the 3rd party crypto app.

NOTE Dual DAR is supported on Samsung S10, Note10, or Samsung Knox version 3.3 or higher for Android Enterprise (Fully Managed or Work Profile on company-owned) devices. Fully Managed Dual DAR is supported on Android 12 or higher and Work Profile on company-owned Dual DAR is supported on Android 11 or higher. For more information about Dual DAR, see https://docs.samsungknox.com/dev/knox-sdk/dual-dar-architecture.htm.

8. On the "Android enterprise profile settings" page, set the following devices settings.

- **System applications**: Select the system application settings.
  - **Disable system applications**: Disable all applications to the device owner's profile.
  - **Leave all system applications enabled**: Enable all applications on the device owner profile. If this option is not selected, only the default applications and the Samsung SDS EMM Agent are installed on the user devices.
- **Privacy Policy, EULAs and Terms of Service**: Click **Samsung Knox Privacy Policy** to view the specific privacy policy text displayed to devices users based on their geographic region.
  - **ADD LEGAL AGREEMENT**: Enter the agreement title and agreement text.
- **Company Name**: Enter the company name displayed at the time of device activation.

9. Click **CREATE**. To view the created MDM profile, navigate to **MDM Profiles** on the Knox Mobile Enrollment Portal.

Modifying MDM profiles

To modify an MDM profile, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **MDM Profiles**.
2. On the profile list, click the profile name to modify its information.
3. Modify the selected profile information, and then click **SAVE**.

NOTE Once you have created an MDM profile, you cannot change the MDM server URI.

Registering devices to the Knox Mobile Enrollment Portal

Depending on the device purchase type, you can register devices to the Knox Mobile Enrollment Portal using the following methods

- Knox Reseller Portal: For devices purchased from approved Samsung resellers
- Samsung Knox Deployment App (NFC tagging): For devices purchased from third-party resellers, or for the purpose of testing

For devices purchased from approved Samsung resellers

If the devices were purchased from approved Samsung resellers, you can register the devices to the Knox Mobile Enrollment Portal using the Knox Reseller Portal. For more information on using the Knox Reseller Portal and how to register devices, see the Knox Reseller Portal Admin Guide (https://docs.samsungknox.com/samsung-reseller-guide/Content/manage-devices.htm) and follow the instructions.

After the devices are registered successfully, on the Knox Mobile Enrollment Portal, navigate to **Devices** > **UPLOADS** to view the registered device information with the reseller's information including the registration date and the number of devices, IMEI information, and applied profiles.

For devices purchased from third-party resellers

To register devices purchased from third-party resellers or for the purpose of testing to the Knox Mobile Enrollment Portal using the Samsung Knox Deployment app through NFC tagging, complete the following steps:

NOTE The user information must be registered in the Knox Mobile Enrollment Portal to register the devices. For more information on how to add device users, see Adding new device users.

1. Download the “Samsung Knox Deployment” app from the Google Play Store on your device and install it.
2. Run the “Samsung Knox Deployment” app on your device.
3. On the login screen, enter your Knox Mobile Enrollment Portal user ID and password, and then tap **SIGN IN**.
4. Tap **ENROLL VIA NFC**.

NOTE The NFC mode on your device must be turned on for NFC tagging.

5. On the “Get started” screen, tap **START**.
6. Select a desired MDM profile to apply, and then tap **NEXT**.
7. Tag the user device to your device. To view the information of the registered devices on the Knox Mobile Enrollment Portal, navigate to **Devices** > **UPLOADS**.

Assigning MDM profiles and user devices

After the devices are registered in the Knox Mobile Enrollment Portal, assign the MDM profiles to the registered devices. You can assign them to the registered devices either individually or in bulk using a CSV file.

Individual Assignment

To assign MDM profiles to a registered device individually, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **Devices**.
2. At the top of the “Devices” page, click the **ALL DEVICES** tab.
3. On the device list, click the IMEI/MEID information or serial number. Alternately, you can also click the checkboxes next to IMEI information, and then click **ACTIONS** > **Configure devices**.

NOTE The device windows appear differently depending on how many devices on the list you select.

4. In the “Device Details” or “Configure selected devices” window, enter the following device information.
   - “Device Details” window (When configuring a single selected device)
     - **MDM Profiles**: Select the desired MDM profile from the drop-down list.
     - **Tags**: Enter a tag to use when searching for specific devices.
     - **User ID**: Enter the EMM user ID.
     - **Password**: Enter the EMM user password.

- "Configure selected devices" window (When configuring two or more selected devices)
  - **Modify the MDM profile of selected devices**: Select the desired MDM profile from the drop-down list.
  - **Add tags to selected devices**: Enter a tag to use when searching for specific devices. Click the checkbox next to **Overwrite existing tags** if you want to use the newly entered tag to overwrite existing tags.
  - **User credentials**: Select one of the following options for the user credentials of devices from the drop-down list.
    - **Keep current credentials**: Maintain the existing user credential information for the selected devices.
    - **Clear user credentials**: Remove the existing user credential information for the selected devices.
    - **Overwrite user credentials**: Modify the user ID and password.

5. Click **SAVE** to save the modified device details. The device status changes to **Profile assigned**. To update the device status, click ↻.

Bulk Assignment

You can assign the MDM profiles and user credentials for up to 10,000 registered devices at once.

To assign MDM profiles and user credential to a registered device individually, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **Devices**.
2. On the "Devices" page, click **ALL DEVICES** > **ACTIONS** > **Download devices as CSV** at the bottom of the page to download the `kme_devices.csv` file.
3. Open the downloaded CSV file and enter the information in the columns of the Excel file, and then save the file as a .csv file.
4. At the left bottom of the Knox Mobile Enrollment Portal, click **BULK ACTIONS**.
5. On the "Bulk actions" page, click **View instructions** in the BULK CONFIGURE section to read the instructions to ensure the CSV file is completely filled out, and the click **GOT IT**.
6. On the "Bulk configure" page, click **BROWSE**, and then select the saved .csv file.
7. In the "(Optional) Configure profiles and tags" area, enter the following information.
   - **Modify the MDM profile of selected devices**: Select the desired MDM profile from the drop-down list.
   - **Tags**: Enter a tag to use when searching for specific devices. Click the checkbox next to **Overwrite existing tags** if you want to use the newly entered tag to overwrite existing tags.
8. Click **SUBMIT**. To view the bulk-added information, navigate to **Devices** > **ALL DEVICES**.

Adding new device users

You can add a new device user to the list of existing users.

To add a new device user, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **Device Users**.
2. On the “Device Users” page, click **ADD DEVICE USERS** to add a new device user.
3. In the “Add device user” window, enter a user ID and password to create unique KME device user credentials.

NOTE The user ID and password should both be the credentials of EMM.

4. Click **ADD** to add new device user.

Deactivating KME devices

To disable the use of KME devices, you must deactivate them in the EMM Admin Portal, and then delete them in the Knox Mobile Enrollment Portal. For more information about how to deactivate activated devices in the Admin Portal, see Deactivating devices.

To delete the KME devices, complete the following steps:

1. On the Knox Mobile Enrollment Portal, navigate to **Devices**.
2. On the “Devices” page, click the ALL DEVICES tab.
3. On the device list, click the checkboxes next to the IMEI information to delete the registered device, click **ACTIONS** > **Delete devices**.
4. In the “Delete devices” window, click **DELETE**. The selected devices will be deleted from the KME Portal.

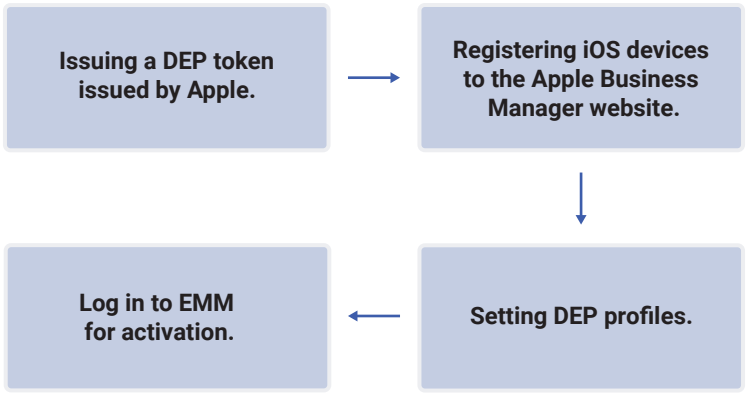
NOTE Once a device is deleted from the KME Portal, the device is permanently removed from the system.

Using the Apple Device Enrollment Program (iOS devices only)

The Apple Device Enrollment Program (DEP) allows you to quickly and easily enroll a large number of organization-owned Apple devices. Devices added by DEP will be enrolled automatically without user intervention with the configured device management profiles.

NOTE Apple has announced a new consolidated platform, Apple Business Manager.
The Device Enrollment Program (DEP) service is no longer available from December 1, 2019. To keep using the DEP service, upgrade to Apple Business Manager. For more information about upgrading to Apple Business Manager, see https://support.apple.com/en-us/HT208817.

To activate devices using DEP, the following procedures must be performed.



Before using the Apple Device Enrollment Program

To use the Apple Device Enrollment Program (DEP) properly, the followings must be prepared:

- Prepare a device from an Apple store, Apple authorized reseller, or carrier.
- Make sure the devices are iOS 9.0 or later.
- Register your Apple Business account in Apple Business Manager or, if you already have a DEP account, upgrade from DEP to ABM. For more information about upgrading to Apple Business Manager, see https://support.apple.com/en-us/HT208817.

Issuing a DEP token

To use Apple Device Enrollment Program (DEP), you must request for a DEP token issued by Apple through a public key, and then set up DEP in the EMM Admin Portal.

To issue a DEP token and set up DEP, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Server Setting**.
   If you have already issued a DEP token, the previous DEP token's information and its expiry date will be displayed. On the DEP Server Setting page, the DEP device sync interval, the DEP device name, and the DEP enrollment method will be displayed.
2. On the "DEP Server Setting" page, click **Download Public Key** to download a public key in the .pem format required to create a new MDM server in the Apple DEP Portal.
3. Visit the Apple Business Manager website at https://business.apple.com, and then enter your Apple ID and password to log in.
4. Sign in using your Apple Business account, and then enter the 6-digit verification code sent to the mobile device registered to your Apple ID.
   - The start window of the ABM site will appear.
5. On the Apple Business Manager website, navigate to **Settings** > **Device Management Settings** at the bottom of the site, and then click **Add MDM Server** on the right of the screen.
6. Configure the MDM server settings, upload the public key file in the .pem format downloaded from the EMM Admin Portal, and then click **Save**.
7. Click **Download Token** on the right of the screen and download the Apple token file in the .p7m format on to the computer.

NOTE Using a single token to activate the DEP devices for one company is recommended.

8. On the "DEP Server Setting" page of the EMM Admin Portal, click **Upload DEP Token**, and then select the DEP token file in the .p7m format issued by Apple.
9. Click **OK**. If the DEP token file is uploaded successfully, the authentication processes between the EMM server and the Apple's DEP server is completed.
10. Click **Set Default Profile** to set up a profile to be assigned to the DEP devices by default, and then click **OK**.
11. Click **Set DEP Device Sync Interval** to set the sync interval of DEP devices, and then click **OK**.

Assigning users to DEP devices

After the DEP devices are enrolled, you can assign users to them.

To assign users, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Device Management**.
2. On the “DEP Device Management” page, click the checkbox for a device you want to assign the user to.
3. Click **Assign User**:
   - Click Unassign User to remove the user assignment from the device. The device must be deactivated before unassigning the user.
4. On the “Select User” window, click the user you want to assign to the device, and then click OK. After the user is successfully assigned, you can send device commands just as you would with other devices controlled by EMM.

Registering DEP devices

When the DEP setting is completed on the Admin Portal, you can register iOS devices on the Apple Business Manager website with the Apple Configurator app downloaded on your MacOS PC.

To register iOS devices in the Apple Business Manager website, complete the following steps:

1. Visit the Apple Business Manager website at https://business.apple.com, and then enter your Apple ID and password to log in.
2. On the **Setting > Device Management Settings** menu of the Apple Business Manager website, click **Add MDM Server** and check that the MDM server is registered.
3. Register iOS devices on the Apple Business Manager website with the Apple Configurator app downloaded on your MacOS PC. For more information, see https://support.apple.com/guide/apple-business-manager/welcome/1/web.
   a. Connect iOS devices to your MacOS PC to reset them.
   b. Select the device to enroll and click **Prepare**.
   c. On the pop-up window that opens, select **Manual Configuration > Add to Apple School Manager** or **Apple Business Manager**, and **Allow devices to pair with other computers** and then click **Next**.
   d. Select **MDM Server** and click **Next**.
   e. Select **Organization** and click **Next**.
   f. Select the **Setup Assistant** options and click **Next**. The activation process will start and take about 10 minutes to complete.
   g. After the activation process, sign in to the devices.

4. Navigate to **Device > Allocation Record** on the Apple Business Manager website, and make sure that the devices enrolled in step 3 are correctly enrolled.

Selecting the DEP device name format

Administrators can select the name format of the DEP devices. You can setup the DEP device name to include the user ID, and the devices that have already been activated also can change the name format when unassigning and reassigning the existing users. You can view the DEP device name in the device name column in the **Device** menu.

To select the DEP device name format, complete the following steps:

1. Navigate to **Setting > iOS > DEP Server Setting**.
2. At the bottom of the "DEP Server Setting" page, click **DEP Device Name**.
3. In the "DEP Device Name" pop-up window, select the name format.
   - **AppleDEP_iOS_#Sequence Number**: The device names will be set in this format.
   - **UserID_AppleDEP_iOS_#Sequence Number**: The device names will be set in this format. When users are assigned or unassigned, the device name will change to a format which includes the user ID. For more information about assigning users, see Assigning users to DEP devices.
4. Click **Save**.

Setting DEP profiles

After the iOS devices are registered to the Apple Business Manager website, you must set the DEP profile to be assigned to the devices through the EMM Admin Portal.

The DEP profile is applied to the DEP devices when the DEP devices are activated.

To set a DEP profile, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Server Setting**.
2. On the “DEP Server Setting” page, click **Set Default DEP Profile**.
3. In the “Set DEP profile” window, set the following items in the DEP profile:
   - **Supervised Mode**: Click the checkbox next to **Apply** to enable the supervised mode that is only available on iOS devices and must be applied to the DEP devices.
     - **Delete MDM profile**: Click the checkbox next to **Allow** to allow users to delete the MDM profile.
     - **Supervising host certificate list**: Click **Add** to add the registered certificate to the Apple device you want to pair with the DEP devices.
   - **Pairing**: Click to allow other Apple devices to pair with the DEP devices.
   - **Skip Settings**: Select the items that appear during the device setup process after users turn on their DEP devices for the first time. If the items are checked, they do not appear on the device.
4. Click **Save** to save the set DEP profile.

Assigning users to DEP devices

After the DEP devices are enrolled, you can either add single users or add users in bulk to DEP devices. The user information to be assigned must be registered in the **User** menu. After assignment, administrators can unassign or reassign users. In this case, the devices will go through the EMM Client update to update the user information. However, if users stop or delete the EMM Client update, reassignment is unavailable.

To assign users, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Device Management**.
2. On the “DEP Device Management” page, click the checkbox for a device you want to assign the user to.
3. Click **Assign User**:
   The user assignment or unassignment feature is available only when the devices are activated or deactivated.
   - Click **Unassign User** to remove the user assignment from the device. The device must be deactivated before unassigning the user.
4. On the “Select User” window, click the user you want to assign to the device, and then click **OK**.

To assign users in bulk, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Device Management**.
2. On the “DEP Device Management” page, click **Bulk Assign Users**.
3. In the “Bulk Assign Users” pop-up window, view the procedure and click **Download Template** and download an xls file.
4. Enter the user and device information in the downloaded template file, upload it and click **OK**. The users in the uploaded file will be automatically assigned to the DEP devices and the devices will be activated.
   - Bulk user assignment is available only when the devices are activated or deactivated. The upload result can be viewed in a separate pop-up window.
   - User information must be registered in advance in the USER menu of the EMM Admin Portal.

Managing DEP devices

The DEP devices enrolled on the Apple Business Manager website can be viewed in the **Device** or **DEP Device Management** menu of the Admin Portal, and the DEP devices can be added or deleted through DEP synchronization. In **Setting > iOS > DEP Device Management**, the EMM server is synchronized with the DEP server to update the DEP device list and manage the DEP devices by assigning users and DEP profiles.

Viewing the DEP device details

To view the DEP device details in the EMM Admin Portal, complete the following steps:

1. Navigate to **Device** or **Setting** > **iOS** > **DEP Device Management**.
2. In the **Device** or **DEP Device Management** menu, click the name or serial number of the DEP device you want to view the information of. DEP devices are displayed as DEP in the Enrolled Type column of the **Device** menu.
3. View the selected DEP device information on the “Device Detail” page.

Synchronizing with the DEP server

To synchronize with the DEP server and the Apple Business Manager website to update the DEP device list in the EMM Admin Portal, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Device Management**.
2. On the “DEP Device Management” page, click **Sync DEP** to synchronize with the DEP server.
3. In the “DEP device sync” window, click **OK**. The DEP device list in the EMM Admin Portal will be updated.

Modifying and assigning the DEP profiles

To modify and assign DEP profiles to DEP devices, complete the following steps:

1. Navigate to **Setting** > **iOS** > **DEP Device Management**.
2. On the “DEP Device Management” page, click the checkboxes next to the DEP devices on the DEP device list, and then click **Set DEP profile** to modify the DEP profile.
3. In the “Set DEP profile” window, modify the desired DEP profile items, and then click **Save** to save the set DEP profile and return to the “DEP Device Management” page. For more information on setting the DEP profiles, see Setting DEP profiles.
4. Click Sync DEP to synchronize with the DEP server to update the DEP device list. The modified DEP profile will be assigned to the DEP devices.

Enrolling DEP devices in EMM

You can select the EMM enrollment method for the DEP devices. The DEP devices can be enrolled after administrator's assigning users or when users enter their login information.

To select the enrollment method, complete the following steps:

1. Navigate to **Setting > iOS > DEP Server Setting**.
2. At the bottom of the "DEP Server Setting" page, click **DEP Enrollment method**.
3. In the "DEP Enrollment Method" pop-up window, select **User Assignment** or **User Authentication**.
   - **User Assignment**: Assign users to the DEP devices in advance. The devices will be automatically enrolled in EMM.
   - **User Authentication**: The DEP devices will be enrolled when users enter their account information. If users are assigned in advance, the assigned users will be authenticated. If not, users who perform the authentication will be assigned to the devices.
4. Click **Save**.

Deactivating DEP devices

If you want to use DEP devices as general iOS devices or if the DEP devices are no longer required, you can deactivate the DEP devices in the Apple Device Enrollment Program (DEP) Portal.

To deactivate DEP devices, complete the following steps:

1. Visit the Apple DEP Portal at https://business.apple.com, and then enter your Apple ID and password to log in.
2. On the Apple DEP Portal of the "Device Enrollment Program" page, click **Get Started**.
3. On the Apple DEP Portal, navigate to **Device Enrollment Program** > **Manage Servers**.
4. On the "Server Details" page, click an MDM server to disable and delete it, and then click **Delete Server**. In the "Are you sure you want to delete this server?" window, click **Delete**. All the DEP devices on this server will be deleted.

NOTE To delete the MDM server and relocate the DEP devices on this server, select **Reassign Devices** from the drop-down list. Then, select a different MDM server where you want to relocate the MDM devices to and click **Delete**.

5. On the EMM Admin Portal, Navigate to **Setting** > **iOS** > **DEP Device Management**.
6. On the "DEP Device Management" page, click Sync DEP to synchronize with the DEP server.
7. In the "DEP device sync" window, click **OK**. The DEP device list in the EMM Admin Portal will be updated according to the DEP server, and the DEP devices on the DEP server in the EMM Admin Portal will be deleted.

Managing devices

You can change the device's status or send device commands to manage the devices registered in the Admin Portal.

Using device commands, when IT admin collect malicious application information from devices, they also collect logs containing relevant diagnosis information, and view or download log files. EMM provides a function for blocking malicious applications by linking with the Check Point Mobile Threat Prevention (MTP) feature. An IT admin can check the malicious applications detected by the MTP Agent on the Check Point MTP Console.

Changing the Device Status

Samsung SDS EMM manages the devices with several different types of device status as shown in the following table.

Status	Description	Possible status change options
Provisioning	Device has been registered but has not been activated yet.	You can change the status to "Deactivated."
Activated	Device has been activated and can be controlled by the Admin Portal.	You can change the status to "Deactivated" or "Blocked by Admin."
Activation Blocked	Deactivated device which has been blocked from device activation.	You can change the status to "Deactivated."
Blocked by System	The device, which has exceeded Keep Alive due or has been factory-reset, is blocked by the system	You can change the status to "Deactivated."
Expired	The KPE-Premium or Dual DAR license has expired. **NOTE** The EMM server performs an automatic batch job that checks the license every day at 01:00, checks the valid license for expired devices, and transmits the update license device command to them.	You can change the status to "Deactivated."
Deactivated	Device has been deactivated and cannot be controlled by the Admin Portal.	You can change the status to "Activation Blocked."
Blocked by Admin	Device has been blocked by the administrator through the Admin Portal due to the device being lost or changed.	You can change the status to "Deactivated."

NOTE DEP devices can be reactivated only when changed to “Deactivated” from “Activation Blocked,” “Blocked by System,” “Expired,” or “Blocked by Admin.”

To change the device status, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click a checkbox for a device you want to change the status of, and then click **Change Status**.
3. In the “Change Status” window, either select one of the following options or click **OK** if there is only one option.
   - **Device command**: Deactivate a device with a mobile connection via a device command.
   - **Offline Deactivation**: Deactivate a device without a mobile connection. The user can deactivate the device by entering the offline deactivation code that they have received.
   - **Blocked by Admin**: Change the status to “Blocked by Admin” without connecting to the device.
   - **Change status only**: Change the status to “Deactivated” only on the server without connecting to the device.

When the device has an inconsistent status between the server and device server, the device will request a connection to the server, and the device will be deactivated and the audit log will no longer be recorded in the EMM server.

You can choose to delete the internal applications installed on Android devices and the applications installed on devices with iOS devices upon deactivation. You can also set automatic deletion by navigating to **Setting** > **Server** > **Configuration**, and then setting **Delete App upon Unenrollment** to **TRUE**.

Deactivating devices

You can deactivate the devices managed by EMM. The methods for deactivation differ depending on the device status.

NOTE
- When you deactivate Fully Managed or the Fully Managed with Work Profile devices, the devices will be factory reset and the micro SD cards of the devices with Android 7.0 (Nougat) - 8.0 (Oreo) can be wiped. Please be cautious of potential data loss.
- When you deactivate Work Profile on company-owned devices, the devices will be factory reset and the micro SD cards of the devices with Android 11 can be wiped.

To simply change a logged in user's details, send the Delete account command, and then allow the user log out from the EMM Client. The device then becomes deactivated, and the user can log in again and set the password.

Deactivating connected devices

To deactivate devices that are connected to the server, complete the following steps:

1. Navigate to **Device**.
2. On the "Device" page, click a checkbox for a device you want to deactivate.
3. Click **Change Status**.
4. In the "Change Status" window, select **Device Command**, and then click **OK**.
    - When a user loses or changes the device, select **Blocked by Admin**.

Deactivating disconnected devices

When a device is unable to communicate with the server, you can send an offline deactivation code to the device. Then, the user can change the device's status manually and deactivate the device.

To deactivate devices that are offline, complete the following steps:

1. Navigate to **Device**.
2. On the "Device" page, click a checkbox for a device you want to deactivate.
3. Click **Change Status**.
4. In the "Change Status" window, select **Offline Deactivation**, and then click **OK**.
    - You can view the offline deactivation code from the device detail.
5. Inform users of the use of the offline deactivation code from step 4.
    - When the user enters the received offline deactivation code, the device will become deactivated, corresponding to its status on the server.

Sending device commands to devices

You can send device commands to activated devices by user, organization, group, or device and control them remotely. For devices with Knox Workspace or Work Profile, you can select the tab of the area on the top you want to send a device command to. Available device commands vary depending on the device type. For more information on each device command, see List of device commands: Android Enterprise, List of device commands: Android Legacy/Knox Workspace, List of device commands: iOS, List of device commands: Windows, List of device commands: Tizen Wearable.

NOTE In general, device commands take a higher priority than profile policies. However, policies take a higher priority than the following device commands: Install, Run, Uninstall, Locate the current position, and Reset SD Card. For more information, see the list of device commands.

To send device commands, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click the checkbox next to the device name to send a device command to, and then click **Device Command**.
3. In the “Device Command” window, select the desired device command.
   - For devices that have a Knox Workspace, click the target area between **General** and **KNOX - LightWeight Knox**.
   - For Fully Managed with Work Profile or Work Profile on company-owned devices, click a target area between **Fully Managed Device** and **Work Profile**.
4. In the “Request Command” window, click **OK**.

Checking device commands in request

Check device commands that have not been sent successfully due to network or system issues. You can resend the device commands in request or delete them individually or altogether. You can also download all device commands in queue as an Excel file.

NOTE If no device command has been sent within the past six hours of restarting the device, then EMM agent requests the server for a device command and can have it resent to the device.

To check the device commands in request and resend or delete them individually or altogether, complete the following steps:

1. Navigate to **Service Overview** > **Device in Request**.
2. On the “Device in Request” page, enter a request date, device name and user ID and then click **Search**.
3. In the **Device Command** tab, view the information of the device commands that have been found.
   - To resend the device commands in request, click the checkboxes of the device commands to resend, and then click **Re-Request**.
   - To delete the device commands in request, click the checkboxes of the device commands to delete, and then click **Cancel Request**.
   - To delete all the device commands in the request, click **Cancel All Request**.

NOTE To set the EMM server to resend the device commands in request automatically, navigate to **Setting** > **Configuration**, and then set the number next to **Daily retries for device commands in request**.

Checking the history of application installation in request

You can check the list of applications that have not been installed successfully due to server issues. The device commands in request can be deleted individually or altogether. The list of applications that have not been installed can be downloaded as an Excel file.

NOTE If you try to install an application on more devices than the number set in **Setting > Server > Configuration > Application > Maximum Number of Devices Installing Apps at the Same Time**, you can view the application by device in the history of application installation in request. For more information, see Application.

To view the list of applications that have not been installed by device and delete them individually or altogether, complete the following steps:

1. Navigate to **Service Overview** > **Device in Request**.
2. On the “Device in Request” page, enter a request date, device name, user ID or application name, and then click **Search**.
   - Application name search is available only if you select the application installation tab.
3. In the **Application Installation** tab, view the information of the application that has not been installed.
   - To delete the application that has not been installed, click the checkboxes of the Application & Package Name, and then click **Cancel Request**.
   - To delete all the applications that have not been installed, click **Cancel All Request**.

Viewing device command history

You can view audit logs and audit events related to the device command history by date. Show the detailed flow of audit event and audit log for the result of device command. Audit logs can be collected by using the device command **Collect Audit Log**. For more information about audit log items, see Viewing audit logs.

To view the device command history, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click a device name.
3. On the “Devices Detail” page, click the “Command History” tab.
4. Click a command name to view the audit result of the device command.

NOTE To view the device command logs by each platform, navigate to **Service Overview** > **History** > **Group Command History**, enter a request date and a group ID or organization name, click **Search**, and then click a group or organization name.

List of device commands: Android Enterprise

The available device commands vary depending on the Android Enterprise manage types. For Fully Managed with Work Profile or Work Profile on company-owned devices, you can select either **Fully Managed** or **Work Profile** to send device commands to.

Device (Android Enterprise-Fully Managed/Work Profile)

Device command	Description
Apply Latest Profiles	Sends the latest profile and application information to the device and controls the device with the profile and information.
Enable EAS (Samsung Email App Only)	Allows using Exchange ActiveSync for Samsung Email application.
Disable EAS (Samsung Email App Only)	Disallows using Exchange ActiveSync for Samsung Email application.
Lock Device	Locks a device. You can enter a reason for locking the device and a phone number to contact when the device is lost. The entered information appears on the locked device screen. **NOTE** For non-Samsung Android devices, this policy supports only the devices with Android 8.0 (Oreo) and lower.
Unlock Device	Unlocks a device. **NOTE** For non-Samsung Android devices, this policy supports only the devices with Android 8.0 (Oreo) and lower.
Lock Screen	Locks the device screen. If the device's screen is password-locked, then the user needs to enter the password to access the screen again.
Factory Reset	Performs factory reset and changes the device status to Deactivated.
Power Off Device	Turns off the device. **NOTE** Only Samsung devices are supported except the devices with Android 10 (Q).
Reboot Device	Reboots the device.
Reset Screen Password	Resets the device's screen lock password and creates a temporary password. After sending the device command, the temporary password that can be found on the device's detailed information page will be delivered to the user. For more information, see the screen lock password in Viewing the device details. **NOTE** For devices with Android 12 or higher, temporary passwords will be created according to the minimum complexity requirements.

Device command	Description
Reset SD Card	Initializes the external SD card of the device. **NOTE** For devices whose **External SD Card policy** is set to **Disallowed** in the profile, you cannot reset the SD card using the device command, because the policy takes a higher priority than the device command.
Reset Data Usage	Resets data usage among the Android device's inventory information. • Wi-Fi transfer data (in/out) • Network transfer data (in/out) **NOTE** Only Samsung devices are supported except the devices with Android 10 (Q).
Reset Number of Calls	Resets the number of call(s) and number of missed call(s) among Android device's inventory information, • Number of call(s) • Number of missed call(s)
Delete a CA Certificate	Delete the CA certificate installed in EMM.
Delete a User Certificate	Delete the user certificate installed in EMM.
Delete a User Install Certificate	Delete the user install certificate installed in EMM.
Update FOTA Firmware Version	Updates the E-FOTA firmware version.
Delete a Work Profile CA Certificate	Delete the CA certificate installed in Work Profile.
Delete a Work Profile User Certificate	Delete the user certificate installed in Work Profile.
Delete a Work Profile User Install Certificate	Delete the user install certificate installed in Work Profile.

Device command	Description

Apply Customized Event	Controls devices with the policies configured for a customized event.
	
	To run a user-defined event on a device, complete the following steps:
	
	1. In the “Device Command - Apply customized event” window, select the event code.
	  • If profile has a user-defined event, the event code list appears.
	2. Select an item to run.
	  • **Set on**: You can control a device with policies that are set on the customized event.
	  • **Set off**: Removes the customized event from device and controls the device with the default policies set on the profile.
	3. Click **OK**.
	
	To check the policies applied on a customized event, complete the following steps:
	
	1. Navigate to **Profile**.
	2. Click the icon () next to a profile name from the list.
	  • In the “Conditions” window, check Event type and Conditions.
	3. Click the profile name to open the “Profile Detail” page, and then click **Policy** tab.
	4. Check the policies for Android Enterprise.

Start Gate Access Event	Controls devices with the policies configured for a Start gate access event.
	
	To run a Start gate access event on a device, complete the following steps:
	
	1. In the “Device Command” window, select an event code.
	  • If there is a Start gate access event configured on the profile designated for the device, access code is shown on the list.
	2. Select an item to run.
	  • **Set on**: Control devices with the policies configured on the Start gate access event.
	  • **Set off**: Removes the Start gate access event from the device and control the device with the default policies set on the profile.
	3. Click **OK**.
	
	To check the policies applied for a Start gate access event, complete the following steps:
	
	1. Navigate to **Profile**.
	2. Click the icon () next to a profile name from the list.
	  • In the “Conditions” window, check Event type and Conditions.
	3. Click the profile name to open the “Profile Detail” page, and then click **Policy** tab.
	4. Check the policies for Android Enterprise.

Application (Android Enterprise-Fully Managed/Work Profile)

If the device is a Work Profile on company-owned type, device commands can be sent within the Work Profile area.

Device command	Description
Install or Update App	Installs or updates applications on a device. In the “Request Command” window, select an application to install or update. **NOTE** • To prevent users from deleting public applications other than Android Enterprise applications, you must select the Install Type option as Automatic (Non-removable) when assigning the applications. For more information, see Assigning Managed Google Play applications. • The Application installation blacklist/whitelist policies take a higher priority than device commands.
Run App	Runs applications on a device. In the “Request Command” window, select an application to run. **NOTE** • The Application running blacklist/whitelist policies take a higher priority than device commands. • For non-Samsung devices running Android 10 (Q) or higher, only apps installed in the general area will be executed.
Uninstall App	Deletes applications from a device. In the “Request Command” window, select an application to uninstall. **NOTE** The Application uninstallation prevention list setting policy takes a higher priority than device commands.
Apply Latest internal App Information	Sends the latest internal application information and updates the device according to the information.
Apply the Latest App Managed Configuration	Sends the MC (Managed Configuration) information set in internal and public applications and updates the device according to the information.

EMM (Android Enterprise-Fully Managed/Work Profile)

Device command	Description
Push Notification	Sends an emergency message to the device. The message icon is shown on the status bar of the device. In the “Push Notification” window, enter the title and content of the message, and then select between **Notification** and **Pop up** for the send type.
Deactivate Device	Deactivates a selected device on the device list.
Update License	Updates the devices selected in the device list with a KPE Premium license. **NOTE** Update to the Dual DAR or KPE Premium license on Work Profile on company-owned or Fully Managed devices if licenses expire.
Upgrade License	If the devices selected from the device list are using a KPE Standard license, it will be changed to a KPE Premium license. Be careful, as you cannot downgrade to KPE Standard. **NOTE** When upgrading EMM to v2.4.1 version on a Samsung device, update the EMM app version is unavailable if there is no KPE Premium license in the Work Profile. Upgrade new version of the EMM app is available when upgrading the license through device command in the Work Profile device or Fully Managed With Work Profile/Work Profile with company-owned device activated with KPE Standard license.
Update EMM	Updates the EMM Client on the device for a new patch or version. The agent information registered in the EMM server is sent to a device. The device automatically selects the appropriate agent to request installation files from the server. **NOTE** • In the case of a Non-Samsung device, an update of the EMM app is unavailable. Upgrade of the EMM app is available when the EMM app is installed manually. However, update of the EMM app is unavailable if the Installation of the application from untrusted sources policy is set as Disallow. • Users can directly upgrade on their devices after updating to v2.5.5 by using the **Update EMM** device command.
Update User Information	Updates the device user information such as the user activation status/ username/user settings (Secure Browser website URL information, bookmark information) and license information. If the user is logged out from the deactivated device, you can send this device command to enable the user to log in to EMM automatically.

Device command	Description
Switch to Fully Managed (delete Work Profile)	Change a Fully Managed with Work Profile device to a Fully Managed device. The Work Profile on the device will be deleted. **NOTE** If the OS version of a Fully Managed with Work Profile device is upgraded from Android 10 (Q) to Android 11, the device will be automatically switched to Work Profile on company-owned type. To keep the device as a Fully Managed type, send the Switch to Fully Managed device command and switch the device to Fully Managed type.
Lock Screen of EMM Client	Locks the EMM Client. When the application is locked, the users have to enter the screen lock password which was configured during installation. If a user forgets the password of EMM Client screen lock, you can send the Delete Account command and make the user logged out from the EMM Client. Then, the user can set the password again upon login.
Unlock EMM Client	Unlocks the EMM Client which was locked as a result of compliance violation (ex. Exceeding the maximum number of incorrect password). If it's manually locked by user or administrator, EMM Client cannot be unlocked ty this device command.
Delete Account	Deletes the account registered in the EMM Client.
Exit Kiosk	Exits the Kiosk mode without unenrollment. You can find the status of the Kiosk mode in the Security tab on the Device Detail page.
Collect Audit Log	Collects the EMM audit logs of the device. When the log size exceeds the maximum size, logs are automatically sent to the server, but the log file may be lost. For more detailed information, see Viewing audits.
Collect Device Log	Collects the logs of devices.
Collect Diagnosis Information	Collects a device log to diagnose the cause of device lock,
Deactivate Service	Deactivate a device.
Reset Push Token	Renews the Push token.
Update Terms and Policies	If you change the user terms of the EMM Client app on the EMM Admin Portal, the terms of use will be displayed in a pop-up window so that the user can agree upon logging in again to the EMM Client from the device. If the user agrees to the terms, the policy will be updated, otherwise the EMM Client will no longer be available.

Device Info. (Android Enterprise-Fully Managed)

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.
Sync Device Information	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the “Device Detail” page.
Sync Installed App List	Updates the information of installed applications. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the “Application” tab.
Authenticate SIM Card	Authenticates the SIM card on a device.
Authenticate SD Card	Authenticates the external SD card on a device.
Attestation	Checks if a device’s OS has been compromised. The result can be found from the device details.
SafetyNet Attestation	Checks if a device’s OS has been compromised through Google API. Google API checks the integrity of the device and blocks compromised software or applications. If the device is regarded as compromised while checking, the device will be factory reset and re-registered.

Device Info Sync (Android Enterprise-Work Profile)

Device command	Description
Collect H/W status	Updates the inventory information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the “Device Detail” page.
Sync Installed App List	Updates the information of installed applications. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the “Application” tab.
Collect device/app info	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the “Device Detail” page.

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.
SafetyNet Attestation	Checks if a device's OS has been compromised through Google API. Google API checks the integrity of the device and blocks compromised software or applications. If the device is regarded as compromised while checking, the device will be factory reset and re-registered.

Work Profile (Android Enterprise-Work Profile)

Only the Work Profile area on device is supported.

Device command	Description
Reset Screen Password	Resets the Work Profile area password. When the user forgets the Work Profile password, this command is sent to reset the password. **NOTE** Depending on the Android OS version, the process to re-configure the new password may differ. For Android 8.0 (Oreo) or higher, the user will receive a temporary password after EMM authentication. And then, the user can re-configure the new Work Profile password. For operating systems lower than Android 8.0 (Oreo), the user can re-configure the Work Profile password directly after EMM authentication.
Lock Screen	Locks the Work Profile area.

List of device commands: Android Legacy/Knox Workspace

The available device commands vary depending on device manage type. For Android Legacy with Knox Workspace devices, you can select either the General or KNOX - LightWeight Knox area to send the device command to.

Device (Android Legacy/Knox Workspace)

Device command	Description
Apply Latest Profiles	Sends the latest profile and application information to the device and controls the device with the profile and information.
Enable EAS (Samsung Email App Only)	Allows using Exchange ActiveSync for Samsung Email application.
Disable EAS (Samsung Email App Only)	Disallows using Exchange ActiveSync for Samsung Email application.
Lock Device	Locks a device. You can enter a reason for locking the device and a phone number to contact when the device is lost. The entered information appears on the locked device screen. **NOTE** • For non-Samsung Android devices, Android 8.0 (Oreo) and lower are only supported. • Android 10 (Q) devices are not supported.
Unlock Device	Unlocks a device. **NOTE** • For non-Samsung Android devices, Android 8.0 (Oreo) and lower are only supported. • Android 10 (Q) devices are not supported.
Lock Screen	Locks the device screen. If the device's screen is password-locked, then the user needs to enter the password to access the screen again.
Factory Reset	Performs factory reset and changes the device status to Deactivated.
Power Off Device	Turns off the device. **NOTE** Android 10 (Q) devices are not supported.
Reboot Device	Reboots the device.
Reset Screen Password	Resets the device's screen lock password and creates a temporary password. After sending the device command, the temporary password that can be found on the device's detailed information page will be delivered to the user. For more information, see the EMM password in Viewing the device details. **NOTE** Android 9.0 (Pie) or higher devices are not supported.

<table>
<tr><th>Device command</th><th>Description</th></tr>
<tr><td>Reset SD Card</td><td>Initializes the external SD card of the device.

NOTE For devices whose External SD Card policy is set to Disallowed in the profile, you cannot reset the SD card using the device command, because the policy takes a higher priority than the device command.</td></tr>
<tr><td>CC Mode setting</td><td>If a device supports CC (Common Criteria) mode, apply a policy as below to activate CC mode. This is only supported on high security EMM.
• Factory reset upon exceeded number of login failures
• Not allow to record password history
• Check Certificate Revoke List (CRL) Confirmation
• Use of SD cards and encryption of SD cards or other external drives

To set the CC Mode on the Device Management Profile menu, complete the following steps:
1. Navigate to Profiles.
2. On the “Profile” page, click a profile name allocated for the device from the list.
3. Click the profile name to open the “Profile Detail” page, and then click Modify Policy.
4. On “Set Policy” page, click Android Enterprise and then set the following policies:

<table><tr><th>Category</th><th>Policy</th><th>Description</th></tr><tr><td rowspan="3">Security</td><td>If maximum failed attempts is exceeded</td><td>Select Factory reset.</td></tr><tr><td>Retain history for</td><td>Enter 0.</td></tr><tr><td>CRL confirmation</td><td>Select Allow.</td></tr><tr><td>System</td><td>Encryption for storage</td><td>Select Apply, and then select both System storage and External SD card.</td></tr></table></td></tr>
<tr><td>Release CC Mode</td><td>Release the CC (Common Criteria) Mode of the device.</td></tr>
<tr><td>Reset Data Usage</td><td>Resets data usage among the Android device’s inventory information.
• Wi-Fi transfer data (in/out)
• Network transfer data (in/out)

NOTE Android 10 (Q) devices are not supported.</td></tr>
</table>

Device command	Description
Reset Number of Calls	Resets the number of call(s) and number of missed call(s) among Android device's inventory information. • Number of call(s) • Number of missed call(s)
Update FOTA Firmware Version	Updates the E-FOTA firmware version.
Apply Customized Event	Controls devices with the policies configured for a customized event. To run a user-defined event on a device, complete the following steps: 1. In the "Device Command - Apply customized event" window, select the event code. • If profile has a user-defined event, the event code list appears. 2. Select an item to run. • **Set on**: You can control a device with policies that are set on the customized event. • **Set off**: Removes the customized event from device and controls the device with the default policies set on the profile. 3. Click **OK**. To check the policies applied on a customized event, complete the following steps: 1. Navigate to **Profile**. 2. Click the icon ( ) next to a profile name from the list. • In the "Conditions" window, check Event type and Conditions. 3. Click the profile name to open the "Profile Detail" page, and then click **Policy** tab. 4. Check the policies for Android and Knox Workspace.

Device command	Description
Start Gate Access Event	Controls devices with the policies configured for a Start gate access event. To run a Start gate access event on a device, complete the following steps: 1. In the “Device Command” window, select an event code. • If there is a Start gate access event configured on the profile designated for the device, access code is shown on the list. 2. Select an item to run. • **Set on**: Control devices with the policies configured on the Start gate access event. • **Set off**: Removes the Start gate access event from the device and control the device with the default policies set on the profile. 3. Click **OK**. To check the policies applied for a Start gate access event, complete the following steps: 1. Navigate to **Profile**. 2. Click the icon ( ) next to a profile name from the list. • In the “Conditions” window, check Event type and Conditions. 3. Click the profile name to open the “Profile Detail” page, and then click **Policy** tab. 4. Check the policies for Android and Knox Workspace.

Application (Android Legacy/Knox Workspace)

Device command	Description
Install or Update App	Installs or updates applications on a device. In the “Request Command” window, select an application to be install or update. You can select up to 20 applications from the list. **NOTE** • The Application installation blacklist/whitelist policies take a higher priority than device commands. • You can send Install or Update App by selecting up to 100 devices from the device list at once.
Run App	Runs applications on a device. In the “Request Command” window, select an application to run. **NOTE** The Application running blacklist/whitelist policies take a higher priority than device commands.
Stop App	Stops applications on a device. In the “Request Command” window, select an application to stop.

Device command	Description
Delete App data	Deletes data from applications. In the “Request Command” window, select an application to delete.
Uninstall App	Deletes applications from a device. In the “Request Command” window, select an application to uninstall. **NOTE** The Application uninstallation prevention list setting policy takes a higher priority than device commands.
Enable app running	Allows an application to run on a device. In the “Request Command” window, select an application to run.
Disable app running	Disallows an application to run on a device. In the “Request Command” window, select an application to disallow.
Apply Latest internal App Information	Sends the latest internal application information and updates the device according to the information.

EMM (Android Legacy/Knox Workspace)

Device command	Description
Push Notification	Sends an emergency message to the device. The message icon is shown on the status bar of the device. In the “Push Notification” window, enter the title and content of the message, and then select between **Notification** and **Pop up** for the send type.
Deactivate Device	Deactivates a selected device on the device list.
Update License	Updates the devices selected in the device list with a Dual DAR or KPE Premium license.
Upgrade License	If the devices selected from the device list are using a Dual DAR license, the Dual DAR license will be updated. If the devices were using a KPE Standard license, it will be changed to a KPE Premium license. Be careful, as you cannot downgrade to KPE Standard.
Update EMM	Updates the EMM Client on the device for a new patch or version. The agent information registered in the EMM server is sent to a device. The device automatically selects the appropriate agent to request installation files from the server.
Update User Information	Updates the device user information such as the user activation status/ username/user settings (Secure Browser website URL information, bookmark information) and license information. If the user is logged out from the activated device, you can send this device command to enable the user to log in to EMM automatically.

Device command	Description
Lock Screen of EMM Client	Locks the EMM Client. When the application is locked, the users have to enter the screen lock password which was configured during installation. If a user forgets the password of EMM Client screen lock, you can send the Delete Account command and make the user logged out from the EMM Client. Then, the user can set the password again upon login.
Unlock EMM Client	Unlocks the EMM Client which was locked as a result of compliance violation (ex. Exceeding the maximum number of incorrect password). If it's manually locked by user or administrator, EMM Client cannot be unlocked ty this device command.
Delete Account	Deletes the account registered in the EMM Client. The user is logged out from the EMM Client. Then, the user can set the password again when logging in.
Exit Kiosk	Exits the Kiosk mode without unenrollment. You can find the status of the Kiosk mode in the Security tab on the Device Detail page.
Collect Audit Log	Collects the EMM audit logs of the device. When the log size exceeds the maximum size, logs are automatically sent to the server, but the log file may be lost. For more detailed information, see Viewing audits.
Collect Device Log	Collects the logs of devices.
Collect Diagnosis Information	Collects a device log to diagnose the cause of device lock,
Reset Push Token	Renews the Push token.
Update Terms and Policies	If you change the user terms of the EMM Client app on the EMM Admin Portal, the terms of use will be displayed in a pop-up window so that the user can agree upon logging in again to the EMM Client from the device. If the user agrees to the terms, the policy will be updated, otherwise the EMM Client will no longer be available.

Device Info. (Android Legacy/Knox Workspace)

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.

Device command	Description
Sync Device Information	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the "Device Detail" page. **NOTE** For iOS devices, only the hardware status is updated.
Sync Installed App List	Updates the information of installed applications. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the "Application" tab.
Authenticate SIM Card	Authenticates the SIM card on a device.
Authenticate SD Card	Authenticates the external SD card on a device.
Attestation	Checks if a device's OS has been compromised. The result can be found from the device details.

Container (Android Legacy/Knox Workspace)

Only the Workspace area of Knox Workspace is supported.

Device command	Description
Lock Knox Workspace	Locks the Knox Workspace. Users cannot access the Knox Workspace unless you unlock it by sending this command.
Unlock Knox Workspace	Unlocks the Knox Workspace.
Reset Knox Workspace Password	Resets the Knox Workspace password. When the user forgets the Knox Workspace password, this command is sent to reset the password. **NOTE** Depending on the Android OS version, the process to re-configure the new password may differ. For Android 8.0 (Oreo) or higher, the user will receive a temporary password after EMM authentication. And then, the user can re-configure the new Knox Workspace password. For operating systems lower than Android 8.0 (Oreo), the user can re-configure the Knox Workspace password directly after EMM authentication.
Uninstall Knox Workspace	Deletes the selected Knox Workspace. Inventory information is updated on the server upon deletion.

List of device commands: iOS

The available device commands vary depending on device manage type. Some device commands are only supported in iOS supervised mode.

Device (iOS)

Device command	Description
Apply Latest Profiles	Sends the latest profile and application information to the device and controls the device with the profile and information.
Apply Customized Event	Controls devices with the policies configured for a customized event. To run a user-defined event on a device, complete the following steps: 1. In the “Device Command - Apply customized event” window, select the event code. • If profile has a user-defined event, the event code list appears. 2. Select an item to run. • **Set on**: You can control a device with policies that are set on the customized event. • **Set off**: Removes the customized event from device and controls the device with the default policies set on the profile. 3. Click **OK**. To check the policies applied on a customized event, complete the following steps: 1. Navigate to **Profile**. 2. Click the icon ( ) next to a profile name from the list. • In the “Conditions” window, check Event type and Conditions. 3. Click the profile name to open the “Profile Detail” page, and then click **Policy** tab. 4. Check the policies for iOS.

Device command	Description
Start Gate Access Event	Controls devices with the policies configured for a Start gate access event. To run a Start gate access event on a device, complete the following steps: 1. In the “Device Command” window, select an event code. • If there is a Start gate access event configured on the profile designated for the device, access code is shown on the list. 2. Select an item to run. • **Set on**: Control devices with the policies configured on the Start gate access event. • **Set off**: Removes the Start gate access event from the device and control the device with the default policies set on the profile. 3. Click **OK**. To check the policies applied for a Start gate access event, complete the following steps: 1. Navigate to **Profile**. 2. Click the icon ( ) next to a profile name from the list. • In the “Conditions” window, check Event type and Conditions. 3. Click the profile name to open the “Profile Detail” page, and then click **Policy** tab. 4. Check the policies for iOS.
Lock Device	Blocks some functions of the device without locking the device.
Unlock Device	Unlocks a device.
Factory Reset	Performs factory reset and changes the device status to Deactivated.
Reset Screen Password	Resets the device’s screen lock password and creates a temporary password. After sending the device command, the temporary password that can be found on the device’s detailed information page will be delivered to the user. For more information, see the screen lock password in Viewing the device details.
Initialize Blocked Information (Supervised)	Initializes the block settings of the device. **NOTE** Only iOS Supervised devices are supported.

Application (iOS)

Device command	Description
Install	Installs applications on a device. In the “Request Command” window, select an application to install. **NOTE** The Application installation blacklist/whitelist policies take a higher priority than device commands.
Uninstall App	Deletes applications from a device. In the “Request Command” window, select an application to uninstall. **NOTE** The Application uninstallation prevention list setting policy takes a higher priority than device commands.
Apply Latest internal App Information	Sends the latest internal application information and updates the device according to the information.

EMM (iOS)

Device command	Description
Push Notification	Sends an emergency message to the device. The message icon is shown on the status bar of the device. In the “Push Notification” window, enter the title and content of the message.
Deactivate Device	Deactivates a selected device on the device list.
Update User Information	Updates the device user information such as the user activation status/username/user settings (Secure Browser website URL information, bookmark information) and license information. If the user is logged out from the activated device, you can send this device command to enable the user to log in to EMM automatically.
Lock Screen of EMM Client	Locks the EMM Client. When the application is locked, the users have to enter the screen lock password which was configured during installation. If a user forgets the password of EMM Client screen lock, you can send the Delete Account command and make the user logged out from the EMM Client. Then, the user can set the password again upon login.
Unlock EMM Client	Unlocks the EMM Client.
Delete Account	Deletes the account registered in the EMM Client.
Collect Audit Log	Collects the EMM audit logs of the device. When the log size exceeds the maximum size, logs are automatically sent to the server, but the log file may be lost. For more detailed information, see Viewing audits.

Device command	Description
Collect Device Log	Collects the logs of devices.
Collect Diagnosis Information	Collects a device log to diagnose the cause of device lock,
Sync App Auto-removal Property (When service is deactivated)	Syncs the application auto-deletion property when managed applications are deactivated if the value of **Delete app during Unenrollment process** has changed in the server configuration.
Update Terms and Policies	If you change the user terms of the EMM Client app on the EMM Admin Portal, the terms of use will be displayed in a pop-up window so that the user can agree upon logging in again to the EMM Client from the device. If the user agrees to the terms, the policy will be updated, otherwise the EMM Client will no longer be available.

Device Info. (iOS)

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.
Sync Device Information	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the “Device Detail” page. **NOTE** For iOS devices, only the hardware status is updated.
Sync Installed App List	Updates the information of installed applications. For iOS devices, you can also request to delete application feedback when sending the device command. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the “Application” tab.
Check Connection Status	Checks the service connection status of the device. After sending this device command, check the connections status between the device and the server with Keepalive and the last connection time in the device detailed information.
Collect Profile ID	Collects the ID of the profile applied to the device. If the device has been activated, then the ID is automatically collected from the device’s inventory information without sending the device command.

List of device commands: Windows

The available device commands vary depending on device manage type.

Device (Windows)

Device command	Description
Lock Device	Locks the device.
Factory Reset	Performs factory reset and changes the device status to Deactivated.
Reset Screen Password	Resets the device's screen lock password and creates a temporary password. After sending the device command, the temporary password that can be found on the device's detailed information page will be delivered to the user. For more information, see the screen lock password in Viewing the device details.

EMM (Windows)

Device command	Description
Push Notification	Sends an emergency message to the device. The message icon is shown on the status bar of the device. In the "Push Notification" window, enter the title and content of the message.
Deactivate Device	Deactivates a selected device on the device list.
Update User Information	Updates the device user information such as the user activation status/ username/user settings (Secure Browser website URL information, bookmark information) and license information. If the user is logged out from the activated device, you can send this device command to enable the user to log in to EMM automatically.
Lock Screen of EMM Client	Locks the EMM Client. When the application is locked, the users have to enter the screen lock password which was configured during installation. If a user forgets the password of EMM Client screen lock, you can send the Delete Account command and make the user logged out from the EMM Client. Then, the user can set the password again upon login.
Unlock EMM Client	Unlocks the EMM Client.
Delete account	Deletes the account registered in the EMM Client.

Device Info. (Windows)

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.
Sync Device Information	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the "Device Detail" page.
Sync Installed App List	Updates the information of installed applications. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the "Application" tab.

List of device commands: Tizen Wearable

The available device commands vary depending on device manage type.

Device (Tizen Wearable)

Device command	Description
Apply Latest Profiles	Sends the latest profile and application information to the device and controls the device with the profile and information.
Enable EAS (Samsung Email App Only)	Allows using Exchange ActiveSync for Samsung Email application.
Disable EAS (Samsung Email App Only)	Disallows using Exchange ActiveSync for Samsung Email application.
Lock Device	Locks a device. You can enter a reason for locking the device and a phone number to contact when the device is lost. The entered information appears on the locked device screen.
Unlock Device	Unlocks a device.
Factory Reset	Performs factory reset and changes the device status to Deactivated.
Power Off Device	Turns off the device.
Reboot Device	Reboots the device.

Device command	Description
Reset Screen Password	Resets the device's screen lock password and creates a temporary password. After sending the device command, the temporary password that can be found on the device's detailed information page will be delivered to the user. For more information, see the EMM password in Viewing the device details.
Reset SD Card	Initializes the external SD card of the device. **NOTE** For devices whose **External SD Card policy** is set to **Disallowed** in the profile, you cannot reset the SD card using the device command, because the policy takes a higher priority than the device command.

Application (Tizen Wearable)

Device command	Description
Install or Update App	Installs or updates applications on a device. In the "Request Command" window, select an application to be install or update. **NOTE** The Application installation blacklist/whitelist policies take a higher priority than device commands.
Run App	Runs applications on a device. In the "Request Command" window, select an application to run. **NOTE** The Application running blacklist/whitelist policies take a higher priority than device commands.
Stop App	Stops applications on a device. In the "Request Command" window, select an application to stop.
Uninstall App	Deletes applications from a device. In the "Request Command" window, select an application to uninstall. **NOTE** The Application uninstallation prevention list setting policy takes a higher priority than device commands.
Apply Latest internal App Information	Sends the latest internal application information and updates the device according to the information.

EMM (Tizen Wearable)

Device command	Description
Push Notification	Sends an emergency message to the device. The message icon is shown on the status bar of the device. In the “Push Notification” window, enter the title and content of the message.
Deactivate service	Deactivates a selected device on the device list.
Update License	Updates the license of a selected device on the device list.
Update EMM	Updates the EMM Client on the device for a new patch or version. The agent information registered in the EMM server is sent to a device. The device automatically selects the appropriate agent to request installation files from the server.
Update User Information	Updates the device user information such as the user activation status/ username/user settings (Secure Browser website URL information, bookmark information) and license information. If the user is logged out from the activated device, you can send this device command to enable the user to log in to EMM automatically.
Lock Screen of EMM Client	Locks the EMM Client. When the application is locked, the users have to enter the screen lock password which was configured during installation. If a user forgets the password of EMM Client screen lock, you can send the Delete Account command and make the user logged out from the EMM Client. Then, the user can set the password again upon login.
Unlock EMM Client	Unlocks the EMM Client.
Delete Account	Deletes the account registered in the EMM Client.
Collect Audit Log	Collects the EMM audit logs of the device. When the log size exceeds the maximum size, logs are automatically sent to the server, but the log file may be lost. For more detailed information, see Viewing audits.
Collect Device Log	Collects the logs of devices.
Collect Diagnosis Information	Collects a device log to diagnose the cause of device lock,

Device Info. (Tizen Wearable)

Device command	Description
Collect current location	Shows the current location of the device. To view the location of a device after sending a device command, navigate to **Device**, click the checkbox for the device, and then click **Check Location**.
Sync Device Information	Updates the inventory and application information on the device. To view the updated information after sending the device command, navigate to **Device**, click a device name, and view the information on the “Device Detail” page.
Sync Installed App List	Updates the information of installed applications. To view the list of installed applications after sending a device command, navigate to **Device**, click a device name, and click the “Application” tab.
Authenticate SIM Card	Authenticates the SIM card on a device.
Authenticate SD Card	Authenticates the external SD card on a device.

Managing limited enrollment

You can set only the devices that are registered with their IMEI (International Mobile Equipment Identity) numbers to be activated in EMM.

IMEI numbers can be registered individually or collectively using an XLS file. You can also register Wi-Fi only devices with their serial numbers instead of IMEI numbers.

To register IMEI numbers individually, complete the following steps:

1. Navigate to **Setting** > **Android** > **Limited Enrollment**.
2. Click **Activate** next to **Limited Enrollment**.
   - You can also activate the Limited Enrollment feature by navigating to **Setting** > **Server** > **Configuration**, and then setting **Limited Enrollment** to **TRUE**.
3. Click + and select **Add Single Device**.
4. In the “Add Single Device” window, enter an IMEI into the field.
   - Enter the serial number of a Wi-Fi only device.
5. Click **Save**.

To register IMEI numbers collectively, complete the following steps:

1. Navigate to **Setting** > **Android** > **Limited Enrollment**.
2. Click **Activate** next to **Limited Enrollment**.
   - You can also activate the Limited Enrollment feature by navigating to **Setting** > **Configuration**, and then setting **Limited Enrollment** to **TRUE**.
3. Click + and select **Add Multiple Devices**.
4. In the “Add Multiple Devices” window, click **Download Template**.
5. Enter the IMEI numbers in the downloaded XLS file, and then save it.
   - Enter the serial number of a Wi-Fi only device.
6. In the “Add Multiple Devices” window, click **Browse**, and select the saved XLS file.
7. Click **OK**.

NOTE The following types do not support limited enrollment.

- Android Legacy or Non-Samsung devices running Android 10 (Q) or higher
- Work Profile devices running Android 12 (S) or higher

Viewing device logs

View a device log to verify that the device commands sent from the Admin Portal were successfully received by the device.

To view a device log, complete the following steps:

1. Navigate to **Device**.
2. On the “Device” page, click the device to view its log.
3. On the “Device Detail” page, click **Command History**.
4. View the device command history.
    - To download the device logs, click **Device Log**. In the “Device Log” window, set the log collection period and download the desired logs by clicking .
    - To view in detail the audit events that occurred while completing a device command, click **See Audit Event** in the row of the device command.

Checking the locations of the devices

You can check the locations of the selected devices. Only the devices that have the location policy applied can be tracked.

To check the device locations, complete the following steps:.

1. Navigate to **Device**.
2. On the “Device” page, click the device to check the locations.
3. On the “Device Detail” page, click **Device Information**.
4. Click **Detail** next to the Last Location Scanned
5. View the device locations on the “Check Location” window.
    - You can check it on the map only when a value is entered in **Setting** > **Server** > **Configuration** > **Google Maps API Key**.
    - To download the location information, click **Export to GPX**.

5

Application

Application

Manage mobile applications with EMM. Add various types of applications to the application list and assign them to desired mobile devices. Control the settings for the added applications.
For Android Enterprise devices, you can make your company's own exclusive distribution platform by putting the desired applications in Managed Google Play. In addition, you can add iOS applications in bulk through the Apple Volume Purchase Program (VPP). You can also add EMM applications provided by Samsung SDS EMM, such as EMM Client, EMM Agent, Secure Browser, SecuCamera, and Knox Portal.

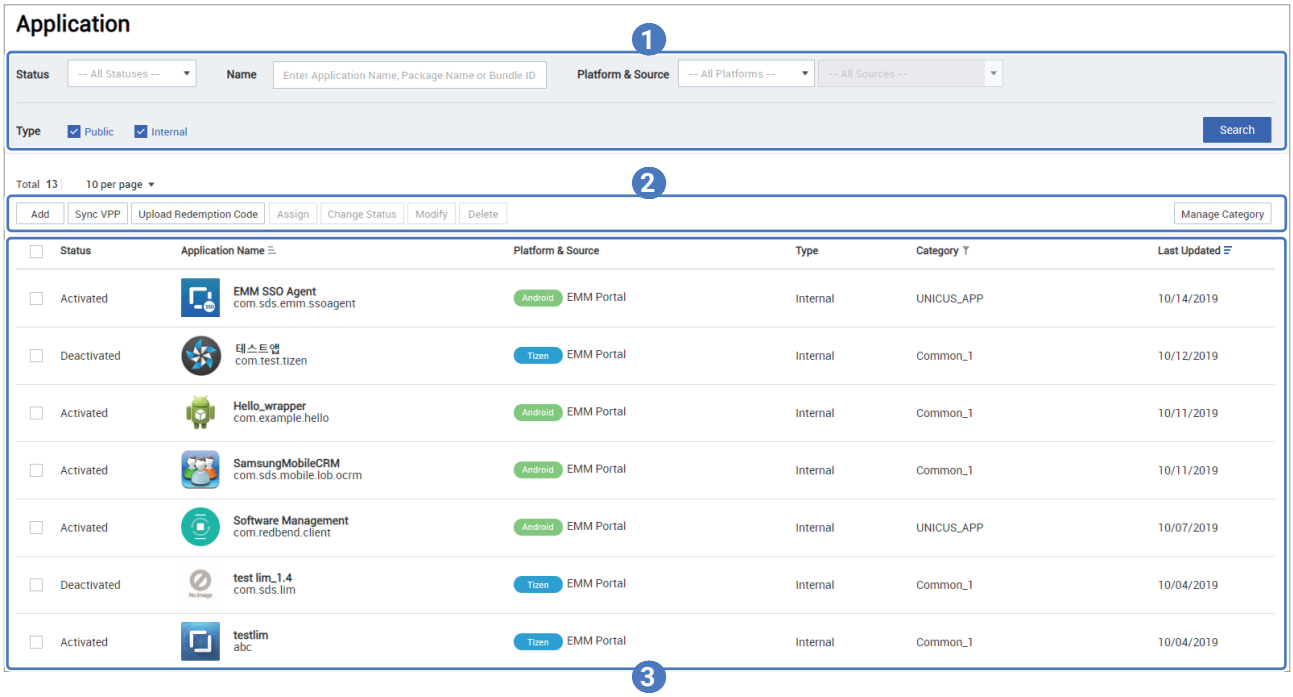
The application types used in EMM are as follows:

Type	Description
Internal applications	An application developed for your company's exclusive use. These applications can be added by uploading APK files for Android devices and IPA files for iOS devices.
Public applications (Google Play Store)	A public application that can be downloaded from Google Play.
Public applications (Managed Google Play Store)	A public application that can be downloaded from Managed Google Play.
Public applications (iOS App Store)	A public application that can be downloaded from iOS App store.
Public applications (Managed Google Play Private)	A private application in Managed Google Play. These applications can be added by uploading the installation files to Managed Google Play.
Public applications (Managed Google Play Private Web)	A web version application that can be downloaded from Managed Google Play.
Public applications (Volume Purchase Program)	A public application that can be purchased from VPP website. These applications can be added by registering the VPP token or uploading redeemable codes.
EMM applications	An application developed by Samsung SDS EMM, such as EMM Client, EMM Agent, Secure Browser, SecuCamera, and Knox Portal.

This chapter explains the following topics:

Viewing the application list

Navigate to **Application** to view all the applications on the “Application” page. You can also perform specific functions for the selected applications on the list.



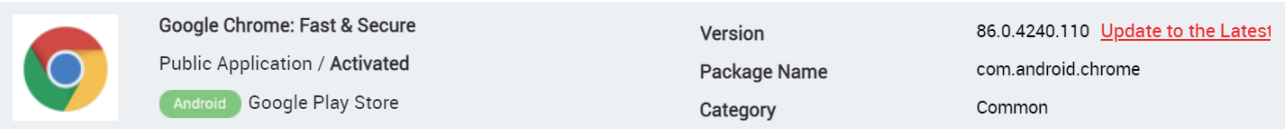
No.	Name		Description
1	Search field		Search for a desired application.
2	Function buttons	Add	Add a public or internal application to the list. For more information, see Adding applications.
		Sync VPP	Synchronize the VPP application data from the VPP website if you purchased the applications through managed distribution. For more information, see Adding VPP applications (managed distribution).
		Upload Redemption Code	Upload the redeemable codes of the VPP applications if you purchased the applications through redeemable codes from the VPP website. For more information, see Adding VPP applications (redeemable codes).
		Assign	Assign and apply the selected applications to group/ organizations. For more information, see Assigning applications.
		Change Status	Activate or deactivate the selected applications. You cannot control deactivated applications unless they are activated.
		Modify	Modify the selected application details. For more information, see Modifying applications.
		Delete	Delete the selected applications. **NOTE** The selected applications can be deleted from both the Admin Portal and user devices if you change the **Manage Deletion** setting in **Setting** > **Server** > **Configuration**. For more information, see Configuring the environment.
		Manage Category	Add a new application category, or delete or modify the existing categories. You can also change the category order. For more information, see Managing application categories. **NOTE** Starting from EMM v2.5.3, Managed Google Play (Store, Private, Web) applications are classified and managed with Collection, the Organize Apps function of Managed Google Play.
		Revert Column Settings	Resets the column settings to the default settings.
3	Application list		View the brief information of the applications on the list.

Viewing the application details

View each application's details by clicking an application name on the application list.

Summary area

The summary area contains the information about the selected application, such as the application name, application type, supported platform, and application version. You can click **Detail** to view more information.



- For public applications, you can click **Update to the Latest Version** to update the application when the latest version of the application is released on the digital distribution platform. Managed Google Play (Store, Private, Web) applications will be automatically updated according to the **Auto Update Mode** set when the applications are assigned.
- For internal applications, you can click **See History** to see the application update history.

Tab: Device

The Device tab shows the list of devices that the application was assigned to. The device list shows the status and name of the device to which application is assigned, IMEI/MEID (additional IMEI is displayed if using Dual SIM), user name, platform and management type, installation status, app version, and the last assignment information. You can check why the application is not installed on the device in the **Install Status** column.

You can perform specific functions on the selected devices among the list. The following function buttons are available:

Function button	Description	Supported application type
Refresh	Update the list of devices.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)

Function button	Description	Supported application type
Install	Install the application directly to the selected devices.	• Internal • Public (Managed Google Play Store) • Public (Managed Google Private) • Public (Managed Google Play Private Web)
Update	Update the internal application directly on the selected devices. To update, the installation file must be replaced with a new one. For more information, see Modifying applications.	• Internal
Uninstall	Remove the application directly from the selected devices.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)

Tab: Assigned Group/Organization

The Assigned Group/Organization tab shows the list of groups and organizations that the application was assigned to. The list of Assigned Group/Organization shows the name of group or organization to which the application is assigned, the type, number of assigned users and devices, device type, and the last assignment information. In the **See Setting** of the Last Assigned column, you can see the Install Area, Install Type, Auto-run after Install, and the Auto Update mode information for each platform assigned to the groups and organizations.

You can perform specific functions on the selected groups and/or organizations on the list. The following function buttons are available:

Function button	Description	Supported application type
Unassign	Unassign applications from groups or organizations.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)
Modify Setting	Modify the assignment settings applied to the selected groups or organizations.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)

Tap: Device/Assigned User/Assigned Group/Organization (For VPP applications)

Displays the devices, users, group, and organizations that VPP applications are assigned to. This tab shows the list of VPP users and devices that the application was assigned to. You can perform specific functions on the selected users on the list. The following function buttons are available:

Function button	Description	Supported application type
Unassign	Unassign applications from users, groups, or organizations.	• Public (Volume Purchase Program)
Modify Setting	Modify the assignment settings applied to the selected groups or organizations.	• Public (Volume Purchase Program)

Function buttons in the footer

You can perform specific functions on the application using the function buttons in the footer. The following function buttons are available:

Function button	Description	Supported application type
Back	Return to the application list.	• All

Function button	Description	Supported application type
Delete	Delete the application from the application list. The application will also be deleted from the devices in the assigned groups/organizations.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)
Modify	Modify the basic information of the application.	• Internal • Public (Google Play Store) • Public (Managed Google Play Store) • Public (iOS App Store) • Public (Managed Google Play Private) • Public (Managed Google Play Private Web)
Install	Install the application directly on the selected devices. You can select the devices to install the application to.	• Internal • Public (Managed Google Play Store) • Public (Managed Google Private) • Public (Managed Google Play Private Web)
Change Status	Activate or deactivate the application.	• All
Assign	Assign the application to groups/organizations/VPP users.	• All

Adding applications

To assign applications to a mobile device, you must first add them to the application list.
For how to add applications by type to the Admin Portal, see below.

Adding internal applications

To add internal applications, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Internal** and click **OK**.
4. On the “Add Application” page, enter the following information. Available items vary depending on the platform.
   - **Platform**: Select the mobile OS.
   - **Application File**: Click  and select either an APK or XAPK file for an Android application or an IPA file for an iOS application.
     - APK files that are 100 MB or smaller can be uploaded. If the file exceeds 100 MB, you can upload a XAPK file, a format consisting of APK and OBB (ZIP, PDF, MP4, etc.) files.

       NOTE
       - When installing the XAPK installation app on devices that are Android Legacy (6.0) and higher or Android Enterprise in Work Profile on company-owned or Work Profile type, the following notifications on acquiring permission will appear according to the file type: The XAPK installation app will be installed via the EMM Extension app.
         - Android Opaque Binary Blob (OBB) file: A notification will appear for permission request during initial installation. After acquiring permission, the notification will not appear.
         - Splits file: A notification for permission request and a pop-up window for installing the application will appear during initial installation. After acquiring permission, only the pop-up window will appear.
       - When installing the XAPK installation app on Android Enterprise devices on a Fully Managed or Fully Managed with Work Profile type, the following notifications on acquiring permission will appear according to the file type: The XAPK installation app will be installed via the EMM Extension app.
         - Android Opaque Binary Blob (OBB) file: A notification will appear for permission request during initial installation. After acquiring permission, the notification will not appear.
         - Splits file: The application will be installed automatically without notifications.

     - When registering a package file, the JPG or PNG icon images in the file can be registered on Android or iOS. And depending on browser supportability, WebP can also be registered.

- **Name**: Enter the application name.
- **Version**: For Tizen Wearable devices, enter the application version.
  For other devices, the retrieved application version is displayed. If there is no value, "-" is displayed.
- **Package Name**: For Tizen Wearable devices, enter the application package name.
  For other devices, the retrieved package name is displayed. If there is no value, "-" is displayed.
- **Managed Configuration**: When uploading a file to add a Managed Google Play (MGP) application as an internal application type, the Managed Configuration (MC) setting availability (Yes/No) is displayed. If you select "Yes," you can enter the MC settings in the application when assigning it. For more information, see Assigning internal applications.
- **Bundle ID**: The retrieved bundle ID for the application is displayed.
- **Bundle Name**: The retrieved bundle name is displayed. If there is no value, "-" is displayed.
- **URL Scheme**: The retrieved URL scheme is displayed. If there is no value, "-" is displayed.
- **Platform & Source**: The application's platform and source are displayed.
- **Type**: The application type is displayed as "Internal."
- **Category**: Select the application category.
  If you click **Manage Category**, you can add or modify application categories.
- **Integrity Validation**: Use a cyclic redundancy check (CRC) that checks the integrity of data sent from applications. A CRC determines the check value used to ensure that there are no errors in the data and sends it along with the data.
- **Auto Update**: Check the application version whenever the EMM Client starts.
  If the application should be updated, a pop-up appears prompting you to begin an update.
- **App Wrapper**: Select **Yes** to wrap the application.
  You can reconfigure the application so that security policies, such as text copy, screen capture, and INI configuration file registration, can be controlled in the Admin Portal. For more information, see Using EMM AppWrapper.
- **Managed App Setting**: Select **Yes** if you are adding an application that is designed to change the Mobile Device Management (MDM) settings of applications on iOS devices. For devices with iOS 7 or higher, the keys or values defined in the Managed App settings can be managed by EMM.
  - **Key & Value**: If you selected **Yes** in **Managed App Setting**, click **Add** and enter the key and value of a MDM setting you want to change. You can add one key and its value at a time.

NOTE Ask the application developers about the key and value for the MDM settings. For example, if you want to add the ManagedAppConfig application and set its default URL to http://www.samsungsds.com, the key is the server URL and the value is http://www.samsungsds.com.

- **Unassign Option**: Click **Uninstall app when unassigned** to delete installed applications from devices when unassigning applications. If the applications are assigned to other groups or organizations, they will not be deleted.

  NOTE The application setting priority is Profile > App assign option > Setting order. In other words, even if the **Uninstall app when unassigned** option is selected, the applications listed in the profile's application uninstallation prevention list cannot be deleted. Also, even if you set the Manage Deletion setting to Console in the Application category of **Setting > Server > Configuration**, the application can be deleted.

- **Description**: Enter a description for the application.
- **Icon**: Select the application icon image.
  - JPG or PNG files under 5MB can be registered, and WebP can also be registered depending on the browser. For the restrictions on the WebP supported browsers, see below.

EMM supported browsers and versions	WebP supported versions
Google Chrome: Chrome 41 and higher	Chrome 32 and higher
Mozilla Firefox: Firefox 37 and higher	Firefox 65 and higher (WebP is not supported in some Firefox versions (37-64))
MS Internet Explorer: Internet Explorer 11	WebP is not supported in IE

- **Screenshot**: Select screenshots of the application to provide a preview for Android device users.

5. Click **Save & Assign** to save the information and proceed to assign the application.
   - Click **Save** to save the information and return to the application list.
     Assign the application. For more information, see Assigning internal applications.

Adding public applications (iOS App Store)

To add public applications via the iOS App Store, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public** and click **OK**.
4. On the “Add Application” page, select **Public - Google Play, iOS App Store** and search for the application you want to add.
   - If you want to change the country of the selected platform, click the checkbox next to **Set Country** and select the country. To check the country set by default, navigate to **Setting** > **Server** > **Configuration** > **Default Country Code**.
5. In the search results, click the application to add.
6. On the “Add Application” page, enter the following information.
   - **Name**: Enter the application name.
   - **Category**: Select the application category. If you click **Manage Category**, you can add or modify application categories.
   - **Description**: Enter a description for the application.
7. Click **Save & Assign** to save the information and proceed to assign the application.
   - Click **Save** to save the information and return to the application list.
     Assign the application. For more information, see Assigning iOS App Store applications.

Adding public applications (Google Play Store)

To add public applications via the Google Play Store, complete the following steps:
Only free applications on the Android Legacy platform provided by the Google Play Store can be registered.

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public - Google Play, iOS App Store** and click **OK**.
4. On the “Add Application” page, select **Google Play Store** and search for the application you want to add.
   - If you want to change the country of the selected platform, click the checkbox next to **Set Country** and select the country. To check the country set by default, navigate to **Setting** > **Server** > **Configuration** > **Default Country Code**.
5. In the search results, click the application to add and then click **Select**.
6. On the “Add Application” page, enter the following information.
   - **Name**: Enter the application name.
   - **Category**: Select the application category. If you click **Manage Category**, you can add or modify application categories.
   - **Unassign Option**: Click **Uninstall app when unassigned** to delete installed applications from devices when unassigning applications. If the applications are assigned to other groups or organizations, they will not be deleted.

     NOTE If **Uninstall app when unassigned** is selected, applications will be deleted from devices even if you set the **Manage Deletion** setting to **Console** in the Application category of **Setting > Server > Configuration**.

   - **Description**: Enter a description for the application.
   - **Additional Languages**: Choose Chinese or Korean and enter a name and description.
7. Click **Save & Assign** to save the information and proceed to assign the application.
   - Click **Save** to save the information and return to the application list.
     Assign the application. For more information, see Assigning Google Play applications.

Adding public applications (Managed Google Play Store)

To add public applications via the Managed Google Play Store, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public - Managed Google Play (Store, Private, Web)** and click **OK**.
4. Select **Search Play Store** from the left button on the “Managed Google Play (Store, Private, Web)” window, enter the application name, and click **Search**.
5. In the search results, click the application to add and then click **Select**.
   - Starting from EMM v2.5.3, the Managed Google Play applications are registered without an application approval procedure.
6. On the “Add Application” page, enter the following information.
   - **Name**: Enter the application name.
   - **Platform & Source**: The application type selected in the “Managed Google Play (Store, Private, Web)” window is displayed.
   - **Unassign Option**: Click **Uninstall app when unassigned** to delete installed applications from devices when unassigning applications. If the applications are assigned to other groups or organizations, they will not be deleted.

     NOTE If **Uninstall app when unassigned** is selected, applications will be deleted from devices even if you set the **Manage Deletion** setting to **Console** in the Application category of **Setting > Server > Configuration**.

   - **Description**: Enter a description for the application.
   - **Managed Configuration**: the Managed Configuration (MC) setting availability (Yes/No) is displayed for the selected Managed Google Play (MGP) application. If you select “Yes,” you can enter the MC settings in the MGP application when assigning it. For more information, see Assigning Managed Google Play applications.
7. Click **Save & Assign** to save the information and proceed to assign the application.
   - Click **Save** to save the information and return to the application list.
     Assign the application. For more information, see Assigning Managed Google Play applications.

Adding public applications (Managed Google Play Private)

To add applications via Managed Google Play Private, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public - Managed Google Play (Store, Private, Web)** and click **OK**.
4. Select **Private apps** from the left button on the “Managed Google Play (Store, Private, Web)” window, and click **+** at the bottom-right corner.
5. Enter the application name, and click **Upload APK** and select the APK file to be uploaded.
6. Click **Create**.
   - The application will appear in the “Managed Google Play (Store, Private, Web)” window.
   - It may take up to 10 minutes for the newly registered Managed Google Play Private applications to appear.
   - Starting from EMM v2.5.3, the Managed Google Play Private applications are registered without an application approval procedure.
7. On the “Add Application” page, enter the following information and click **Save**.
   - You can add a description or screenshots for the application by clicking **Make advanced edits**.
8. To assign applications, navigate to the “Application” page, select the application, and click **Assign**. Assign the application. For more information, see Assigning Managed Google Play Private applications.

Adding public web applications (Managed Google Play Private Web)

Managed Google Play Web applications can be started in Chrome browser, so Chrome browser must be registered and approved on the Admin Portal to use these web applications.

To register web applications, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public - Managed Google Play (Store, Private, Web)** and click **OK**.
4. Select **Web apps** from the left button on the “Managed Google Play (Store, Private, Web)” window, and click **+** at the bottom-right corner.
   - **Title**: Enter the web application name. Entering the same name as the application name of the Managed Google Play Store is recommended.
   - **URL**: Enter the Google Play Store URL of the web application.
   - **Display**: Select how to display the web application on the device screen.
   - **Icon**: Upload an icon image for the web application.
5. Click **Create**.
   - The application will appear in the “Managed Google Play (Store, Private, Web)” window.
   - It may take up to 10 minutes for the newly registered Managed Google Play Web applications to appear.
   - Starting from EMM v2.5.3, the Managed Google Play Web applications are registered without an application approval procedure.
6. To assign applications, navigate to the “Application” page, select the application, and click **Assign**. Assign the application and Chrome browser to devices on the “Assign Application” page. For more information, see Assigning Managed Google Play web applications.

Managing applications with Collection

Configure and manage the Managed Google Play (Store, Private, Web) applications with Collection. The applications configured with Collection, the Organize Apps function of Managed Google Play, can be viewed in the Play Store on the user device. Applications other than Managed Google Play (Store, Private, Web) are managed in categories in the existing method. See Managing application categories for more information, see Managing application categories.

To configure the Managed Google Play (Store, Private, Web) applications as a Collection, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Add**.
3. In the “Select Application Type” window, select **Public - Managed Google Play (Store, Private, Web)** and click **OK**.
4. Select **Organize apps** from the left button on the “Managed Google Play (Store, Private, Web)” window, and click **+ Create a collection**.
5. Enter the Collection name in the Add a name field and click **Next**.
6. Search and select the application you want to add to the Collection and click **Add apps**.
   - The selected Collection and applications will be displayed in the “Managed Google Play (Store, Private, Web)” window.
7. Modify the Collection name, delete and copy Collection, or add and delete applications from the Collection by completing one of the following actions.
   - To change the Collection name, delete or copy the Collection, click the buttons next to the Collection name to execute the task.
   - To add applications to the Collection, click **+ Add apps**.
   - To delete applications added to the Collection, click **X** in the upper-right corner of the application.
8. Click **Save** when Collection creation is complete.
   - Only applications that are approved by the company can be added to Collection through the Organize Apps menu. If the application does not appear in the Organize Apps menu, you can directly approve the application at https://play.google.com/work.

Adding EMM applications

The EMM applications are consist of EMM Client (can be varied depending on OS platform or version such as EMM Agent, EMM Wearable Agent), Secure Browser, SecuCamera, Kiosk Browser and Knox Portal application delivered with installation package file.

You can add EMM applications via **Setting** > **EMM Application and Policy** > **EMM Application**. The EMM application registered are automatically saved as controlled applications since these are prohibited from deletion. For more information about setting policies for EMM applications, see Managing message templates.

NOTE When registering or modifying the application, the package name of the installation file must be the same as the package name in **EMM PackageName** found in **Setting** > **Server** > **Master Data**. If the Package name is different, a message will appear indicating that the file is invalid. To use a different package name, you must modify the EMM PackageName value in **Master Data**. For more information, see Managing master data.

When registering EMM applications, there are the following restrictions for each platform:

- EMM Agent: Agent application can be registered for each Android type, one Agent application for Tizen Wearable can be registered.
  - When the Tizen Wearable Agent is registered, the package name should be “com.sds.emm.wearable.”
- EMM Client: Client applications for Android, iOS, and Windows can be registered one each.
  - In case you are using separate packages for the EMM Client and Agent, a client should beregistered for Android devices.
- One EMM Push Agent for Android can be registered.
  - EMM Push Agent must be registered in the EMM application menu.
- Secure Browser: One application can be registered both for Android and iOS.
- Kiosk Browser: One application for Android can be registered.
- SecuCamera: One application for Android can be registered.
- Knox Portal(Agent, UI): One application can be registered for Agent and UI applications for Android.

To add an EMM application, complete the following steps:
EMM applications are automatically classified and registered as EMM or SYSTEM, depending on the type.

1. Navigate to **Setting** > **EMM Application and Policy** > **EMM Application**.
2. Click **Add** > **Newly Register**.
3. In the "Add EMM Application" window, enter the following information. Available items vary depending on the platform.
   - **Classification**: Select the classification of the application that you want to add.

NOTE You can only select the EMM application's classifications that you have not registered yet.

   - **Platform**: Select the platform that can be entered according to the selected classification.
   - **Application Name**: Once you have selected the classification, the EMM application name will be automatically entered. You can also modify the entered application name.
   - **Installation File**: Click  and select either an APK file for an Android application or an IPA file for an iOS application.
   - **Version**, **Package name** for Android, **Bundle ID** for iOS
     - If you have selected an APK file, its information, such as its platform, package name, and version, is entered automatically.
     - When you enter the iOS Secure Browser, you must enter the URL scheme.
   - **Others**: If you enter a test application, click **No integrity validation**.
     - **No integrity validation**: If you select this option, a cyclic redundancy check (CRC), which checks the integrity of data sent by apps, will not be performed. A CRC determines the check value used to ensure that there are no errors in the data sent through a network, etc., and then sends it along with the data.
     - When you click **Auto update**, the versions of the device's applications are checked and the user is notified of the latest versions.
4. Click **Save**.

Adding Tizen Wearable applications

Add and deploy applications for Tizen wearables in the Samsung Gear App Store. To add and deploy an application for Tizen wearables in the Admin Portal, you must first register the application in the Samsung Gear App store; the approval period may take some time. Aside from store registration, if you want to install a standalone application on a Tizen wearable device without pairing a mobile device, you need Stub API authority for the application.

To add the Tizen Wearable application, complete the following steps:

1. Navigate to **Application**.
2. On the "Application" page, click **Add**.
3. In the "Select Application Type" window, select **Internal** and click **OK**.
4. On the "Add Application" page, enter the following information:
   - **Platform**: Select **Tizen Wearable**.
   - **Name**: Enter the application name.
   - **Version**: Enter the application version
   - **Package Name**: Enter the application package name. The entered application package name must be identical to the package name of the application registered on the Samsung Gear App Store.
   - **Platform & Source**: The application's platform and source are displayed.
   - **Type**: The application type is displayed as "Internal."
   - **Icon**: Select the application icon image.
5. Click **Save & Assign** to save the information and proceed with assigning the application.
   - Click **Save** to save the information and return to the application list.
6. In the "Save & Assign" window, click **OK**. Assign the application to the group or organization. For more information, see Assigning internal applications.

NOTE

- If the registered application has no Stub API authority, a notification saying that you need a Samsung account to install an application will appear. If this happens, contact the Samsung Gear App Store's Technical Support.
- The Tizen Wearable devices support the following modes. For a better B2B environment, using Standalone mode is recommended.
  - Standalone mode: Allows factory-reset Tizen Wearable devices to be used without pairing with mobile devices via Bluetooth.
  - Companion mode: Set by Gear Manager through pairing with mobile devices via Bluetooth.

Assigning applications

Assign the applications registered in the EMM Admin Portal to mobile devices. When an application is deployed to a device, the application is automatically installed or the user can manually install it, or the application can be installed by sending device commands. For more information, see Sending device commands to devices. For how to assign applications by type to mobile devices, see below.

NOTE

- The applications can be assigned to groups or organizations. The application assigned to the parent organization is not inherited, so it must be additionally assigned to the sub-organizations.
- To apply the latest managed configuration of the app to the devices in bulk, send Apply the Latest App Managed Configuration device command. For more information, see Sending device commands to devices.
- Applications can be redundantly assigned to users belonging to a group or organization.

Assigning internal applications

To assign added internal applications, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.
3. On the “Assign Application” page, configure the assignment settings. Available items vary depending on the platform.
   - **Target Device**: For Android internal applications, select the target device type. The installation type may be designated depending on the target device type.
   - **Install Area**: Select the area where the application will be installed.
     - Android Enterprise: The designated installation area based on the device type is displayed.
     - Android Legacy: For Android Legacy with Knox Workspace devices, select the areas to install the application.
   - **Install Type**: Select the installation type. Users can choose to manually install the application directly on the device or install it automatically.
     To install apps in Knox container and Work profile, OS version should be Android 6.0 (Mashmallow) or higher.
     - **Manual**: This type requires users to install the application themselves from the EMM app store.
     - **Automatic (Removable)**: Set the application to be installed automatically. Users are allowed to remove the application.

- **Automatic (Non-removable)**: Set the application to be installed automatically. Users are not allowed to remove the application.

> **NOTE** The application auto installation feature is not supported in the following cases:
>
> 1. When devices are activated with the KPE Standard license (Restriction on Knox API)
> 2. In case of an XAPK application with the following attributes (restriction based on XAPK attributes):
>
> - The application consists of Split APK files.
> - The application includes OBB files.

- **Text copy**: Allow users to copy text in the application.
- **Screen capture**: Allow users to capture screens in the application.
- **Printing (iOS)**: Allow users to print the application screens.
- **Share list (iOS)**: Allow users to use sharing features while using the application.
- **Configuration File**: Set whether to apply the settings INI file to the app. It is applicable only when you have selected to use the AppWrapper when you registered the application, and it is also allowed to send policies of INI file format to the app-wrapped application. For more information about App Wrapper, see Using EMM AppWrapper.

> **NOTE** The INI file for the app-wrapped application can be updated in **Application > Application Detail > Assigned Group/Organization > Modify Setting > Configuration File**, and the changed INI file will be applied to the application.

- **Auto-run after Install**: Set to start the application immediately after installation.
- **Home Screen Shortcut (Samsung device only)**: Add a shortcut for the application on the Home screen of the device.

> **NOTE** Once users delete the shortcut, it will not be added again.

- **Use Deployment Scheduler**: Schedule the time for assigning the application. The distribution scheduler can be applied only on Android Enterprise devices.
- **Deployment Starts by**: Set the time to start assigning the application.
- **Managed Configuration**: Click **Set Configuration** to configure the Managed Configuration (MC) settings in the Managed Google Play (MGP) application. This option can only be set on Android Enterprise devices. If you have previously set the MC, the MC setting items will appear in the “Managed Configuration” window, and the items can be displayed in various languages other than those set in the Admin Portal.

- Set the items in the “Managed Configuration” window and click **Save**. You can click **Lookup** and select the values for the items from the “Set Lookup Item” window.

  NOTE
  - The MC settings of the application is applied when assigning, installing, and updating the application, and can also be applied by sending the **Apply the Latest App Managed Configuration** device command.

4. Select the target type. Search for the target groups/organizations and click the checkbox for the groups/organizations to assign.
5. Click **Assign**.
6. In the “Assign Application” window, view the assignment information and click **OK**.

Assigning iOS App Store applications

To assign the added applications via the iOS App Store, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.
3. On the “Assign Application” page, configure the assignment settings.
   - **Target Device**: The target device type is designated as iOS.
   - **Install Type**: Select the installation type.
     - **Manual**: Allow users to install the application manually.
     - **Automatic (Removable)**: Set the application to be installed automatically. Users are allowed to remove the application.
4. Select the target type. Search for the target groups/organizations and click the checkbox for the groups/organizations to assign.
5. Click **Assign**.
6. In the “Assign Application” window, view the assignment information and click **OK**.

Assigning Google Play applications

To assign the added applications via the Google Play Store, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.

3. On the “Assign Application” page, configure the assignment settings.
   - **Target Device**: The target device type is designated as Android Legacy.
   - **Install Area**: The designated installation area is displayed.
   - **Install Type**: The installation type is designated as manual. Device users will install the application manually.
   - **Auto-run after Install**: To start the application immediately after installation, select **Yes**.
4. Select the target type. Search for the target groups/organizations and click the checkbox for the groups/organizations to assign.
5. Click **Assign**.
6. In the “Assign Application” window, view the assignment information and click **OK**.

Assigning Managed Google Play applications

To assign the added applications via the Managed Google Play Store, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.
3. On the “Assign Application” page, configure the assignment settings.
   - **Target Device**: Select the target device type.
   - **Install Area**: The designated installation area is displayed.
   - **Install Type**: For Android Legacy devices, the installation type is designated as manual. For Android Enterprise devices, you can select the installation type.
     - **Manual**: Allow users to install the application manually.
     - **Automatic (Removable)**: The applications will be automatically installed only once.
       If the applications are installed on the device by selecting the Automatic (Removable) option, the applications cannot be reinstalled if the user deletes them from the device.
       If you want the applications to be reinstalled even if you delete them from the device, you must assign the applications by selecting Automatic (Non-removable) or manually install them from the Play Store.
     - **Automatic (Non-removable)**: The applications will be automatically installed and the applications will be automatically reinstalled if the user deletes them from the device.

     NOTE To install apps in Knox container and Work profile, OS version should be Android 6.0 (Mashmallow) or higher.

   - **Auto-run after Install**: To start the application immediately after installation, select **Yes**.

- **Auto Update Mode**: Select the application Auto Update Mode. The applications will be automatically updated depending on the selected mode.
  - **Default Update**: The applications will be automatically updated if they meet the following conditions:
    When the device is connected to Wi-fi, when the device is charging, when the device usage is not frequent, and when the application to be updated is not running in the foreground.
  - **High Priority**: Applications with high priority will be updated when updating the applications.
  - **Postponed (90 Days)**: Postpone the application update for 90 days. After 90 days, the applications will be automatically updated according to the default mode.
- **Managed Configuration**: Click **Set Configuration** to configure the Managed Configuration (MC) settings in the Managed Google Play (MGP) application. This option can only be set on Android Enterprise devices. If you have previously set the MC, the MC setting items will appear in the "Managed Configuration" window, and the items can be displayed in various languages other than those set in the Admin Portal.
  - Set the items in the "Managed Configuration" window and click **Save**. You can click **Lookup** and select the values for the items from the "Set Lookup Item" window.
  - If you have previously set the MC in the application, you can select the setting type. In the "Select Configuration Type" window, select Previous Configuration (iFrame) or New Configuration (Custom UI) and click **OK**. If you have previously selected the iFrame type, you can select the iFrame or Custom UI type. If you have selected the Custom UI type, you can only set the Custom UI type.

    NOTE
    - For users who belong to both groups A and B, if the MC is set differently in the application with the iFrame type for Group A and the Custom UI type for Group B, the most recently deployed MC settings will be applied to the device.
    - The MC settings of the application is applied when assigning, installing, and updating the application, and can also be applied by sending the **Apply the Latest App Managed Configuration** device command.

4. Select the target type. Search for the target groups/organizations and click the checkbox for the groups/organizations to assign.
5. Click **Assign**.
6. In the "Assign Application" window, view the assignment information and click **OK**.
7. In the "Assign Application" window, view the assignment information and click **OK**.

Assigning Managed Google Play Private applications

To assign the added public applications via Managed Google Play Private, complete the following steps:

1. Navigate to **Application**.

2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.
3. On the “Assign Application” page, configure the assignment settings.
   - **Target Device**: The target device type is designated as Android Enterprise.
   - **Install Area**: The area of the devices where the application will be installed is displayed as **Each Enrolled Area**.
   - **Install Type**: Select the installation type.
     - **Manual**: Allow users to install the application manually.
     - **Automatic (Removable)**: The applications will be automatically installed only once.
       If the applications are installed on the device by selecting the Automatic (Removable) option, the applications cannot be reinstalled if the user deletes them from the device.
       If you want the applications to be reinstalled even if you delete them from the device, you must assign the applications by selecting Automatic (Non-removable) or manually install them from the Play Store.
     - **Automatic (Non-removable)**: The applications will be automatically installed and the applications will be automatically reinstalled if the user deletes them from the device.
   - **Auto-run after Install**: To start the application immediately after installation, select **Yes**.
   - **Auto Update Mode**: Select the application Auto Update Mode. The applications will be automatically updated depending on the selected mode.
     - **Default Update**: The applications will be automatically updated if they meet the following conditions:
       When the device is connected to Wi-fi, when the device is charging, when the device usage is not frequent, and when the application to be updated is not running in the foreground.
     - **High Priority**: Applications with high priority will be updated when updating the applications.
     - **Postponed (90 Days)**: Postpone the application update for 90 days. After 90 days, the applications will be automatically updated according to the default mode.
4. Select the target type. Search for the target groups/organizations and click the checkbox for the groups/organizations to assign.
5. Click **Assign**.
6. In the “Assign Application” window, view the assignment information and click **OK**.

Assigning Managed Google Play web applications

You can assign web applications registered in Managed Google Play to user devices. Managed Google Play web applications can only be started in Chrome browser, so Chrome browser must be assigned to the devices you want to assign the web applications.

To assign web applications, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be assigned and click **Assign**.
3. On the “Assign Application” page, configure the assignment settings.
   - **Target Device**: The target device type is designated as Android Enterprise.
   - **Install Area**: The area of the devices where the application will be installed is displayed as **Each Enrolled Area**.
   - **Install Type**: Select the installation type.
     - **Manual**: Allow users to install the application manually.
     - **Automatic (Removable)**: The applications will be automatically installed only once.
       If the applications are installed on the device by selecting the Automatic (Removable) option, the applications cannot be reinstalled if the user deletes them from the device.
       If you want the applications to be reinstalled even if you delete them from the device, you must assign the applications by selecting Automatic (Non-removable) or manually install them from the Play Store.
     - **Automatic (Non-removable)**: The applications will be automatically installed and the applications will be automatically reinstalled if the user deletes them from the device.
   - **Auto-run after Install**: To start the application immediately after installation, select **Yes**.
   - **Auto Update Mode**: Select the application Auto Update Mode. The applications will be automatically updated depending on the selected mode.
     - **Default Update**: The applications will be automatically updated if they meet the following conditions:
       When the device is connected to Wi-fi, when the device is charging, when the device usage is not frequent, and when the application to be updated is not running in the foreground.
     - **High Priority**: Applications with high priority will be updated when updating the applications.
     - **Postponed (90 Days)**: Postpone the application update for 90 days. After 90 days, the applications will be automatically updated according to the default mode.
   - **Chrome App Settings**: Managed Google Play Web applications can be started in Chrome browser. To assign Chrome browser to the groups or organizations with the web applications, select **Yes**. If Chrome browser is not installed on the devices, the web applications will be started through the default browser on the devices.
     - If you select **Yes**, set the Install Type, Auto-run after Install, and Managed Configuration option on the Chrome browser.
4. Select the target groups or organizations to assign the applications and click **Assign**.
5. In the “Assign Application” pop-up window, view the assignment information and click **OK**.

Managing applications

Modify the registered applications in EMM. You can also categorize the applications and customize the categories.

Modifying applications

To modify the basic information of applications, such as the name and category, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to be modified and click **Modify**.
3. On the “Modify Application” page, modify the basic information.
   - For internal applications, you can change the installation file for updating.
4. Click **Save**.
5. In the “Save Changes” window, click **OK**.
   - If you changed the installation file for updating, you can enter your comment for the update history. After saving the comment, you can also send an update request to the users who have installed the application.

Deleting applications

To delete the applications, complete the following steps: You can delete applications registered in Admin Portal. Depending on the **Manage Deletion** setting from **Setting** > **Server** > **Configuration**, applications can be deleted from both console and devices.

1. Navigate to **Application**.
2. On the “Application” page, click the checkbox for the applications to delete and click **Delete**.
3. In the “Delete Application” window, click **OK**.
   - The application will be removed from all assignment.

NOTE To delete EMM applications, navigate to **Setting** > **EMM Application and Policy** > **EMM Application** and click 🗑. However, if a profile configured and assigned with the EMM application to delete, you cannot delete the application.

Managing application categories

If you register application categories, applications will be displayed in categories on the mobile devices. Add new categories or modify the existing categories for classifying applications. Starting from EMM v2.5.3, Managed Google Play (Store, Private, Web) applications are classified and managed with Collection, the Organize Apps function of Managed Google Play. The applications configured with Collection can be viewed in the Play Store on the device. For more information, see Managing applications with Collection.

Adding categories

To add a new category, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Manage Category**.
3. In the “Manage Category” window, click **Add**.
4. In the “Add Category” window, enter the following information:
   - **Name**: Enter the category name. It can be written in English, Korean, or Chinese.
   - **Description**: Enter a description for the category.
5. Click **Save**.

NOTE

- Up to 15 categories can be added and up to 100 applications can be registered in each category.
- A new category is added as the last in the order. If you do not set the category when adding an application, the application will be in the Common category.

Changing the category order

To rearrange the category, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Manage Category**.
3. In the “Manage Category” window, select one or more categories to be moved and click ↓ or ↑.
4. Click **Save**.
5. In the “Save Changes” window, click **OK**.

Modifying categories

To modify an existing category, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Manage Category**.
3. In the “Manage Category” window, select a category to be modified and click **Modify**.
4. In the “Modify Category” window, modify the existing information.
5. Click **Save**.

Deleting categories

To delete an existing category, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Manage Category**.
3. In the “Manage Category” window, select a category to be deleted and click **Delete**.
4. In the “Delete Category” window, click **OK**.

Using EMM AppWrapper

If you use the EMM AppWrapper, you can add security policies, such as screen lock, text copy, and screen capture lock. It also reconfigures the application by adding codes that can control the security policies without editing the source codes of the application. Therefore, it has the advantage of enabling adding new features without any platform development knowledge.

Please note the following when using EMM AppWrapper:

- When using the EMM AppWrapper, app wrapping is limited to internal applications. There may be copyright issues when converting public applications.
- The security logic application that checks the signing key may not function normally.
- The kiosk conversion function and app wrapping function cannot be used simultaneously.

Features of the EMM SDK that are supported by the EMM AppWrapper include: user authentication, screen lock, text copy, and screen capture lock. On the user device, the existing internal application and the wrapped internal application are differentiated with icons but can both be used. You can also register the required INI file for the app-wrapped application in the Admin Portal. If you register the INI file when assigning the application to the device, the INI file is saved in the device's data storage. For more information, see Assigning internal applications. For registering the required source codes to read the INI file in the application when registering the INI file, see Reading the configuration file.

The default package name is automatically assigned when the application is wrapped and can be changed by the IT admin. When you change the package name, the App wrapping does not finish normally in the following cases:

- If the package name is hard-coded in the application source
- If the application includes an INI file
- If multiple application rights are assigned to the IT admin

For how to install the EMM AppWrapper to the IT admin's PC other than using the AppWrapper provided in the Admin Portal and using additional features, see EMM AppWrapper in the Appendix.

Reading the configuration file

To register the INI configuration file to an internal application, search for the path and file name of the configuration file and register the sources for reading the strings as below. For more information and the code samples of the configuration file, see the Samsung SDS Developer Manual.

Below are the code examples for reading the configuration file:

```
private String readINIFile(String fileName) throws FileNotFoundException,
IOException, Exception
{
StringBuffer sb = new StringBuffer();
BufferedReader br = null;
int ch = 0;
br = new BufferedReader(new FileReader(fileName));
while((ch = br.read()) != -1) {
sb.append((char) ch);
    }
br.close();

return sb.toString();
}

// Path : /data/data/[packagename]/files/ini
private String getINIFolder(Context context)
{
   return context.getFilesDir() + File.separator + "ini";
}

// ini File Name : [packagename].ini */
private String getINIFileName(Context context)
{
   return context.getPackageName() + "." + "ini";
}
```

- The `getINIFolder` function searches for the directory path where the configuration file is saved.
- The `getINIFileName` function searches for the name of the `{PackageName}.ini` file.
- The `readINIFile` function reads the configuration file through the file path received as a parameter value, and then sends a text value.

Below are the code examples to judge the existence of the file and call the `readINIFile()` function.

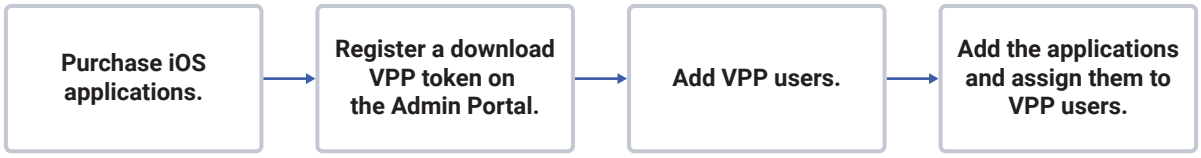
```
btnIniRead.setON-CLICKListener(new ON-CLICKListener() {
   @Override
   public void ON-CLICK(View v) {
      String text = null;

      String filePath = getINIFolder(mContext) + File.separator +
getINIFileName(mContext);
      File file = new File(filePath);
      if(file.exists())
      {
         try {
            text = readINIFile(filePath);
         } catch (FileNotFoundException e) {
            text = "FileNotFoundException";
            e.printStackTrace();
         } catch (IOException e) {
            text = "IOException";
            e.printStackTrace();
         } catch (Exception e) {
            text = "Exception";
            e.printStackTrace();
         }
      }
      else
      {
         text = "File Not Found";
      }
      editIniRead.setText(text);
   }
});
```

- The full path where a configuration file can be saved: `getINIFolder(mContext) + File.separator + getINIFileName(mContext)`

Using the Volume Purchase Program (iOS only)

The Apple Volume Purchase Program (VPP) enables the buying and uploading of iOS applications in bulk and lets you easily deploy the applications to iOS device users. You can add the applications purchased on the VPP website to the EMM Admin Portal and deploy them to iOS device users or devices. For more information about the Apple VPP, see https://www.apple.com/business/vpp/ or the Apple VPP guide (https://images.apple.com/business/docs/VPP_Business_Guide.pdf).

To add applications through the VPP, the following procedures must be performed.



Before using the VPP

Verify the following prerequisites before using the Apple VPP.

- Make sure that the Apple VPP is available in your country. For more information about VPP availability, see https://support.apple.com/en-us/HT207305.
- Make sure that your organization has an Apple Business account. If not, create an account at https://business.apple.com.
- The VPP applications can be assigned to the devices running iOS 7.0 or higher, or macOS 10.9 or higher.

NOTE The VPP website (http://deploy.apple.com) has been incorporated into the Apple Business Manager website (https://business.apple.com) as of December 1, 2019. Upgrade to the Apple Business Manager website.

Distribution method of application

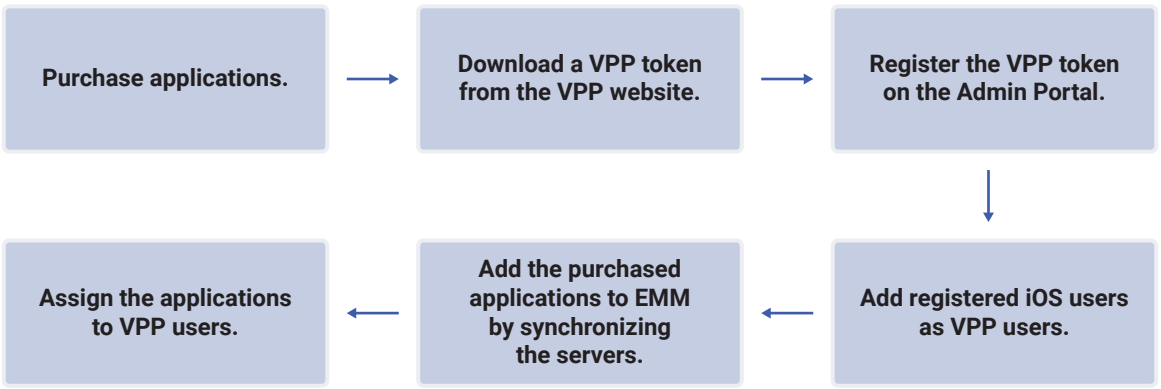
When you purchase applications through the VPP website, you must deploy the applications by one of the following methods. EMM recommends using the managed distribution method.

- Method of managed Distribution
- Method of redeemable Codes

Managed Distribution

If you use managed distribution, the VPP applications are synchronized and added to EMM Admin Portal when you register a VPP token on the EMM Admin Portal. You can assign, unassign, and reassign the VPP applications to users and devices. Upon a change in the application assignment, the application information and total number of license codes will be updated automatically.

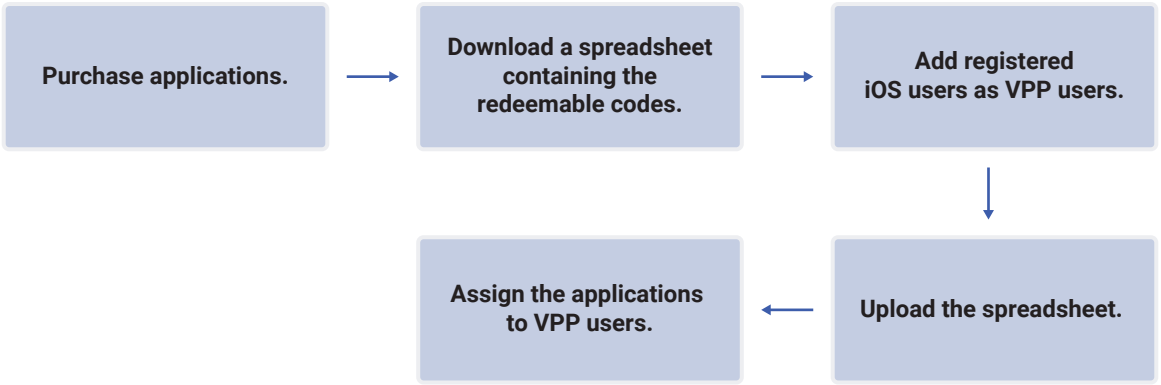
To add purchased applications through managed distribution, the following procedures must be performed.



Redeemable Codes

The applications will be added to EMM when you upload the spreadsheet containing the redeemable codes for the purchased applications on the Admin Portal. The spreadsheet is downloaded after purchase. Once you assign the VPP applications to users, you cannot unassign or reassign them.

To add purchased applications through redeemable codes, the following procedures must be performed.



Purchasing applications on the VPP website

To purchase applications on the VPP website, complete the following steps:

1. Visit the Apple Business Manager website (https://business.apple.com).
2. Sign in to the website using your Apple Business account.
3. Search for and click the application you want to buy.
4. Enter the application quantity and select the distribution method.
   - **Managed Distribution**: Add the application by registering a VPP token. For more information, see Managed Distribution.
   - **Redeemable Codes**: Add the application by uploading a redeemable code. For more information, see Redeemable Codes.
5. Purchase the application.
   - If you buy a paid application, use your VPP Credit or a credit card to pay for it.

Setting up the VPP

To use the VPP service through managed distribution, register the VPP token downloaded from the VPP website in the Admin Portal. A VPP token functions as a link between the VPP website and EMM, and can be renewed on a yearly basis. Thirty days prior to the expiration date a pop-up alert will appear reminding you to renew the token.

NOTE If you purchase applications through redeem code, you do not have to register the VPP token on the EMM Admin Portal.

Downloading the VPP token from the VPP website

To download a token on the VPP website, complete the following steps:

1. Sign in to the Apple Business Manager website (https://business.apple.com) using your Apple Business account.
2. Click **Apps and Books** and download the token.

Registering the VPP token

To register the downloaded token on the Admin Portal, complete the following steps:

1. Navigate to **Setting** > **iOS** > **VPP Server Setting**.
2. On the “VPP Server Setting” page, click **Browse** and select the downloaded token file.
3. Click **Upload**.
   - When the upload is finished, VPP integration will be complete and the VPP applications will be added to the application list in the Admin Portal.
4. Enter the interval at which the VPP server will be synced to the EMM server and click **Setting**.
   - You can enter an interval from 0 to 120 hours. The VPP users and the application are synced according to the interval.

Managing VPP users

VPP applications can be assigned to the iOS devices or VPP users.
To assign the VPP applications to VPP users, you must add iOS users enrolled on the EMM Admin Portal as VPP users. If you assign the applications to iOS devices, you do not need to enroll VPP users.
If there are VPP users who are registered but did not accept the invitation on their devices, you can resend the invitation message. When VPP users are removed or their statuses are changed on the Admin Portal, you can synchronize the user information with the VPP website.

Status of VPP users

The VPP users’ statuses are divided into three types. The VPP users can be checked under **Setting** > **iOS** > **VPP User Management** in the Admin Portal.

- Registered: The user is registered as a VPP user.
  A VPP invitation has been sent to the user, but the user has not yet accepted the invitation.
- Associated: The user is registered as a VPP user and has accepted the invitation.
  The user’s device is associated with the user’s Apple account. Apple gives the user a VPP Client user ID, which allows them to use the assigned applications.
- Retired: The user has been removed from the VPP user list on the Admin Portal.
  The user information is no longer visible in the Admin Portal but remains on the VPP website.

Adding VPP users

Add the users of activated iOS devices as VPP users. The users will be registered on the VPP website as well as the Admin Portal.

To add VPP users, complete the following steps:

1. Navigate to **Setting** > **iOS** > **VPP User Management**.
2. On the “VPP User Management” page, click  .
3. In the “Add VPP User” window, select the users you want to add.
4. Click **Save**.
   - The invitation message is sent to the users through notifications or email. If the users accept this invitation, they will be added to **Setting > iOS > VPP User Management**.

Reinviting VPP users

Send another invite to the users who have not accepted the invitation yet.

To send an invitation message, complete the following steps:

1. Navigate to **Setting** > **iOS** > **VPP User Management**.
2. On the “VPP User Management” page, click the checkboxes for the users with a registered status you want to invite.
3. Click  .
4. In the “Invite” window, click **OK**.

Removing VPP users

To remove VPP users, complete the following steps:

1. Navigate to **Setting** > **iOS** > **VPP User Management**.
2. On the “VPP User Management” page, click the checkboxes for the users you want to remove.
3. Click  .
4. In the “Remove” window, click **OK**.
   - The selected users are removed from **Setting > iOS > VPP User Management**.

Synchronizing VPP user information

There are two ways of syncing the VPP users of the VPP website and the VPP users of the Admin Portal.

- Automatic synchronization via scheduling in **Setting** > **iOS** > **VPP Server Setting**
- Manual synchronization

To synchronize the user information manually, complete the following steps:

1. Navigate to **Setting** > **iOS** > **VPP User Management**.
2. On the “VPP User Management” page, click  .

Managing VPP applications

Assign the applications registered through the managed distribution or the redeem codes to the iOS devices or VPP users. Applications registered with managed distribution can be unassigned from a VPP user and then reassigned to another VPP user. Applications registered with redeem codes cannot be unassigned or reassigned. When unassigning VPP applications, the licenses will also be retrieved.

Adding VPP applications (managed distribution)

There are two ways of syncing the VPP applications purchased from the VPP website and the VPP applications of the Admin Portal.

- Automatic synchronization via scheduling in **Setting** > **iOS** > **VPP Server Setting**
- Manual synchronization

To synchronize the applications manually, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Sync VPP**.
3. In the “Sync VPP” window, click **OK**.

Adding VPP applications (redeemable codes)

Add the purchased applications through redeemable codes by uploading the code spreadsheet on the Admin Portal.

To upload the redeemable codes, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, click **Upload Redemption Code**.
3. In the “Upload Redemption Code” window, click  and select the code spreadsheet downloaded from the VPP website.
4. View the code list and click **Save**.

Assigning a VPP application

Assign the registered VPP application to iOS devices or VPP users. Assigning multiple VPP applications (up to 10) is allowed only when VPP applications are assigned to iOS devices. In this case, you can view the application list to be assigned by clicking **See Other Apps** on the “Assign Application” page. For more information, see Assigning multiple VPP applications.

To assign a VPP application to iOS devices or VPP users, complete the following steps:

1. Navigate to **Application**.
2. On the “Application” page, search for the application you want to assign.
   - To search, enter the name or select the **iOS** for platform and **Volume Purchase Program** for source and click **Search**.
3. Click the checkbox for the application, and then click **Assign**.
4. On the “Assign Application” page, configure the assignment settings.
   - **Assignment Type**: Set the assignment type of the application. You can assign the application by devices or users.
     - **Device (Recommended)**: Assign the VPP application to devices. If you select this, you can set the installation type as manual or automatic.
     - **User**: Assign the VPP application to users. If you select this, you can set the installation type as follows. The VPP applications added through redeem codes can be assigned to users only.
       - **Registered**: The VPP application must be installed manually.
       - **Associated**: The VPP application will be installed automatically.

- **Install Type**: If you selected **Device** as the assignment type, select the application installation type. You can set the application to be installed automatically or allow users to install the application manually.
  - **Manual**: The user must install the application manually.
  - **Automatic**: The application will be assigned and automatically installed. Users are allowed to remove the application.
- **Auto Update:** If you selected **Device** as the assignment type and **Automatic** as the installation type, specify whether you want the application to be automatically updated.

5. If you have selected **Device** as the assignment type, select the target groups or organizations.
6. If you have selected **Device** as the assignment type, select the target groups or organizations and click **Assign**. If you're assigning the VPP applications to users, select the target users and click **Assign**.
7. In the "Assign Application" pop-up window, click **OK**.

Assigning multiple VPP applications

Assign multiple applications at the same time. You can assign up to 10 VPP applications at the same time. This operation is only possible if you assign the applications to devices and they have the same settings. That is, they will have the same Assignment Type, Install Type, and targets.

To assign multiple applications to devices, complete the following steps:

1. Navigate to **Application**.
2. On the "Application" page, select the VPP applications you want to assign.
   - Enter an application's name, or select iOS as the platform and Volume Purchase Program as the source, and click **Search**.
3. Select multiple applications to assign, and click **Assign**.
4. On the top of the "Assign Application" page, click **See Other Apps** to view the list of applications, select the Assignment Type, Install Type, and Target Type, and then click **Assign**.
5. In the "Assign Application" pop-up window, click **OK**.

Unassigning a VPP application

Only the applications of the managed distribution type can be unassigned. When you unassign an app, that app is automatically uninstalled from the devices you selected.

To unassign the assigned application, complete the following steps.

1. Navigate to **Application**.
2. On the “Application” page, search for the application you want to unassign.
    - To search, enter the name or select the **iOS** for platform and **Volume Purchase Program** for source and click **Search**.
3. Click the application you want to unassign.
4. In the Device, Assigned User, or Assigned Group/Organization tab on the “Application Detail” page, select the targets you want to unassign and click **Unassign**.
5. In the “Unassign Application” window, click **OK**.
    - Unassigned applications can no longer be used.

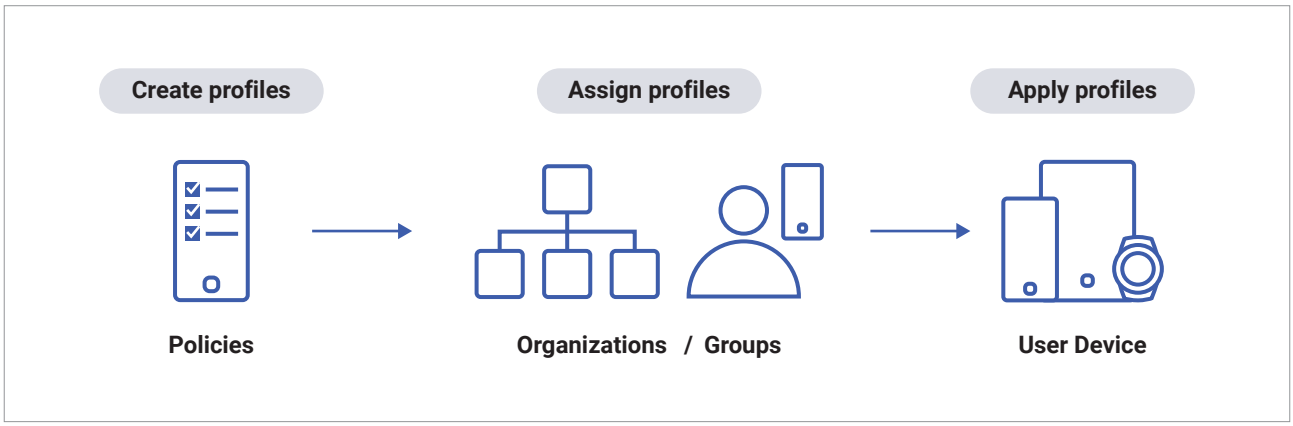
6

Profile

Profile

A profile is a set of policies containing device configurations and settings. Profiles allow you to control device functions and data, such as the camera, screen lock, Bluetooth, or firewalls quickly and efficiently. With profiles, you can also install the Wi-Fi, VPN, and Exchange settings of your company on user devices.

Profiles can also be configured to run in specific situations, such as at a specific time or when the device is running a specific application.

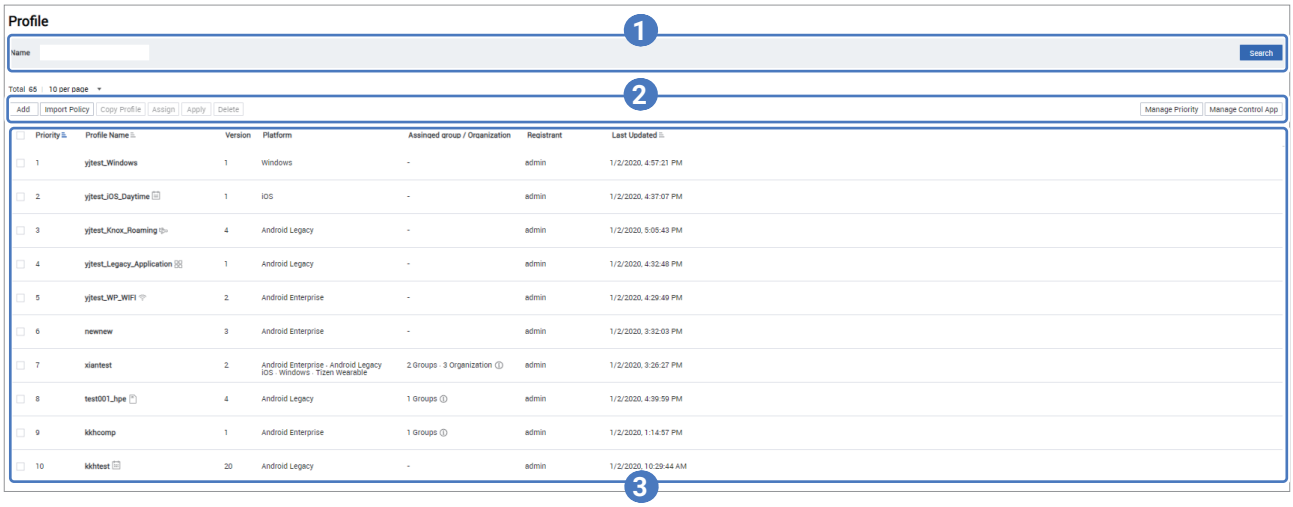


This chapter explains the following topics:

Viewing the profile list

Navigate to **Profile** to view all the profiles on the “Profile” page. You can also perform specific functions on the selected profiles on the list.

On the profile list, the personalized settings of the columns will be saved. The saved settings will be retained before you delete the web browser’s cookies. You can also return the column settings to their default settings by clicking **Revert Column Settings**.



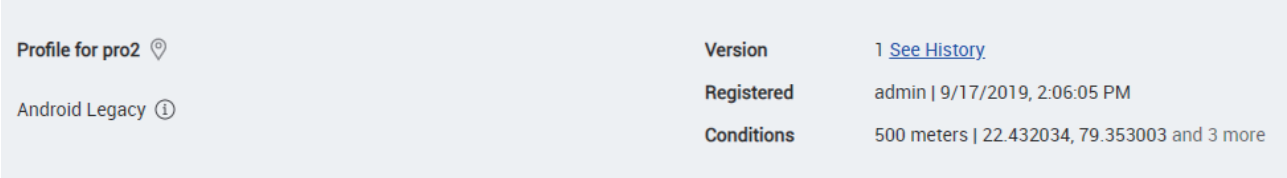
No	Name		Description
1	Search field		Search for a desired profile.
2	Function buttons	Add	Create a new profile. For more information, see Creating a new profile.
		Import Policy	Import policies from a CEA file. In the “Import Policy” window, enter the profile name, click to open a CEA file, and then click **OK**. You can add a profile by importing policies that were downloaded in the ‘Profile Detail’ screen.
		Copy Profile	Copy the selected profile and create a new profile.
		Assign	Assign the selected profile to a group or an organization. For more information, see Assigning to groups and Assigning to organizations.
		Apply	Apply the selected profile to a group or an organization after assigning it.
		Delete	Delete the selected profile. If the profile has been applied to a group or an organization, it cannot be deleted.
		Manage Priority	Set up the profile priorities for when multiple profiles are being applied to the same group or organization. For more information, see Setting up the profile priorities.
		Manage Control App	Add applications by package name to control them with a blacklist or whitelist. For more information, see Managing applications for specific purposes.
		Revert Column Settings	Resets the column settings to the default settings.
3	Profile list		View the brief information of the profiles on the list.

Viewing the profile details

View each profile's details by clicking a profile name on the profile list.

Summary area

The summary area contains the information about the profile, such as the profile name, description, supported platform, and profile version.



- Hover the mouse over i to see controllable device types.
- Click **See History** to see the profile update history.
- Click the icon next to the profile name to check the conditions under which event profiles can be applied.

Tab: Policy

The Policy tab shows the policies that belong to the selected profile.

Tab: Device

The Device tab shows the list of devices that the profile was applied to. You can perform specific functions to the selected devices on the list.

- Click **See Policy** to view a summary of the policies currently applied to the device. With this information, you can determine the precise status of each policy on a device, and whether individual policies are out of date.

The following function button is available:

Function button	Description
Refresh	Update the list of devices.
Apply	Apply the profile to selected devices.

Tab: Assigned Group / Organization

The Assigned Group / Organization tab shows the list of groups and organizations that the profile was applied to. You can perform specific functions on the selected groups and organizations on the list.

The following function buttons are available:

Function button	Description
Unassign	Remove the profile from the selected groups/organizations.
Apply	Apply the profile to the devices that belong to the selected groups/organizations.

Tab: User (exceptional profile)

A list of users with the exceptional profile is displayed. You can perform a specific function on the selected user list.

The following function buttons are available:

Function button	Description
Unassign	Remove the exceptional profile from the selected users.

Function buttons in the footer

You can perform specific functions on the profile using the function buttons in the footer.

The following function buttons are available:

Function button	Description
Back	Return to the profile list.
Delete	Delete the profile. If the profile has been applied to a group or an organization, it cannot be deleted. You cannot delete an exceptional profile if it has been applied to a user.
Export Policy	Download a list of all the policies in the selected profile as a CEA file or Excel file. You can use the Import Policy feature to add a profile from a file.
Modify Profile Info.	Modify the existing information of the selected profile. For more information, see Modifying profiles in detail.
Modify Policy	Modify the policies of the profile. For more information, see Modifying profiles in detail.
Assign	Assign the profile to a group or an organization. For more information, see Assigning to groups and Assigning to organizations and Assigning exceptional profiles.
Apply	Apply the profile to devices after assigning it.

Creating profiles

Create a new profile or copy an existing one to make another. You can also specify events such as the time for profiles. You can create an exceptional profile with a policy that applies only to a specific user for a specific time period. Alternatively, you can select a Knox Portal application user to create a Knox Portal policy as an exceptional profile.

NOTE

- On Android Enterprise devices running Android 11 or higher, the Fully Managed with Work profile type is not supported but the Work Profile on company-owned type is.
- To apply policies on the Work Profile on company-owned devices or apply Dual DAR policies on Fully Managed or Work Profile on company-owned devices, you must create the Work Profile area and set to use Dual DAR in registering user accounts or adding organizations. For more information, see Creating user accounts and Adding an organization.

Creating a new profile

To add a new profile, complete the following steps:

1. Navigate to **Profile**.
2. Click **Add**.
3. On the “Add Profile” page, enter the following information:
   - **Name**: Enter a name for the profile. The entered name cannot be changed after saving.
   - **Platform**: Click the checkboxes to select device platforms.
     - If you want to set the policy using the Samsung Knox API in Android Enterprise devices, **Samsung Knox** should also be selected.
     - If you have selected the Android Enterprise platform, you can activate a device as a Fully Managed with Work Profile type by clicking the **Create Work Profile on Fully Managed** checkbox.
     - If you have selected the Android Legacy platform, you can create a Knox Workspace by clicking the **Knox Workspace** checkbox.
       - You can create a Dual DAR Workspace by clicking the **Enable Dual DAR** checkbox. The Dual DAR setting must be enabled in the environment settings, and a Dual DAR Workspace cannot be created without the Dual DAR license.
   - **Event Profile**: Click to enable an event profile. For more information, see Adding events for profiles.
   - **Description**: Enter a description for the profile.

4. Click **Save & Set Policy** to save the information and to proceed with configuring the profile detail.
    - Click **Save** to save the information and return to the profile list.
5. Configure the profile details. For more information, see Configuring policies by device platform.

Copying a profile

Copy an existing profile and create a new profile. When you reuse a profile, you cannot load information about the organizations or groups to which the profile has been assigned.

To copy a profile, complete the following steps:

1. Navigate to **Profile**.
2. On the “Profile” page, click the checkbox for the profile to be copied.
3. Click **Copy**.
4. On the “Copy” page, modify the existing information if necessary.
    - **Name**: Enter the name of a profile.
    - **Platform**: Select a device platform.
    - **Event Profile**: Click to enable an event profile. For more information, see Adding events for profiles. When copying an existing event profile and creating a new one, the event type of the new profile cannot be changed.
    - **Description**: Enter a description for the profile.
5. Click **Save & Set Policy** to save the information and proceed to configure the profile details.
    - Click **Save** to save the information and return to the profile list.
6. Configure the profile details. For more information, see Configuring policies by device platform.

Exporting a profile

You can export a registered profile, save it as a CEA file or Excel file, and import a CEA file to an EMM server for management.

To export a profile, complete the following steps:

1. Navigate to **Profile**.
2. On the “Profile” page, click a profile name.
3. On the “Profile Detail” page, click **Export Policy**.
4. In the “Export Policy” window, select a file format to download the profile policies, and then click **OK**.
   - The exported file shows the policies for each platform like Android Enterprise, Samsung Knox, and so on. The policies are displayed under their respective category, and the value for each policy is mentioned—Allow, Disallow, or custom value specific to policy.

NOTE

- Policies about the settings, such as Wi-Fi, VPN, Exchange, Certification, APN, and Email Account, and the policies below cannot be exported.

Platform	Policy
Android Enterprise	Application • App Execution Blacklist Setting • Application uninstallation prevention list Setting • System App Activation Setting Kiosk • Kiosk app settings
Samsung Knox (Android Enterprise)	Application • Battery optimization exceptions DeX • Application execution blacklist(Android)

NOTE

Platform	Policy
Android Legacy	Application • Application black/whitelist settings • Battery optimization exceptions Kiosk • Kiosk app settings Phone • Set app voice recording whitelist System • Device Administrators to install and activate apps DeX • Application execution blacklist(Android)
iOS	Application • Application black/whitelist Settings • Autonomous single app mode
Windows	• Application • Add App Install Black/Whitelist
Tizen Wearable	Application • Application black/whitelist
Knox Workspace	Application • Application black/whitelist settings • App installation authority whitelisting settings • TIMA CCM profile whitelist • TIMA CCM profile app access restriction exception list settings • Settings for whitelisting apps allowing external SD card • Battery optimization exceptions • Set General area app installation list • App Data deletion control setting Security • Enterprise Identity Authentication

Adding events for profiles

Profiles can be configured with specific events for them, such as time or application. The policies in these profiles will be applied only when the set events are met. If multiple platforms are selected, only the applicable events for the selected platform will be displayed. For example, the Day & Time will be displayed if Android Legacy and iOS are selected at the same time.

Event types and information

Profiles can have seven different event types. See the table below for details.

Type	Description	Offline support
Day & Time	Applies the profile configured to the devices on a specified day or time. You should configure the time zone, days and the timeframe to apply policies on a specified day and time only.	Supported
Application	Applies the profile configured to devices when a specified application is being used on the user's device. Internal applications or app-wrapped applications contain the SDK functions so that they can have the event applied. **NOTE** • In order to apply the Application event, the selected application should not be blacklisted. • The SecuCamera must have priority over the Gate access events. You have to be very careful with the event policies so they do not cause security issues.	Supported
Wi-Fi SSID	Applies the profile configured to devices when the device is connected to a specific Wi-Fi SSID. **NOTE** For devices with Android 9.0 or a higher version, the location setting must be turned on to enable searching Wi-Fi SSIDs and use events.	Supported

Type	Description	Offline support
SIM Change	Applies the profile configured or locks the device when an unauthorized SIM is installed. **NOTE** • If a device has been locked because of a SIM card change, then an administrator can unlock it by sending the **Unlock Device** device command. Alternatively, they can send an unlock code to the user and instruct them to enter it. The device will be locked after an hour when the event is applied again. • eSIM does not support the SIM Change event.	Not supported
Roaming	Applies the profile configured to devices when the roaming service is used. If the device cannot communicate with the server temporarily due to roaming, the profile is applied when the communication network becomes available again, such as when airplane mode is turned off or the device is rebooted.	Not supported
Custom	Enter the value defined in customer's legacy in **Code** and click +. When sending a custom device command, selecting the Code value set in Custom will apply the profile to the device.	Not supported
Gate access	Enter **Gate access code** and click +. When sending the gate access event device command, selecting the Gate access code value will apply the profile to the device.	Not supported

You can only add or edit event types for profiles that have **Event Profile** turned on during the profile creation process. To add or edit event types for profiles where Event Profile is turned off, you must create a new profile with all the same options and turn on Event Profile while you create the profile.

To add an event for a profile, complete the following steps:

1. Navigate to **Profile.**
2. Click **Add**.
3. On the “Add Profile” page, enter the following information:
   - **Name**: Enter the name of a profile.
   - **Platform**: Select a device platform.
   - **Event Profile**: Click  to enable the use of events.
   - **Event Type**: Select an event type.
   - **Requirement**: Shows the requirements for the selected event type. This option appears only when an event profile is enabled.
     - **Day & Time**: The policy for changing the date and time should be restricted. Navigate to **Android Enterprise** > **System** or **Android (Legacy)** > **System** in the profile and set the **Automatic Date and Time** option to **Disallow**.
     - **Application**: If an application is on the blacklist, that application cannot be selected for this type.
     - **Wi-Fi SSID**: Wi-Fi should be allowed.
   - **Conditions**: Configure the conditions depending on the selected event type. This option appears only when the profile has events enabled. For more information about the condition’s details, see Supported platforms by event type.
   - **Activity Transition Allowance Time(ms)**: If you set more than one application as an event, set the amount of time (ms) from the first application launch to the second application launch. The default value is 50 ms and can be up to 1000 ms. If you change the application transition allowance time to be larger than the default value, applying the application event policy will be postponed, which may cause a security hole. This option only supports the application type.

     NOTE For camera applications, setting to the default value is recommended due to a security hole.

   - **Allow Run Offline**: Allow the profile to be applied to the device even when it is offline. This option appears only if events are enabled. This option only supports the Day & Time, Application, and Wi-Fi SSID types.

     NOTE Profile policies may not be applied if there are two or more event types for which **Allow Run Offline** is set to **Disallow**. If **Allow Run Offline** is set to **Disallow**, the event can be applied only when communicating with the server, so it is recommended to set it to **Allow**.

- **Lock Device when changing SIM**: Locks the device when the SIM is changed. This option appears only when the SIM Change type event has been selected.
- **Notification**: Sends a notification to device users when the profile starts or stops being applied.
- **Show on Device**: The descriptions of events you entered will be displayed as pop-ups or messages when the events are applied.

4. Click **Save & Set Policy** to save the information and proceed to configure the profile details.
   - Click **Save** to save the information and return to the profiles list.

Supported platforms by event type

Event Type	Supported platforms and managed type				
	Android Enterprise		iOS	Knox Workspace	Android Legacy
	Fully Managed	Work Profile			
Day & Time	O	O	O	O	O
Application	O	O	X	O	O *
Wi-Fi SSID	O	O	X	O	O
SIM Change	O	X	X	O	O
Roaming	O	X	X	O	O
Custom	O	O	O	O	O
Gate access	O	O	O	O	O

NOTE

- The SIM Change, and Roaming types allow only one event per profile.
- eSIM does not support the SIM Change event.
- Mark with * for the event applicable only Samsung devices.

Configuring policies by device platform

Specify the policies for device controls, such as the security policy or application policy. After specifying the policies, you can directly apply the profile to the assigned organization or group.

To add policies to a profile, complete the following steps:

1. Navigate to **Profile**.
2. On the “Profile” page, click **the name of the profile** to configure policies for.
3. On the “Profile Detail” page, click **Modify Policy**.
   - Click **Save & Assign** to add device’s platforms to profile.
4. On the “Set Profile” page, configure the policy details by device platform. Each device platform has different groups of policies.
   - Select the platform to configure, for example, Samsung Knox.
   - Find the setting you want to configure by selecting the proper category or by performing a keyword search in the **Search Policy** field.
   - Configure the policy as needed.
5. Save the policy:
   - Click **Save & Assign** to save your changes and proceed to assigning the profile to groups or organizations.
   - Click **Save** to save your changes.

→ Configuring Android Enterprise Policies

→ Configuring Samsung Knox (Android Enterprise) Policies

→ Configuring Android Legacy Policies

→ Configuring Knox Workspace Policies

→ Configuring iOS Policies

→ Configuring Windows Policies

→ Configuring Tizen Wearable Policies

Configuring Android Enterprise Policies

Create a profile and register policies for Android Enterprise devices.

EMM supports four types of Android Enterprise: Fully Managed, Work Profile, Fully Managed with Work Profile, Work Profile on company-owned.

Type	Description
Fully Managed	This type allows you to control the whole device.
Work Profile	This type only allows you to control the work area on the device.
Fully Managed with Work Profile	This type allows you to control both the personal and work areas and apply separate policies. Supported on devices running from Android 8 (Oreo) to Android 10 (Q).
Work Profile on company-owned	This type allows you to control both the personal and work areas and is enhanced in aspect of privacy protection compared to the Fully Managed with Work Profile type. Separate policies are applied. Supported on devices running Android 11 or higher.

NOTE The high version of EMM supports only Samsung devices.

You can configure the policies below for Android Enterprise devices. The availability of each policy varies depending on the enrollment type and the OS version.

→ System (Android Enterprise)

Provides backup and restore settings, developer options, and other features.

→ Interface (Android Enterprise)

Controls the network settings, such as Bluetooth, Wi-Fi Direct, and tethering.

→ Security (Android Enterprise)

Configures the security settings, such as the password and lock screen.

→ Kiosk (Android Enterprise)

Configures Kiosk applications on a Kiosk device and controls the device settings.

→ Application (Android Enterprise)

Configures options for application controls such as installation, verification, and permission.

→ Location (Android Enterprise)

Allows the use of GPS or collecting location data from a device.

→ Phone (Android Enterprise)

Configures the phone settings, such as airplane mode, the microphone settings, and the cellular network settings.

→ Container (Android Enterprise)

Allows data transfers within the Work Profile or with other devices.

→ Wi-Fi (Android Enterprise)

Configures the Wi-Fi settings, such as SSID, security type, and proxy.

→ Bookmark (Android Enterprise)

Configures the bookmark settings such as the icons and URL that will be displayed on devices.

→ Knox VPN (Android Enterprise)

Configures the VPN (Virtual Private Network). Android 13 and later, this policy is no longer support.

→ Certificate (Android Enterprise)

Set the certificate and the user authentication method on devices for when device users authenticate.

System (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
User Certificate Settings	Allows the setting of user certificates.	DO/PO: Android 4.3 or higher
Camera	Allows using the camera. **NOTE** If the device is activated as a Work Profile, the camera function only in the Work Profile will be controlled.	DO: Android 4.0 or higher, Samsung Knox 1.0 or higher PO: Android 5.0 or higher WP-C
Screen capture	Allows use of the screen capture function, which is already set as default. Screen capture is allowed in the Work Profile. **NOTE** Although this policy is not allowed, you can use screen capture through the RS Viewer.	DO: Samsung Knox 1.0 or higher PO: Android 5.0 or higher WP-C
Account modification	Allows modification (add/delete) of the accounts added for each application. • **Disallow**: Disallows to add or delete users even if the Add/Delete User policies are allowed.	DO/PO: Android 4.3 or higher
> Account Blacklist	Add a specific account type blacklist that should not be added on the device (Setting> Accounts and backup > Accounts). Specify the correct account name to block. For instance, enter com.google.android.gm.pop3 for a Gmail (pop3) account. **NOTE** If you change the value of this policy when the account list contains values, all values in the account list will be erased.	

Policy	Description	Supported devices
Allow Account in Google Play	Set an account that can log in to Google Play. Use Managed Google Play (MGP) account and unmanaged Google accounts on the device. • **Allow only MGP Account**: Allow the MGP account and an allowlist defined by the **Account Blacklist** policy. **NOTE** **Account modification** policy must be set to **Allow** before using this policy.	DO/PO: Android 4.3 or higher WP-C
> Account Allowlist	Specifies an allowlist of accounts on the device that can access Google Play.	
System update	Allows setting if and how over-the-air (OTA) updates are applied to devices. Choose one of the following setting option: • **Automatic**: Automatically apply updates as soon as they become available. • **Postpone**: Postpone OTA updates for up to 30 days. • **Windowed**: Schedule OTA updates to occur at a specific time within a daily maintenance window.	DO: Android 6.0 or higher WP-C
> Schedule (Start - End Time)	If you select **Windowed** as the **System update** policy, enter a time in 24-hour format.	
> Freeze Period	Set a freeze period of system updates. When the device's clock is within any of the freeze periods, all incoming system updates, including security patches, will be blocked and cannot be installed. Each individual freeze period can be a maximum of 90 days long, and adjacent freeze periods must be at least 60 days apart from each other. Also, any freeze periods must not be duplicated or overlap with each other. **NOTE** The freeze period setting is applied only on the Android 9.0 or higher.	
Add User	Allows adding the user account.	DO: Android 5.0 or higher
Delete User	Allows deleting the added user account.	DO: Android 5.0 or higher
Safe mode	Allows using Safe Mode. This policy retains device command functions such as camera control, but not EMM applications and internal applications.	DO: Android 6.0 or higher, Samsung Knox 1.0 or higher WP-C

Policy	Description	Supported devices
Change wallpaper	Allows changing the home and lock screens.	DO: Android 7.0 or higher, Samsung Knox 1.0 or higher
Custom Wallpaper	The administrator can set the user's device wallpaper. The Custom Wallpaper (Apply) policy is available only when the Change Wallpaper is No Setting (-) or **Allow**. • After applying this policy, navigate to the **Home screen setting** and set **Rotate to landscape mode**, and then click the rotate button at the bottom of the device to use the device in landscape mode. • After setting the Custom Wallpaper (Apply) policy and releasing it to No Setting (-) again, the wallpaper will be the device's factory default wallpaper.	DO: Android 7.0 or higher
> Wallpaper File	Click the  and register a file to upload. If you set a custom wallpaper, the wallpaper will be applied to the device. You can add files in the bmp, gif, ico, jpg, jpeg, or png format. Each file must be less than 10 MB.	
External SD card	Allows using the external SD card. • **Allow**: If Allow is selected, an additional control is possible for writing to the external SD card.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higherWP-C
> Write to external SD card	Allows writing to an external SD card. **NOTE** If the **external SD card** policy is allowed but the **Write to external SD card** policy is not, then external SD cards can only be read and do not have reset control.	DO: Samsung Knox 1.0 or higherWP-C
Factory reset	Allows a device factory rest. **NOTE** If Disallow is selected, the factory reset mode using the hardware key also can be controlled. After entering the download mode, factory reset using a firmware update utility cannot be controlled.	DO: Android 5.1 or higher, Samsung Knox 1.0 or higher
S Beam	Allows using Android Beam which transfers data via NFC.	DO: Android 5.1 or higher, Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Create Window	Allows a window to be created and launched at the top when users use a multi-window transformed into a pop-up window or a split screen mode on the device.	DO: Android 5.0 or higher
Easter Egg	Allows executing the Easter Egg games on devices with specific actions.	DO: Android 6.0 or higher
Brightness Setting	Allows changing of the screen brightness level. **NOTE** For Android 7.0 or lower devices, this applies to Samsung(Knox1.0+) only.	DO: Android 9.0 or higher
AOD	Allows the always on display feature that displays brief information on the lock screen, such as notifications or time.	DO: Android 9.0 or higher
System Error Screen	Allows an error dialog display function when an application shutdowns abnormally.	DO: Android 9.0 or higher
If compromised OS is detected	Select a measure to take when a compromised OS is detected. • **Lock device**: Locks the device. • **Lock Email**: Locks email use. • **Factory reset + Initialize SD card**: Simultaneously factory resets the user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. **NOTE** The factory reset function is unsupported in Android 2.0 or lower. To reset the device, select the Factory reset + Initialized SD card option.	DO: Android 2.2 or higher
Set Notifications from an event to On.	Set the device to display a notification when an event for device control is applied. • **User defined**: Users can set event notifications on the device from the Settings menu of the EMM Agent. • **Show notification**: Displays the notification when an event for device control is applied. • **Hide notifications**: Hides the notification when an event for device control is applied.	DO: Android 1.0 or higher, Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Set Notifications from an event to Off.	Set the device to display a notification when an event for device control is disengaged. • **User Defined**: Users can set event notifications on the device from the Settings menu of the EMM Agent. • **Show notification**: Displays a notification when an event for device control is disengaged. • **Hide notifications**: Hides a notification when an event for device control is disengaged.	DO: Android 1.0 or higher, Samsung Knox 1.0 or higher
Fix Event Notification	Set the removal of notifications from the device Quick panel. • **User Defined**: Users can remove notification on the device from the settings menu of the EMM Agent. • **Disallow to Remove Notification**: Users cannot remove notifications on the device Quick Panel. • **Allow to Remove Notification**: Users can remove notifications on the device Quick Panel.	DO: Android 1.0 or higher, Samsung Knox 1.0 or higher
Encryption for storage	Specifies the encryption of the device's internal storage or the external SD card.	DO: Android 4.1 or higher, Samsung Knox 1.0 or higher
> Storage encryption	Check the checkbox to select the storage to be encrypted. **NOTE** External SD card encryption is applicable to Samsung Galaxy devices only.	
NTP Settings	Allows using the NTP (Network Time Protocol) server. If NTP server is registered, the time information of the server can be applied to the device. **NOTE** Android 13 and later, this policy is no longer support.	DO: Samsung Knox 5.5 or higher
> Server address	Enter the NTP server address.	
> Maximum number of attempts	Set the maximum number of attempts for connecting to the NTP server to retrieve the time information. The value can be between 0 – 1000 attempts.	
> Polling cycles (hr)	Set the cycle to reconnect to the server via NTP. The value can be between 0 – 8760 hours (8760 hours = 1 year).	
> Short polling cycle (sec)	Set the cycle to re-connect to the NTP server after experiencing a timeout. The value can be between 0 – 1000 seconds.	
> Timeout (sec)	Set the connection timeout on the NTP server. The value can be between 0 – 1000 seconds.	

Policy	Description	Supported devices
VPN Setting	Allows viewing and modifying the VPN settings on the device.	DO: Android 5.0 or higher
Automatic Date and Time	Allows changing the date and time settings. • **Enforce Time Zone**: Override the time zone and prevent the device user from changing it. **NOTE** **Enforce Time Zone** is supported on the Android 9.0 or higher devices.	DO: Android 5.0 or higher
> Time Zone	Specifies the time zone. Only available if **the Automatic Date and Time** policy is set to **Enforce Time Zone**.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higher WP-C
Language Setting	Allows the language setting policy.	DO: Android 9.0
Location Setting	Allows users to change the Location settings. • **Disallow**: Users cannot change the on/off setting of the device location.	DO: Android 8.0 or higher
Backup	Allows backup of the device data. **NOTE** If the backup function can be found on your device at Google > Backup, it may seem possible to turn the backup setting on or off, even if this policy is set to **Disallow**. However, the functionality of backup is prohibited, regardless of mobile UI, when the **Backup** policy is set to **Disallow**.	DO: Android 8.0 or higher
Set a Message for Lock Screen	Enables a custom message on the device's lock screen. • If this value is unset, the message only contains the user information, if it's available.	DO: Android 7.0 or higher
> Message	Specifies the custom message on the lock screen. Enter the message in the text field. Click **Lookup** to browse and select available lookup items to add to the message. You can add lookup items to the message, which substitute for device and user information like username and phone number in the Android environment. **NOTE** • If the message contains only whitespace characters, then no lock message displays, and the user can't change it. • Up to 65 characters are displayed on the device.	

Interface (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Printing	Allows the printing function.	DO/PO: Android 9.0 or higher
Autofill Service	Allows auto-completion of information that you enter on websites in the Android browser.	DO/PO: Android 8.0 or higher
Bluetooth Share	Allows Bluetooth sharing. **NOTE** For Android 7.0 or lower devices, this applies to Samsung(Knox1.0+) only.	DO/PO: Android 8.0 or higher
Network Reset	Allows the network usage rest function on a set date. **NOTE** For Android 7.0 or lower devices, this applies to Samsung(Knox1.0+) only.	DO: Android 6.0 or higher
Mobile Network Setting	Allows configuring the mobile network settings.	DO: Android 5.0 or higher
Allow Wi-Fi Change	Allows changing the Wi-Fi Settings.	DO: Android 4.3 or higher

Policy	Description	Supported devices
Wi-Fi	Allow using Wi-Fi. If the Wi-Fi policy has not been applied successfully, the device will try to apply it again 30 minutes later after EMM is activated. **NOTE** • When a new device is enrolled, this policy is applied after internal applications with their installation types set as **Automatic (Non-removable)** are installed. • Android 13 and later, this policy is no longer support. • **Allow**: Allows using Wi-Fi • **Disable On**: Disallows turning Wi-Fi on. It is turned off at all times. • **Disable Off**: Disallows turning Wi-Fi off. It is turned on at all times.	DO: Android 1.0 or higher, Samsung Knox 1.0 or higherWP-C
> Wi-Fi Direct	Allows use of the Wi-Fi Direct (Wi-Fi P2P) connection. **NOTE** • Set the Wi-Fi policy to **Allow** or **Disable Off** before using this policy. • The direct connection of the two devices may cause the device function or the menu to be controlled, depending on the device type.	DO: Samsung Knox 1.0 or higherWP-C
Tethering Setting	Allows tethering Settings.	DO: Android 5.0 or higher
Bluetooth	Allows using Bluetooth. • **Allow**: Allows turning Bluetooth on. • **Disable On**: Disallows turning Bluetooth on.	DO: Android 8.0 or higher, Samsung Knox 1.0 or higherWP-C
> Desktop PC connection	Allows PC connection with the user's device via Bluetooth. **NOTE** Android 13 and later, this policy is no longer support.	DO: Samsung Knox 1.0 or higherWP-C
> Data transfer	Allows data exchanges with other devices via Bluetooth connection.	DO: Samsung Knox 1.0 or higherWP-C
> Search mode	Allows device search mode.	DO: Samsung Knox 1.0 or higher
Bluetooth Setting	Specifies the controls for the Bluetooth use.	DO: Android 8.0 or higher

Policy	Description	Supported devices
PC connection	Allows connecting user's device to PC.	DO: Android 4.3 or higher, Samsung Knox 1.0 or higherWP-C

Security (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher. The personal area on a Work Profile on company-owned device is called WP-C.

NOTE

- For devices running Android 12 or higher and EMM v2.5.5, the security policies in the profiles made for versions lower than EMM v2.5.5 will not be applied.
- Before upgrading to EMM v2.5.5, the administrator should set the policies in **Android Enterprise > Security > Device Password > Minimum Complexity (Android 12 or later)** and apply them to the devices.

Policy	Description	Supported devices
Device Password	Set the password for the device screen lock. Use of the camera is prohibited when the device is screen locked. **NOTE** In case of devices using One Lock, the stronger password policy will be applied between areas.	
> Minimum Complexity (Android 12 or later)	Set the minimum lock screen complexity. The device user must use a lock screen that meets or exceeds the minimum level. Set the minimum complexity level of the lock screen: • **N/A**: No restrictions on the lock screen. • **Low**: A pattern or PIN, with repeating (4444) and ordered (1234, 4321, 2468) sequences allowed. • **Medium**: A PIN without repeating (4444) or ordered (1234, 4321, 2468) sequences. Or, a password with 4 or more characters. • **High**: A PIN with 8 or more characters, without repeating (4444) or ordered (1234, 4321, 2468) sequences. Or, a password with 6 or more characters.	DO/WP-C: Android 12.0 or higher

Policy	Description	Supported devices
> Minimum Strength (Android 11 or earlier)	Set the minimum password strength on the screen. Users cannot set a password that does not satisfy the minimum strength level. • **Weak Biometric**: Set the password using a low-security biometric recognition method. • **Pattern**: Set the password using a pattern or a password with a higher degree of complexity. • **Numeric**: Set the password using numbers or a password with a higher degree of complexity. • **Numeric Complex**: Set the password containing at least numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences. • **Alphabetic**: Set the password containing at least alphabetic (or other symbol) characters. • **Alphanumeric**: Set the password using alphanumeric characters or a password with a higher degree of complexity. • **Complex**: Set it so that the passwords must include alphanumeric and special characters. **NOTE** The password strength increases in the following ascending order: Pattern < Numeric < Alphanumeric < Complex.	DO/WP-C: Android 6.0 ~ Android 11.0
>> Minimum length	Set the minimum length of the password. The value can be between 4 - 16 characters for **Numeric** or **Alphanumeric**. The value can be between 6 - 16 characters for **Complex**. **NOTE** If Minimum strength is set to Pattern, setting Minimum length does not apply.	DO: Android 4.4 or higher, Samsung Knox 2.0 or higher PO: Android 7.0 or higher
>> Minimum number of letters	Set the minimum number of password letters. The value can be between 1 - 10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher
>> Minimum number of non-letters	Set the minimum number of numeric and special characters required in the password. The value can be between 2 - 10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher
>> Minimum number of lowercase letters	Set the minimum number of lowercase letters required in the password. The value can be between 3 - 10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher

Policy	Description	Supported devices
>> Minimum number of capital letters	Set the minimum number of uppercase letters required in the password. The value can be between 1 - 10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher
>> Minimum number of numeric characters	Set the minimum number of numeric characters allowed in the password. The value can be between 1 - 10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher
>> Minimum number of special characters	Set the minimum number of special characters required in the password. The value can be between 1 -10 characters.	DO: Android 4.4 or higher PO: Android 7.0 or higher
>> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 1 - 10 times. **NOTE** If the password is 'Knox123!' and the minimum value is set as 10, the user must use ten other passwords before reusing 'Knox123!' as password.	DO: Android 4.4 or higher, Samsung Knox 1.0 or higher PO: Android 7.0 or higher
>> Expiration after (days)	Set the maximum number of days before passwords must be reset. The value can be between 1 - 365 days.	DO: Android 4.4 or higher, Samsung Knox 1.0 or higher PO: Android 7.0 or higher
>> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before access is restricted. You can set this only when **Numeric**, **Alphanumeric**, or **Complex** is selected. The value can be between 1 - 10 times.	DO: Android 4.4 or higher, Samsung Knox 2.0 or higher

Policy	Description	Supported devices
>>> If maximum failed login attempts exceeded	Select the action to be performed when the maximum number of failed attempts is reached. For the Fully Managed (DO) type: • **Lock device**: Locks the device. • **Factory reset + Initialize SD card**: Simultaneously resets the user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. For the Work Profile (PO) type: • **Factory Reset or Remove Work Profile** – Work Profile for company-owned devices: Resets the device to default factory settings. – Work Profile for personally owned devices: Removes the Work Profile on personally owned devices.	DO: Android 4.4 or higher, Samsung Knox 2.0 or higher PO: Android 7.0 or higher
>> Maximum length of sequential numbers	Set the maximum number of consecutive numeric characters allowed in a password. The value can be between 1 - 10 words.	DO: Samsung Knox 1.0 or higher
>> Maximum length of sequential characters	Set the number of consecutive letters allowed in a password. The value can be between 1 - 10 words.	DO: Samsung Knox 1.0 or higher
> Password Lifecycle Settings (Android 6 or later)	The password lifecycle settings can be set for each lock screen available on a device.	DO: Android 6.0 or higher
>> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 1 - 10 times. **NOTE** If the password is 'Knox123!' and the minimum value is set as 10, the user must use ten other passwords before reusing 'Knox123!' as password.	
>> Expiration after (days)	Set the maximum number of days before passwords must be reset. The value can be between 1 - 365 days.	

Policy	Description	Supported devices
>> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before access is restricted. You can set this only when **Numeric**, **Alphanumeric**, or **Complex** is selected. The value can be between 1 - 10 times.	
>>> If maximum failed login attempts are exceeded	Select the action to be performed when the maximum number of failed attempts is reached. For the Fully Managed (DO) type: • **Lock device**: Locks the device. • **Factory reset + Initialize SD card**: Simultaneously resets the user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. For the Work Profile (PO) type: • **Factory Reset or Remove Work Profile**: If the device is company-owned, it factory resets. If the device is personally-owned, the Work Profile is removed. **NOTE** The device controls policy is applied only when there is no EMM Agent in the general area.	
Block function setting on lock screen	Set Keyguard lock screen features to be disabled on the device. Keyguard features are the various features available on the screen of a locked device, such as secure camera and fingerprints. If it is not configured, users cannot use the Keyguard features. **NOTE** The visibility of the notifications on the lock screen depends on the options you set in the application.	

Policy	Description	Supported devices
> Block functions on lock screen	Select the functions to be blocked on the lock screen when a password policy is set on a device. For the Fully Managed (DO) type: • **All**: Blocks all functions on the lock screen. • **Camera**: Blocks direct camera control on lock screen. • **Trust Agent**: Trust Agent notifies the system whether the device is in a safe condition. If you block the Trust Agent, the Smart Lock function will be blocked, which automatically unlocks the screen in certain conditions. • **Fingerprint**: Blocks the fingerprint unlock function. **NOTE** Android 13 and later, this policy is no longer support. • **Previews in pop-ups**: Displays notifications on the lock screen but hides private content set in the application. • **Notifications**: All notifications are hidden via the lock screen For the Work Profile (PO) type: • **Trust Agent**: Trust Agent notifies the system whether the device is in a safe condition. If you block the Trust Agent, the Smart Lock function will be blocked, which automatically unlocks the screen in certain conditions. • **Fingerprint**: Blocks the fingerprint screen unlock function.	DO: Android 5.0 or higher PO: Android 7.0 or higher
Enforce Multi factor Authentication	Enable multifactor authentication (2FA) that unlocks a device only after two authentication methods are provided, including one biometric input (face/iris/fingerprint) and one lock screen method (PIN/password/pattern) **NOTE** • Incorrect use of this policy together with “One Lock” and “Biometric policy” can lock your device. • Android 13 and later, this policy is no longer support.	DO: Samsung Knox 2.2 or higher
Screen timeout	Allows the user to change the Screen Timeout setting.	DO: Android 9.0 or higher
Maximum screen timeout	Set the maximum screen timeout for when a user is not using or working with the applications on the device.	DO: Android 2.2 or higher, Samsung Knox 2.0 or higher

Policy	Description	Supported devices
Delay Time for Device Lock	Set the amount of time it takes for the device to be locked after the screen is turned off. The sum of the Screen timeout and Auto lock when screen turns off set on the device is the maximum delay time that can be set on the device. (Auto lock when screen turns off: The time required for a password when the screen is turned on again after being turned off) The maximum delay time varies depending on the device model, and the Delay Time for Device Lock may differ depending on the set value of Screen timeout. **NOTE** • The following situations can occur even if this policy is applied to the device. - The user can change the set value of Auto lock when screen turns off in the Settings menu of the device. - The set values of the Auto lock when screen turns off and the Delay Time for Device Lock set on the device may be different from the one applied to the profile. - If the device is unlocked by Smart Lock, the set Delay Time for Device Lock does not apply to the device.	DO: Android 2.3 or higher
Work profile password	Set to use the Work Profile container screen lock password on the Work Profile installation, the users are directed to set the Work Profile screen lock password. **NOTE** • If users forget their password and ask you, you should send the device command to reset the password and guide them to input the temporary password that was sent. For more information about the procedure, see Viewing the device details. • In case of devices using One Lock, the stronger password policy between areas will be applied.	

Policy	Description	Supported devices
> Minimum Complexity (Android 12 or later)	Set the minimum lock screen complexity. The device user must use a lock screen that meets or exceeds the minimum level. Set the minimum complexity level of the lock screen: • **N/A**: No restrictions on the lock screen. • **Low**: A pattern or PIN, with repeating (4444) and ordered (1234, 4321, 2468) sequences allowed. • **Medium**: A PIN without repeating (4444) or ordered (1234, 4321, 2468) sequences. Or, a password with 4 or more characters. • **High**: A PIN with 8 or more characters, without repeating (4444) or ordered (1234, 4321, 2468) sequences. Or, a password with 6 or more characters.	PO: Android 12.0 or higher
> Minimum strength (Android 11 or earlier)	Set the minimum password strength on the screen. Users cannot set a password that does not satisfy the minimum strength level. • **Pattern**: Set a password with a pattern or with a higher degree of complexity. • **Numeric**: Set a password with numbers or with a higher degree of complexity. • **Alphanumeric**: Set a password with alphanumeric characters or with a higher degree of complexity. • **Complex**: All passwords must include alphanumeric and special characters. **NOTE** The password strength increases in the following ascending order: Pattern < Numeric < Alphanumeric < Complex.	PO: Android 7.0 or Android 11.0
>> Minimum length	Set the minimum length of the password. The value can be between 4 - 16 characters. for **Numeric** or **Alphanumeric**. The value can be between 6 - 16 characters for **Complex**. **NOTE** If Minimum strength is set to Pattern, setting Minimum length does not apply.	PO: Android 6.0 or higher
>> Minimum number of letters	Set the minimum password length. The value can be between 1 - 10 characters.	PO: Android 6.0 or higher
>> Minimum number of non-letters	Set the minimum number of numeric and special characters allowed in the password. The value can be between 2 - 10 characters.	PO: Android 6.0 or higher

Policy	Description	Supported devices
>> Minimum number of lowercase letters	Set the minimum number of lowercase letters allowed in the password. The value can be between 3 - 10 characters.	PO: Android 6.0 or higher
>>Minimum number of capital letters	Set the minimum number of uppercase letters allowed in the password. The value can be between 1 - 10 characters.	PO: Android 6.0 or higher
>> Minimum number of numeric character	Set the minimum number of numeric characters allowed in the password. The value can be between 1 - 10 characters.	PO: Android 6.0 or higher
>> Minimum number of special characters	Set the minimum number of special characters allowed in the password. The value can be between 1 - 10 characters.	PO: Android 6.0 or higher
> Password Lifecycle Settings (Android 6 or later)	The password lifecycle settings can be set for each lock screen available on a device.	PO: Android 6.0 or higher
>> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 1 - 10 times. **NOTE** If the password is 'Knox123!' and the minimum value is set as 10, the user must use ten other passwords before reusing 'Knox123!' as password.	PO: Android 6.0 or higher
>> Expiration after (days)	Set the maximum number of days before the password must be reset. The value can be between 1 - 365 days.	PO: Android 6.0 or higher
>> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before access is restricted. The value can be between 1 - 10 times.	PO: Android 6.0 or higher
Block function setting on lock screen	Allows blocking functions on the lock screen. **NOTE** The visibility of the notifications on the lock screen depends on the options you set in the application.	PO: Android 6.0 or higher

Policy	Description	Supported devices
> Block functions on lock screen	Select the function to be blocked on the lock screen when a password policy is set on a device. • **Trust Agent**: Trust Agent notifies the system whether the device is in a safe condition. If you block the Trust Agent, the Smart Lock function will be blocked, which automatically unlocks the screen in certain conditions. • **Fingerprint**: Blocks the fingerprint screen unlock function. • **Previews in pop-ups**: Displays notifications on the lock screen but hides private content set in the application.	

Kiosk (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Kiosk app settings	Select a Kiosk feature to use on a device. • **Single app**: Runs a single application on the device's home screen. • **Multi app**: Runs multiple applications that are developed using the Kiosk Wizard. • **Kiosk Browser**: Opens webpages that are specified by the administrator. **NOTE** • To use the Kiosk Browser, the Kiosk Browser application must be registered as an EMM application. For more details, contact the TMS administrator. • Single App Kiosks are not available with non-Samsung Android Enterprise Fully Managed (DO) devices that are equipped with Android 6.0-8.0. • EMM provides Single App Kiosk with Google managed applications for Android Enterprise devices with version 9.0(Pie) or higher.	DO: Samsung Knox 1.0 or higher Non-Samsung DO: Android 9.0 or higher

Policy	Description	Supported devices
> Set application	Click **Select**, and then choose Public applications (Managed Google Play Store) or Kiosk applications from the Kiosk application list. Alternatively, click **Add**, and then manually add applications. For more information about adding single applications, see Creating a Single App Kiosk.	
> Set application	Click **Select** to select multiple Kiosk applications from the list or click **New** to create a Multi App Kiosk. To learn how to use the Kiosk Wizard, see Exploring Kiosk Wizard.	
> Set Kiosk Browser	When setting up the Kiosk Browser, the package name of the application registered as the Kiosk Browser will be automatically selected.	
> Default URL	Set the default page URL to call in the Kiosk Browser. **NOTE** You can enter a URL that is up to 128 bytes including alphanumeric characters and some special characters (_,., -, *, /).	
> Screen Saver	Use the screen saver for the multi-app kiosk and the Kiosk Browser. When no user activity has been sensed for a certain amount of time set in the Auto Screen Off or Session Timeout settings on the device, the registered images or video files will be activated on the device display. **NOTE** The Screen Saver only runs while the device is charging.	
>> Screen Saver Type	Select either an image or video type screensaver.	
>>> Image	Select image files for the screen saver. You can add up to 10 image files in the PNG, JPG, JPEG, or GIF format (animated files are not supported). Each image file must be less than 5 MB. • To upload an image file, click **Add** and select a file. • To delete an image file, click next to the name of the uploaded image file. **NOTE** The device command must be sent to the device to apply an image file to it.	

Policy	Description	Supported devices
>>> Video	Select a video file for the screen saver. You can add only one video file in the MP4 or MKV format. The video file must be less than 50 MB. • To upload a video file, click **Add** and select a file. • To delete a video file, click 🗑 next to the name of the uploaded video file. **NOTE** The device command must be sent to the device to apply a video to it.	
> Session timeout	Allows the use of the session timeout feature for the Kiosk Browser. If the user does not use the device for a set time, the device deletes user information, such as the cache and cookies, in the device Kiosk Browser and goes to the main page URL: • **Apply**: Enables the session timeout feature for the browser.	
>> Time (sec)	Set the session timeout in seconds for the Kiosk Browser. The value can be between 10 - 3600 secs (default is 1800).	
> Text Copy	Allow the copying of text strings in the Kiosk Browser.	
> Javascript	Allow the running of the JavaScript contained in websites.	
> Http Proxy	Allow the use of an HTTP proxy for communications in the Kiosk Browser.	
>> IP/ Domain:Port	Set the HTTP proxy server IP or domain address, and Port. When not entered, the Port number is automatically set to 80.	
> User agent settings key value	Set the key value to be added to the user agent. Allow the Kiosk Browser to access the Web server and the user agent key values contained in the HTTP header. **NOTE** User agent key settings can be used to detect access to non-Kiosk Browsers on the web server.	
File Upload	Allows the use of attaching files to a website through the Kiosk Browser. Kiosk Browser does not support pop-up windows, so cloud attachment is not possible.	DO: Samsung Knox 1.0 or higher Non-Samsung DO: Android 9.0 or higher

Policy	Description	Supported devices
Utilities setting	Allows the use of specific buttons or features of the device. **NOTE** If you allow the recent apps or system status bar policy, the use of the home button is automatically prohibited.	
> Power	Allows the use of the Power button to turn off or restart the device by pressing and holding the Power button.	
> Recent apps	Allows the use of the Recent apps button. The Home button also needs to be allowed to use the Recent apps button.	
> System status bar	Allows the use of the system status bar.	
> Notification bar	Allows the use of the notification bar. The Home button also needs to be allowed to use the notification bar.	
> Home	Allows the use of the Home button.	
> Key guard	Allows the use of the keyguard feature that displays the lock screen on the device.	
> Whitelisted Apps Setting	Set whether to register applications to use on Kiosk devices. The whitelisted applications can run even if they are not included in Single App Kiosk, Multi App Kiosk, or Kiosk Browser.	DO: Android 9.0 or higher
> Whitelisted Apps	Add applications to use on Kiosk devices. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	
Delete Kiosk app when policy is removed	Allows to delete applications along with policies from a device when the applied policy is deleted.	DO: Samsung Knox 1.0 Non-Samsung DO: Android 9.0
Prohibit hardware key	Specify the hardware keys to disallow in Default and Kiosk mode.	
> Disallow hardware key(s)	Select hardware keys to disallow. The type of hardware keys may vary depending on the device. If you set the task manager to Disallowed, the task manager is not launched even if you tap the left menu key on the navigation bar at the bottom the screen.	DO: Samsung Knox 1.0 or higher

Application (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Installation of application from untrusted sources	Allows the installation of applications from untrusted sources instead of just the Google Play Store.	DO/PO: Android 1.0 or higher
Skip app tutorial	Allows the users to skip application tutorials. • If you select **Allow**, you can choose either some or all of the apps.	DO/PO: Android 6.0 or higher
App Control	Allows application control from the settings application. The following actions can be configured: • Delete / Execute / Prevention / CACHE Removal / Data Removal / Focused Exit / Default App Removal.	DO: Android 5.0 or higher
App Installation	Allows application installation.	DO/PO: Android 1.0 or higher
App Uninstallation	Allows application uninstallation.	DO/PO: Android 1.0 or higher
App Verification	Allows application verification via Google for all device applications.	DO: Android 5.0 or higher PO: Android 5.0 - 7.1

Policy	Description	Supported devices
App Permission	Allow runtime permission settings for internal applications and public applications for all areas. • **Prompt**: Prompts users to grant or deny permissions. • **Grant**: Grants all relevant permissions. • **Deny**: Denies all relevant permissions. **NOTE** In Android 12 or later, even if the app permission setting is set to Grant, some privacy-related functions (camera, location, and microphone) are not allowed.	DO/PO: Android 6.0 or higher
> App permission exception policy list	Add individual application. Set different permission policies for each application. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** • This policy takes priority over the **App Permission** policy when both are applied. • Among the application permissions, only the **dangerous permissions** can be added to this policy. For more information, see https://developer.android.com/guide/topics/permissions/overview.	DO/PO: Android 6.0 or higher
App Execution Blacklist Setting	Set to prevent the execution of the device applications.	
> App execution blacklist	Add applications to prevent their execution. Icon of the blacklisted application disappears and users cannot run the application. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** • An application that has been added on the Application installation whitelist policy cannot be added. • In the personal area on Work Profile on company-owned devices, only system applications can be added and third party applications cannot.	DO/PO: Android 5.0 or higher WP-C

Policy	Description	Supported devices
Application uninstallation prevention list Setting	Set to prevent the uninstallation of the device application.	
> Application uninstallation prevention list	Add applications to prevent their uninstallation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** • Starting from EMM v2.5.3, system applications (EMM Agent, Push Agent, etc.) are automatically registered on the App execution blacklist. • In the personal area on Work Profile on company-owned devices, only system applications can be added and third party applications cannot.	DO/PO: Android 5.0 or higher
System App Activation Setting	Set to activate hidden system applications for Android Enterprise devices to view. If a device is activated with Android Enterprise, only designated applications appear on the device. **NOTE** Applications cannot be activated if they are listed under **Application installation blacklist**.	
> System App Activation	Add system applications to be activated. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	DO/PO: Android 5.0 or higher
App delegation scope management	Set to delegate additional scopes to certain apps on the device. Enables delegated scopes for apps, which is a device policy controller function that grants elevated Android DevicePoliceManager API and policy control to an app. An app with delegated scopes can dictate policies and configuration settings to other apps.	DO/PO: Android 8.0 or higher WP-C

Policy	Description	Supported devices
> App Delegation Scope	Configures delegated scopes for apps. You can only manage one delegation configuration per app. • To add a Package Name, click **Select**, and then select package name in the “Select Application” window. • Select the permission to delegate from the Delegation Scope list and click **+**. You can select multiple permissions. – App permissions that can be delegated include Certificate installation and management, Managed configurations management, Blocking uninstallation, Permission policy and permission grant state, Package access state and Enabling system apps. • To remove privileges delegated to a package, click 🗑 next to the added packages.	
Settings for whitelisting apps allowing external SD card	Allows the use of an external SD card. The external SD card cannot be used by default.	PO: Samsung Knox 2.2 or higher
> Whitelisted apps for external SD card	Add applications that can use an external SD card. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	

Location (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
GPS	Configure to force quit the GPS feature of device. Users can freely change this feature setting on the device if the Location Setting policy is set to **Allow**. • **Disable On**: Disables the GPS feature on the device.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higher PO: Android 5.0 or higher WP-C
Report device location	Allows collecting location data. • **User consent**: Allows location data collection only with the user's consent. • **Allow**: Allow collection of location information. Fully Managed devices with EMM v2.5.5 automatically acquire location permission. **NOTE** • If the Fully Managed with Work Profile type is used, location data from devices is collected based on the Report Device Location value, which is specified in the Fully Managed Device policy. • The report device location interval will be deprecated after EMM v2.5.0. From EMM v2.5.0 or later, you can set the policy in Setting > Location Report Interval.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higher PO: Android 5.0 or higher
> Report device location interval	Set an interval period to save the location data of the device. **NOTE** To set the collection interval, select either **Allow** or **User consent** for the Report device location policy.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higher PO: Android 5.0 or higher
High Accuracy Mode	Set to use for collecting accurate GPS locations of the devices.	DO: Android 5.0 or higher, Samsung Knox 1.0 or higher PO: Android 5.0 or higher

Phone (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Airplane mode	Allows the use of airplane mode.	DO: Android 9.0 or higher, Samsung Knox 2.0 or higher WP-C
Cell Broadcast Setting	Allows the use of emergency broadcast settings. The carrier can send a same message, such as an emergency alert, to the devices connected to the same cellular base station.	DO: Android 5.0 or higher-
Volume Adjustment	Allows adjusting the volume.	DO: Android 5.0 or higher
Microphone	Allows the use of the microphone.	DO: Android 1.0 or higher, Samsung Knox 1.0 or higher WP-C
> Recording	Allows recording with the microphone.	DO: Samsung Knox 1.0 or higher, WP-C
> S Voice	Allows the use of S Voice.	DO: Samsung Knox 1.0 or higher
Voice Call (except Samsung Device)	Allows the use of voice calls. **NOTE** To control Samsung devices, use the Prohibit voice call policy.	DO: Android 5.0 or higher WP-C
SMS (except Samsung Device)	Allows the use of text messages.	DO: Android 5.0 or higher
Data connection during roaming	Allows a data connection while using roaming service.	DO: Android 7.0 or higher, Samsung Knox 1.0 or higher

Container (Android Enterprise)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Copy and Paste Clipboard per Profile	Allows copying and pasting with the clipboard between the personal and work areas.	PO: Android 7.1 or higher
Bluetooth Low Energy	Allows using Bluetooth Low Energy that enables very low power operation of the device.	PO: Samsung Knox 2.4 or higher
Phone Book Access Profile (PBAP) via Bluetooth	Allows sharing contacts from the Profile Owner to the connected device via Bluetooth. **NOTE** The Bluetooth share policy must be set to **Allow** before using this policy.	PO: Android 8.0 or higher

Wi-Fi (Android Enterprise)

You can add more Wi-Fi policy sets by clicking +.

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

For devices activated as Fully Managed with Work Profile, Wi-Fi settings are only applied to the DO area of the device. Wi-Fi settings do not affect the PO area of the device.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for each Wi-Fi setting.
Description	Enter a description for each Wi-Fi setting.
Network Name (SSID)	Enter an identifier of a wireless router to connect to. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.

Policy	Description
Remove available	Allows users to delete the Wi-Fi settings.
Automatic Connection	Set automatic connection of the configured network for the device. • **Use**: The device sets the configured network as a default network and automatically connects the network when the Wi-Fi is on. • **Do not use**: The network configuration is deployed on the device, but the device user will select a network (Wi-Fi AP) to connect to.
Hidden Network	Check the checkbox to hide the network from the list of available networks on the device. The SSID does not broadcast.
Security type	Specifies the access protocol used and whether certificates are required.
> WEP	Set a WEP KEY index from WEP KEY 1 to 4.
> WPA/WPA2-PSK	Enter a password.
> 802.1xEAP	Configure the following items: • **EAP Method**: Select an authentication protocol from between PEAP and TTLS. • **2-step authentication**: Select one from PAP and MSCHAP as a secondary authentication method. • **User information input method**: Select an input method for entering user information. – **Manual Input**: Enter the user ID and Password for the Wi-Fi connection. – **Connector interworking**: Choose a connector from the User information Connector. – **User Information**: Use the user information registered in EMM to access Wi-Fi. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Proxy configuration	Select a proxy server configuration method. You can use the server to route through the proxy server when the device is connected to Wi-Fi.
> Manual	Configure the proxy server manually. • **Proxy host name**: Enter the host name of the IP address of the proxy server • **Proxy port**: Enter the port number used by the proxy server • **Proxy exception**: Enter the IP address or domain address that cannot be accessed through the proxy server. If server authentication is required to use the proxy server, check the Server authentication check box. • **User name**: Enter the username for the proxy server. • **Password**: Enter the password for the proxy server.

Policy	Description
> PAC automatic configuration	Configure the proxy server automatically. You should enter the PAC web address, the URL of the PAC file that automatically determines which proxy server to use.

Bookmark (Android Enterprise)

You can create a shortcut to the bookmarked address of a specific URL on the home screen of the device. You can add more Bookmark policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each bookmark setting.
Description	Enter a description for each bookmark setting.
Installation area	Specifies a location to install the bookmark. • **ShortCut**: Creates a shortcut of the bookmarked address on the home screen of the device. Shortcut icons are created based on the Samsung Launcher. – Shortcut icons may not be able to be created depending on the type of launcher set by the user. – An administrator cannot delete the shortcut icon, but the user can delete it manually.
ShortCut image	Select a shortcut icon to be created on a user device.
Bookmark page URL	Enter a website address to go to when a bookmark is selected.
Bookmark name	Enter the bookmark name to be displayed as a title in the bookmark.

Knox VPN (Android Enterprise)

Knox VPN settings are provided to help you set up a VPN on a Samsung Galaxy device more easily. You can add more Knox VPN policy sets by clicking +.

NOTE

- If the Knox VPN vendor is Cisco, then Work Profile can be installed in both the Work Profile area and personal area. To use a Knox VPN on both areas, you need to install the vendor's VPN Client application in each area.
- For Android Enterprise devices, Knox VPN can be installed on the Work Profile area, Fully Managed area, or both areas.
- Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for the Knox VPN setting.
VPN name	Enter a VPN name to display on the user device.
Description	Enter a description for the Knox VPN setting.
Remove available	Allows users to delete the Knox VPN settings.
VPN vendor name	Select a VPN vendor from among **Cisco**, **StrongSwan**, and **User defined**. Input fields vary depending on the selected VPN vendor name. **NOTE** Select **User defined** to set up a different vendor's VPN service, such as the Sectra mobile VPN. For more information, see Entering a VPN vendor manually.
VPN client vendor package name	Entered automatically according to the selected VPN vendor name. If **User defined** is selected, you must manually enter this protocol.
VPN type	Entered automatically when you select **StrongSwan**. If **Cisco** or **User defined** is selected, you must manually select this protocol.
Entering methods for Knox VPN	Select an entering method for Knox VPN information. • **Manual Input**: Only allowed for **StrongSwan** and **Cisco**. For more information, see Configuring a Knox VPN profile manually. • **Upload profile**: Allowed for all VPN vendors. **NOTE** Input fields vary depending on the selected VPN vendor and the entering method.
Upload Knox VPN profile	Allows uploading a Knox VPN profile when you set **Entering methods for Knox VPN** to **Upload profile**. You can upload a text file in the JSON format. JSON varies depending on the VPN vendor and VPN type. For more information about sample files, see the sample file of a Sectra Mobile VPN configuration in Configuring a Knox VPN profile manually. And see the sample file of Cisco VPN configuration in Sample file for uploading a Knox VPN profile.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
CA Certificate	Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **Knox VPN** and the Type set as **Root** will appear on the list.
Server certificate	Select a certificate to use from the certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose has been set as **Knox VPN** and the Type set as **User** will appear on the list.
FIPS mode	Allows the use of FIPS mode. FIPS (US Federal Information Processing Standards) encrypts all data with FIPS-140-2 authentication modules between the server and client.

Policy	Description
Auto Re-connection	Allows connecting automatically when an error occurs.
VPN route type by application	Select to use a VPN for selected applications or for all applications in the General area. • **By Application**: Click **Add** next to **The VPN applied package name per app**, select applications, and then click **Save**. • **All packages of general area**: All applications in the General area are subject to a VPN.

Entering a VPN vendor manually

To use a VPN provided by a vendor other than StrongSwan or Cisco, select **User defined** in the **VPN vendor name** field. Then upload a text profile in the JSON format. The VPN Client must be installed on the device before using a VPN.

For example when a Sectra VPN is used, set the options as below:

1. Enter `com.sectra.mobilevpn` in the **VPN client vendor package name** field.
2. Set **VPN type** to **SSL**.
3. Click **Add** next to **Upload Knox VPN profile** and upload a configuration file with the Sectra Mobile VPN configuration parameters set.
   - Upload a file in the JSON format to fully integrate the Sectra Mobile VPN in the EMM Admin Portal.
   - Set the parameters as shown in the example below.

Parameter	Description	Example
profileName	The name of the VPN configuration profile that will be listed on the EMM application and the VPN client GUI.	Sectra Mobile VPN
servers	A list of 1 – 6 VPN servers with IP addresses and a network port. This list will be in an order of priority, with the default VPN server being the first on the list. The remaining VPN servers will be used only if the default server is damaged.	[{"address":"1.1.1.1", "port":443} {"address":"2.2.2.2", "port":444} {"address":"3.3.3.3", "port":445}]
pkcx12BaseUrl	A download server's HTTP/S URL, where the encrypted key materials are downloaded to.	http://download.server.com/certs/
mtuSize	The MTU (Magnetic Tape Unit) is a size used on EMM's virtual network interface. It is the maximum size for the outgoing UDP (User Datagram Protocol) tunnel packets before being fragmented The value must be between 576 – 1500 bytes.	1300
UseDtle	Determines whether a DTLS tunnel is used. A DTLS tunnel should be used if sensitive data is being transmitted in real-time. E.g.) When streaming video and/or using VoIP calls. The value must be either True or False. If unsure, set to True.	True
diffServe	Tunnel packets' QoS (Quality of Serve) tag sent from a client. Differentiated service is part of an IP header. The value must be between 0 – 63. 0 means disabled.	0
tcpKeepAlive	Timer value for the interval of a KeepAlive packet sent from a TCP tunnel. The value must be between 1 – 18000. • Sectra recommends to set this value as 1200 seconds since is compatible with most mobile networks. **NOTE** This is an important parameter that needs to be selected with caution.	1200

Parameter	Description	Example
dtlsInactivityTimeout	The timer value for the standby period of a DTLS tunnel that determines how long it idles without receiving any data before it goes inactive. The value must be between 1 – 300 seconds. **NOTE** Sectra does not recommend setting this value to 300 seconds.	30

trarricProfiles	1 – 3 traffic profiles the users can choose, for when a normal configuration is not sufficient. Traffic profiles can change the following configuration parameters: mtuSize, useDtls, diffServ, tcpKeepAlive and/or dtlsInactivityTimeout. The traffic profile also requires the name of the profile which is shown in the client GUI.	`[ {"profileName": "BadNetworkProfile","mtuSize":800, "tcpKeepAlive":600},`
		`{"profileName":" RealTimeProfile" ,"mtuSize":1500, "useDtls":"true", "diffServ":63}`
		`]`

The following is a sample file of a Sectra Mobile VPN configuration:

```
{
     "KNOX_VPN_PARAMETERS":{
           "profile_attribute":{
                 "profileName":"Sectra Mobile VPN",
                 "vpn_type":"ssl",
                 "vpn_route_type":1
           },
           "knox":{
                 "connectionType":"keepon"
           },
            "vendor":{
                 "connection":{
                       "servers": [
                             {"address":"1.1.1.1", "port":443},
                             {"address":"2.2.2.2", "port":444},
                             {"address":"3.3.3.3", "port":555}
                       ],
                       "ssl": {
                             "basic": {
                                 "pkcs12BaseUrl":"http://download.server.com/
certs/",
                                 "mtuSize":1300,
                                 "useDtls":true,
                                 "diffServ":0,
                                 "tcpKeepalive":1200,
                                 "dtlsInactivityTimeout":30
                             }
                       }
                 },
                 "trafficProfiles": [
                       {
                             "profileName": "BadNetworkProfile",
                             "mtuSize":800,
                             "tcpKeepAlive":600
                       },
                       {
                             "profileName":"RealTimeProfile",
                             "mtuSize":1500,
                             "useDtls":"true",
                             "diffServ":63
                       }
                 ]
           }
      }
}
```

Configuring a Knox VPN profile manually

You can manually enter a profile only when the VPN vendor is StrongSwan or Cisco. Select **Manual Input** in the **Entering method for Knox VPN** field. Then set the options as below:

1. Enter the IP address, host name, or URL of the VPN server in the **Server address**.
   - The VPN route type, which enables the use of VPN tunneling, is automatically entered.
2. Select to use **user authentication**.
3. Enter the user information for authentication depending on the selected **method of entering user information**:

Method	Description
Manual Input	Enter the user ID and Password for the VPN connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Connector interworking	Choose a connector from the **User certificate Connector**. All the connectors are listed in **System** > **Connector** > **Directory**.

4. Select a connection type and enter the parameters. The required parameters vary depending on the selected connection type.

Item	Description
PPTP	Select whether to use **PPP Encryption (MPPE)**.
L2TP/IPSec PSK	Enter the **L2TP Secret Key**, **Identifier**, and **Pre-shared Key**.
L2TP/IPSec RSA	Enter the **L2TP Secret Key**.
IPSec Xauth PSK	Enter the **IPSec Identifier** and **Pre-shared Key**.
IPSec Xauth RSA	Enter the **User certificate input method**, **CA Certificate**, and **Server Certificate**.
IPSec Hybrid RSA	Enter the **CA Certificate** and **Server Certificate**
IPSec IKE2 PSK	Enter the **Identifier** and **Pre-shared Key**.
IPSec IKE2 RSA	Enter the **User certificate input method**, **OCSP URL**, **CA Certificate**, and **Server Certificate**.

5. Configure the advanced option.

Item	Description
DNS search domain	Enter the DNS name.
DNS server	Enter the DNS address according to the IP pattern.
Forwarding route	Entered automatically when **Subnet Bits** is selected
Subnet Bits	Select **None** or **/1** from **/30**.

6. Select a VPN connection type.
   - **Keep On**: Keep the VPN connection.
   - **On Demand**: Connect to the VPN upon request.
7. Select the chaining type.
8. Select to use the UID PID.

Sample file for uploading a Knox VPN profile

The following is a sample file with Cisco as the VPN vendor and IPSec as the VPN type:

```
{
     “KNOX_VPN_PARAMETERS”:{
          “profile_attribute”:{
               “profileName”:”c1”,
               “host”:”12.3.456.78”,
               “isUserAuthEnabled”:true,
               “vpn_type”:”ipsec”,
               “vpn_route_type”:1
          },
          “ipsec”:{
               “basic”:{
                    “username”:””,
                    “password”:””,
                    “authentication_type”:1,
                    “psk”:””,
                    “ikeVersion”:1,
                    “dhGroup”:0,
                    “p1Mode”:2,
                    “identity_type”:0,
                    “identity”:”test@sta.com”,
                    “splitTunnelType”:0,
                    “forwardRoutes”:[
                         {
                              “route”:””
                         }
                    ]
               },
               “advanced”:{
                    “mobikeEnabled”:false,
                    “pfs”:true,
                    “ike_lifetime”:”10”,
                    “ipsec_lifetime”:”25”,
                    “deadPeerDetect”:true
               },
               “algorithms”:{
               }
          },
          “knox”:{
               “connectionType”:”keepon”,
               “chaining_enabled”:”-1”,
               “uidpid_search_enabled”:”0”
          },
          “vendor”:{
               “setCertCommonName”:”space”,
               “SetCertHash”:”pluto”,
               “certAuthMode”:”Automatic”
          }
     }
}
```

The following is a sample file with Cisco, as the VPN vendor, and SSL, as the VPN type:

```
{
     "KNOX_VPN_PARAMETERS":{
          "profile_attribute":{
               "profileName":"c3",
               "host":"cisco-asa.gnawks.com",
               "isUserAuthEnabled":true,
               "vpn_type":"ssl",
               "vpn_route_type":1
          },
          "ssl":{
               "basic":{
                    "username":"demo",
                    "password":"samsung",
                    "authentication_type":1,
                    "splitTunnelType":0,
                    "forwardRoutes":[
                         {
                              "route":""
                         }
                    ]
               },
               "algorithms":{
                    "ssl_algorithm":0
               }
          },
          "knox":{
               "connectionType":"keepon",
               "chaining_enabled":"-1",
               "uidpid_search_enabled":"0"
          },
          "vendor":{
               "setCertCommonName":"space",
               "SetCertHash":"pluto",
               "certAuthMode":"Automatic"
          }
     }
}
```

Certificate (Android Enterprise)

You can install a user certificate on a device and use the certificate through Wi-Fi or on websites. You can add more certificate policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each certificate setting.
Description	Enter a description for each certificate setting.
Automatic Installation	Select whether to install each certificate automatically. The default value is **Use**. However, if you set only one certificate, it will be automatically installed. **NOTE** • Certificates are installed per the setting values of the automatic installation only when devices have EMM Agent v2.5.5 and the server is EMM v2.5.5 or higher. • For certificate settings created on lower versions than EMM v2.5.5, the automatic installation value will be displayed as **Do not use**.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. - **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. - **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Certification category	Select a certification category when **EMM Management Certificate** is selected in **User certificate input method**, • **CA certificate**: Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **CA Cert** and the Type set as **Root** will appear on the list. • **User certificate**: Select a certificate to use from the User Certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose has been set as **CA Cert** and the Type set as **User** will appear on the list.

Configuring Samsung Knox (Android Enterprise) Policies

Create a profile and register policies only for Android Enterprise manage type Samsung devices. You can configure the policies below for Android Enterprise devices.

→ System (Android Enterprise-Samsung Knox)
Provides data sharing or save settings, developer options, and other features.

→ Interface (Android Enterprise-Samsung Knox)
Controls the network settings, such as Wi-Fi Hotspot and Bluetooth tethering, and controls the USB media player settings.

→ Security (Android Enterprise-Samsung Knox)
Configures security settings, such as the Google Android security update policy.

→ Kiosk (Android Enterprise-Samsung Knox)
Configures the Kiosk device settings.

→ Application (Android Enterprise-Samsung Knox)
Configures the battery optimization exceptions setting.

→ Browser (Android Enterprise-Samsung Knox)
Configures the settings for the default web browser and Chrome browser.

→ Phone (Android Enterprise-Samsung Knox)
Configures the phone settings, such as the cellular network settings.

→ Firewall (Android Enterprise-Samsung Knox)
Configures the IP or a domain firewall policy for each application.

→ DeX (Android Enterprise-Samsung Knox)
Allows the use of DeX mode, an interface to use a mobile device like a desktop.

→ Dual DAR (Android Enterprise-Samsung Knox)
You can set policies, such as the **Data Lock Timeout** and **Restrict DE Storage Access**, for the Dual DAR area on devices. Fully Managed Dual DAR only supports devices with Android 12 or higher, and Work Profile on company-owned Dual DAR supports devices with Android 11 or higher only.

→ APN (Android Enterprise-Samsung Knox)
Configures the APN (Access Point Name) settings.

System (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Allow Remote Control	Allows remote control within the Work Profile via Remote Support. Remote Support should be installed in the personal area. **NOTE** • Policy changes using Remote Support in the Work Profile do not apply to the Remote Support Viewer immediately. In this case, reload the Work Profile area. • This policy is not available for the high security version.	DO/PO: Samsung Knox 2.2 or higher
Domain blacklist Settings	Allow using the domain blacklist.	
> Domain blacklist	Enter a domain blacklist that should not be used when registering an Exchange or email account. • To add a domain, enter the domain name in the field, and click +. • To delete a domain, click 🗑 next to the added domain name.	DO: Samsung Knox 1.0 or higher
Power off	Allows powering off the device. **NOTE** • If this policy is disallowed, the use cannot turn off the device and cannot perform factory rest. • The device command from an administrator for factory reset is also blocked.	DO: Samsung Knox 1.0 or higher WP-C
OTA Upgrade	Allows an OTA upgrade for the device.	DO: Samsung Knox 1.0 or higher WP-C
Settings	Allows the configuration changes within the System Settings.	DO: Samsung Knox 1.0 or higher WP-C

Policy	Description	Supported devices
App crash report to Google	Allows reporting the application error occurrence information to Google.	DO: Samsung Knox 1.0 or higher
Expand status bar	Allows the expansion of the status bar.	DO: Samsung Knox 1.0 or higher
Clipboard	Allows using the clipboard feature and sets the range. • **Allow**: Allows the clipboard feature throughout the entire system. • **Disallow**: Disallows the clipboard feature throughout the entire system. • **Allow within the same app**: Allows using the clipboard feature only within the same application.	DO/PO: Samsung Knox 2.0 or higher
Share via apps	Allows the share app feature.	DO/PO: Samsung Knox 4.0 or higher
Smart Select	Allows using the Smart Select, which is one of the Samsung device features. It allows users to clip a content by drawing a circle with the S pen. Clipped contents can be used on notes or anywhere else.	DO: Samsung Knox 5.2 or higher
Developer mode	Allows using a developer mode.	DO: Samsung Knox 5.0 or higher WP-C
> Mock location	Allows using a mock location, which specifies an arbitrary location for development or test purposes. Use this policy if the location information from the Update Device Information in the Send Device Command seems incorrect.	DO: Samsung Knox 1.0 or higher
> Background process limitation	Allows setting the number of background processes. If this policy is disabled, the default number of background processes will be set at the maximum number.	DO: Samsung Knox 1.0 or higher
> Quit application upon killing activities	Enables closing all running applications when the user logs out of the device. If this policy is disabled, the activation setting is disabled on the device and the user cannot control the device settings.	DO: Samsung Knox 1.0 or higher
Reboot banner	Allows using the reboot banner which appears on the user's device when the device reboots.	DO: Samsung Knox 1.0 or higher WP-C

Policy	Description	Supported devices
> Reboot banners stationery	Enter the text for the reboot banner. You can enter up to 1000 bytes. **NOTE** You can customize banners for Samsung Knox 2.2 + devices. For Samsung Knox 1.0 devices, only the message or banner registered by the manufacturer is displayed.	DO: Samsung Knox 2.2 or higher WP-C
Control Power saving mode	Allows power saving controls on the device.	DO: Samsung Knox 5.8 or higher
Firmware download mode control	Allows using the hardware key on the device to update firmware. • **Disallow**: Allows navigating download mode using the hardware key but disallows firmware updates.	DO: Samsung Knox 5.0 or higher WP-C
Samsung Keyboard settings control	Allows accessing the settings key from the Samsung keyboard.	DO: Samsung Knox 5.0 or higher
Data saver mode	Allows the setting of a device in **Settings** > **Connections** > **Data saver**. If you use the data saver mode, apps running in the background (e.g., EMM Agent) on the device cannot use mobile data **NOTE** If the data saver mode policy is disallowed on the devices running Android 9 (Pie), all apps previously selected as “Allow app while Data saver on” will be removed from the target. If the data saver mode policy is disallowed on the devices running Android 7, all apps selected as “Use without data restriction” will be removed from the target. However, if the data saving mode policy is allowed, apps that were previously selected as “Use without data restriction” will be displayed again.	DO: Samsung Knox 2.7.1 or higher

Interface (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
NFC Control	Allows NFC (Near Field Communication) control.	DO: Samsung Knox 1.0 or higher
USB host storage (OTG)	Allows a device connection via OTG (On the Go). OTG controls only the storage items and not the non-storage items, such as a keyboard or mouse. **NOTE** To use DeX, configure the policy to allow DeX mode. If the configuration value is set as either allow or disallow, make the USB exception list as below: • **Using DeX only**: All block. • **Using DeX, Keyboard, and Mouse**: Hid. • **Using DeX, Keyboard, Mouse, Ethernet**: Hid, Communication, Cdc Data, Vendor Spec.	DO: Samsung Knox 1.0 or higherWP-C
> Set usb exception allowed list	Select an USB interface to use if the USB host storage (OTG) policy is disallowed.	
>> USB exception allowed list	Select the USB interface to use from the USB exception allowed list. For more information, see https://www.usb.org/defined-class-codes.	DO: Samsung Knox 3.0 or higher
Wi-Fi hotspot	Specify using mobile Wi-Fi hotspot on the device. **NOTE** Android 13 and later, this policy is no longer support.	DO: Samsung Knox 1.0 or higher WP-C

Policy	Description	Supported devices
Xj.Gj!TTJE!xijufmjtu!tfuujoh	Bmmpxt!vtjoh!uif!Xj.Gj!TTJE!xijufmjtu/!Efwjdft!dbo!poez!dpoofdu!up!uif!Xj.Gj!BQt!po!uif!xijufmjtu/ **NOTE** • Gps!opo.Tbn tvoh!efwjdft!xju i!Boespje!9/1!ps!b!ijhifs!wfstjpo-!uijt!qpmjdz!dbo!poez!cf!bqqmjfe!xifo!ju!ibt!cffo!bhsffe!up!hsbou!bddftt!up!mpdbujpo!jogpsn bujpo/ • Boespje!24!boe!mbufs-!uijt!qpmjdz!jt!opmpohfs!tvqqpsu/ • Jo!psefs!up!vtf!uijt!qpmjdz-!Xj.Gj!TTJE!gpsFNN!mphjo!tipvme!cf!beefe!jo!uif!Xj.GjTTJE!Xijufmjtu/!Jg!opu-!uif!efwjdf!xjmm!gbjmup!mphjo!xifo!uif!Xj.Gj!TTJE!jt!opu!xijuf.mjtufe/	
? Xj.Gj!TTJE xijufmjtu	Bee!Xj.Gj!BQt!up!uif!xijufmjtu/!Uijt!qpmjdz!jt!jssfmfwbou!up!beejoh!ps!efmfujoh!uif!Xj.Gj!tfuujoh!qspgjmf/ • Up!bee!b!Xj.Gj!BQ!fou fs!b!Xj.Gj!TTJE!boe!dmjdl!+/ • Up!bee!bm!Xj.Gj!BQt-!dmjdl!**Add all**!up!bddftt!uif!Xj.Gjmjtu/ • Up!efmfuf!b!Xj.Gj!BQ!tfmfdu!b!Xj.Gj!TTJE!boe!dmjdl!🗑/	EP;!Tbn tvoh!Lopy!2/1!ps!ijhifs XQ.D
Xj.Gj!TTJE!Cmbdlmjtu!tfuujoh	Bmmpxt!vtjoh!uif!Xj.Gj!TTJE!cmbdlmjtu/!Efwjdft!dboopu!dpoofdu!up!Xj.Gj!BQt!po!uif!cmbdlmjtu/ **NOTE** • Gps!opo.Tbn tvoh!efwjdft!xju i!Boespje!9/1!ps!b!ijhifs!wfstjpo-!uijt!qpmjdz!dbo!poez!cf!bqqmjfe!xifo!ju!ibt!cffo!bhsffe!up!hsbou!bddftt!up!mpdbujpo!jogpsn bujpo/ • Boespje!24!boe!mbufs-!uijt!qpmjdz!jt!opmpohfs!tvqqpsu/	
? Xj.Gj!TTJE Cmbdlmjtu	Bee!Xj.Gj!BQt!up!uif!cmbdlmjtu/!Uijt!qpmjdz!jt!jssfmfwbou!up!beejoh!ps!efmfujoh!uif!Xj.Gj!tfuujoh!qspgjmf/ • Up!bee!b!Xj.Gj!BQ!fou fs!b!Xj.Gj!TTJE!boe!dmjdl!+/ • Up!bee!bm!Xj.Gj!BQt-!dmjdl!**Add all**!up!bddftt!uif!Xj.Gjmjtu/ • Up!efmfuf!b!Xj.Gj!BQ!tfmfdu!b!Xj.Gj!TTJE!boe!dmjdl!🗑/	EP;!Tbn tvoh!Lopy!2/1!ps!ijhifs XQ.D
Xj.Gj!bvup!dpoofdujpo	Bmmpxt!bvupn bujd!dpoofdujpo!up!uif!Xj.Gj!TTJE!bmsfbez!tupsfe!jo!uif!efwjdf/ **NOTE** Boespje!24!boe!mbufs-!uijt!qpmjdz!jt!op!mpohfs!tvqqpsu/	EP;!Tbn tvoh!Lopy!2/1!ps!ijhifs XQ.D

Policy	Description	Supported devices
Wi-Fi minimum security level setting	Set a minimum security level for Wi-Fi. **NOTE** • The security level increases in the following ascending order: OPEN < WEP < WPA < LEAP, PWD < FAST, PEAP < TSL, TTLS, SIM, AKA, AKA' • Android 13 and later, this policy is no longer support.	DO: Samsung Knox 1.0 or higher WP-C
USB tethering	Allows USB tethering.	DO: Android 4.3 or higher, Samsung Knox 1.0 or higher WP-C
Bluetooth tethering	Allows Bluetooth tethering to share the internet connection from one device to another.	DO: Samsung Knox 1.0 or higher WP-C
Bluetooth UUID Whitelist Setting	Allows connecting Bluetooth devices based on their Universal Unique Identifier (UUID).	
> Bluetooth UUID whitelist	Select devices to allow Bluetooth connections with. Click the checkboxes for **Audio**, **File transfer**, **Phonebook**, **Headsets**, or **Hands-free**. **NOTE** When updating the policy, current Bluetooth connection gets disconnected. Users must reconnect.	DO: Samsung Knox 2.2 or higher
Bluetooth UUID Blacklist Setting	Allows disconnecting Bluetooth devices based on their Universal Unique Identifier (UUID).	
> Bluetooth UUID blacklist	Select devices to block Bluetooth connections with. Click the checkboxes for **Audio**, **File transfer**, **Phonebook**, **Headsets**, or **Hands-free**. **NOTE** When updating the policy, current Bluetooth connection gets disconnected. Users must reconnect.	DO: Samsung Knox 2.2 or higher
USB Debugging	Allows USB debugging.	DO: Samsung Knox 1.0 or higher PO: Android 5.0 or higher WP-C

Policy	Description	Supported devices
Allow USB Devices for Default Access by App	Set whether to grant user permission for one or more USB devices to be used by a particular package. • **Allow**: Allow user permission for USB devices to be used by a particular package. Supported by Samsung Knox 2.5 or higher devices. • **Disallow**: Disallow user permission for USB devices to be used by a particular package. Supported by Samsung Knox 2.1 or higher devices. **NOTE** • Verizon devices are not supported. • A KPE license is required to apply policies to the Work Profile.	DO/PO: Samsung Knox 2.1 or higher
> Package & Vendor List	Add USB devices to allow user permission in the particular package. • To add an USB device enter a package name, vendor Id and product Id and click +. • To delete a package & vendor name, select the package & vendor name and click 🗑.	

Security (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Google Android security update policy	Allows the user to select whether to receive updates on the device. • **Forced use**: Set to receive security updates by default.	DO: Samsung Knox 2.6 or higher

Kiosk (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Task manager	Allow the use of the Task Manager.	DO: Samsung Knox 1.0 - 2.4
System bar	Use the System bar which refers to the Status bar in the Notifications area at the top of the device and the Navigation bar in the Buttons area at the bottom. For non-Samsung devices, even if you selected either **Allow status bar only** or **Allow navigation bar only**, both the status bar and the navigation bar will be disabled.	DO: Samsung Knox 1.0 or higher
Multi Windows	Allows the use of multiple windows. This is available for devices that provide the functionality of multiple windows.	DO: Samsung Knox 1.0 or higher
Air command	Allows the use of Air command. Air command is a function provided on Samsung devices. Menu items appear when the user brings an S pen close to the screen.	DO: Samsung Knox 2.2 or higher
Air view	Allows the use of Air view. Air view is a function provided on Samsung devices. Users can preview a picture or email when they bring the S pen or finger close to the picture or other content.	DO: Samsung Knox 2.2 or higher
Edge screen	Allows the use of the Edge screen of the device. The Edge screen allows users to create shortcuts on the edges of the screen panel to frequently used applications, favorite contacts, or the camera.	DO: Samsung Knox 2.5 or higher

Application (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Battery optimization exceptions	Set to exempt applications from the battery optimization mode. **NOTE** This policy may cause battery loss.	DO: Samsung Knox 2.7 or higher
> Apps excluded from battery optimization	Add applications to be exempted from battery optimization mode. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	
App installation authority whitelisting settings	Set the applications with installation permissions on Work Profile.	PO: Samsung Knox 3.0 or higher
> App installation authority whitelist	Add applications to allow installation on the Work Profile. Selected applications will be added to the View list with the package name of the applications. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	
Application black/ whitelist settings	Set to control the application installation policies. • **Application blacklist settings**: Blacklist is the list of applications that should not be installed on the user devices. • **Application whitelist settings**: Whitelist is the list of applications that could be installed on the user devices.	

Policy	Description	Supported devices
> Application installation blacklist	Add applications to prohibit their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click  next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Blacklisted applications cannot be installed and will be deleted even if they were previously installed. • An application that has been added on the **Application installation whitelist** cannot be added. • Preloaded applications and EMM applications (the EMM Agent, Samsung SDS Push, etc.) cannot be registered in the application installation blacklist.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Application installation whitelist	Add applications to allow their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Any applications not on the whitelist are deleted, even if they are not on the blacklist. • An application that has been added on the **Application installation blacklist** cannot be added. • If you register at least one application in the application whitelist, all preloaded applications, EMM applications (the EMM Agent, Samsung SDS Push, etc.), and Kiosk applications will be also installed on the devices.	Samsung Knox 1.0 or higher

Browser (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Cookies	Allows cookies in the Android browser. **NOTE** If cookies are not allowed, you cannot access websites that authenticate users with cookies.	DO: Samsung Knox 1.0 or higher

Policy	Description	Supported devices
JavaScript	Allows JavaScript in the Android browser.	DO: Samsung Knox 1.0 or higher
Autofill	Allows auto-completion of information that you enter on websites in the Android browser.	DO: Samsung Knox 1.0 or higher
Pop-up block	Allows blocking pop-up window in the Android browser.	DO: Samsung Knox 1.0 or higher
Browser proxy URL	Set the proxy server address for the Android browser. Enter the value in the form of IP:port or domain:port in the fields. **NOTE** • The Chrome browser and Samsung S browser are supported. • The supported version for Chrome is Knox 4.0.1 - 5.6.	DO: Samsung Knox 1.0.1 or higher

Phone (Android Enterprise-Samsung Knox)

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.

The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Prohibit voice call	Prohibits incoming and outgoing voice calls.	
> Voice call	Specifies the types of voice calls to block: • **Incoming**: Blocks incoming voice calls only. • **Outgoing**: Blocks outgoing voice calls only. If both are selected, only emergency calls can be made or received.	DO: Samsung Knox 1.0 or higher WP-C
Disallow SMS/MMS	Allows sending and receiving SMS/MMS messages.	
> Disallow Incoming/ Outgoing SMS/ MMS	Select the types of SMS/MMS messages to disable. **NOTE** At least one of the types should be selected.	DO: Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Incoming SMS blacklist	Add phone numbers to the blacklist to block incoming SMS/MMS messages. • To add a phone number, enter it in the field and click ⊕. • To delete a phone number, click 🗑 next to it.	
> Outgoing SMS blacklist	Add phone numbers to the blacklist to block outgoing SMS/MMS messages. • To add a phone number, enter it in the field and click ⊕. • To delete a phone number, click 🗑 next to it.	
WAP push during roaming	Allows WAP push communications while roaming.	DO: Samsung Knox 1.0 or higher
Data sync during roaming	Allows data synchronization while roaming.	DO: Samsung Knox 1.0 or higher
Voice calls during roaming	Allows voice calls while roaming.	DO: Samsung Knox 1.0 or higher
Use SIM card locking	Prevents the use of the SIM card on a user device. To use this policy, the default PIN of the SIM card should be entered. Then, the new PIN number for the SIM card should be entered. If the locked SIM card is registered to another device, the device is locked and the user must enter a valid PIN to unlock it. **NOTE** eSIM does not support the **Use SIM card locking** policy.	DO: Samsung Knox 1.0 or higher
> Default SIM PIN	Enter the default PIN found on the SIM card. The value is 4 - 8 digit numbers. **NOTE** This policy is intended for use by Corporate-Owned, Personally Enabled (COPE) devices and is only applied if the PIN found on the SIM card matches the default PIN.	
> New SIM PIN	Enter the new PIN number for the SIM card. The new PIN number can be found next to **SIM PIN Number** in the “Network“ tab of the “Device Detail” page. The value is 4 - 8 digit numbers.	

Firewall (Android Enterprise-Samsung Knox)

Firewall configuration sets rules to block access to the network. You can add more firewall policy sets by clicking +.

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Firewall	Set to use the firewall to set target IP addresses. If the policy is not applied, the firewall is enabled by default. Enable policy is used to set IPs and ports to be excluded from the Disable policy. **NOTE** If the firewall policy is set incorrectly, communication between the EMM server and the EMM Agent is failed, and device control is not possible.	

Policy	Description	Supported devices
> Permitted policy (IP)	Enter the target IP Address (range) and Port (range) to permit and select the network interface that can access the network. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the IP Address (range) and Port (range). 3. Select the Network Interface. 4. Select the Network Type: • **All** • **Data**: Only mobile network access is enabled. • **Wi-Fi**: Only Wi-Fi network access is enabled. 5. Select Port Range: • **All** • **Local**: Port access from the device is enabled. • **Remote**: Port access from the target server is enabled. 6. Click + to add. **NOTE** • To permit the target IPs, ports, and networks, you must set the IP Address (range) and Port (range) to * in Prohibited policy (IP). • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings.	DO/PO: Samsung Knox 2.5 or higher WP-C

Policy	Description	Supported devices
> Prohibited policy (IP)	Enter the target IP Address (range) and Port (range) to prohibit and select the network interface to prohibit network access. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Enter the IP Address (range) and Port (range). • Enter a wildcard character (*) as an IP Address to prohibit the use of the bandwidth. 3. Select the Network Interface. 4. Select Network Type: • **All** • **Data**: Mobile network access is disabled. • **Wi-Fi**: Wi-Fi network access is disabled. 5. Select Port Range: • **All** • **Local**: Port access from the device is disabled. • **Remote**: Port access from the target server is disabled. 6. Click + to add. **NOTE** • When entering the IP address, you can use a wildcard character (*) to disable the bandwidth usage. • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings.	DO/PO: Samsung Knox 2.5 or higher WP-C

Policy	Description	Supported devices
> Permitted policy (Domain)	Input values to permit the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** • To allow specific domains only, you must set all domains in the **Prohibited policy (Domain)** using the wildcard then allow specific domains. • Use a wildcard character (*) to allow the use of a specific domain. The wildcard must be placed before or after the address and not in the middle. e.g.) *android.com / www.samsung*	DO/PO: Samsung Knox 2.6 or higher WP-C
> Prohibited policy (Domain)	Input values to prohibit the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** Use a wildcard character (*) to prohibit a specific domain.	DO/PO: Samsung Knox 2.6 or higher
> DNS setting	Input values to specify the domain server address of all applications or registered applications. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input DNS values. • **DNS1**: Primary DNS. • **DNS2**: Secondary DNS. **NOTE** Only one DNS per application can be set and it is effective only when there are no VPN or Proxy policies assigned to the application.	DO/PO: Samsung Knox 2.7 or higher WP-C

NOTE

- If there are multiple firewalls, restricted firewalls have a higher priority.
- If a firewall is configured to all applications as well as in specific applications, the policy for each application has a higher priority.
- For example, specify firewall Enable/Disable policies as follows to allow only specific domains in Chrome:
  - Enable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *.samsungknox.com
  - Disable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *
- Firewall settings supports IPv6 for SDK 2.6 or later. Even if IPv4 and IPv6 addresses refer to a physically identical address, each must be configured separately.

DeX (Android Enterprise-Samsung Knox)

Samsung DeX is an accessory that extends the functionalities of a mobile device. By connecting a monitor, keyboard, and mouse to a Dex docking station, the mobile device can function as a desktop computer. In EMM, you can allow the use of DeX mode and control applications according to the Application execution blacklist setting.

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue. The policies are supported only on devices running Android 11 or higher.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Allow DeX Mode	Allows the use of DeX mode. • **Disallow**: The DeX station will not function even if a mobile device is mounted on it.	DO: Samsung Knox 3.0 or higher
Allow Ethernet Only	Allows ethernet only for DeX. Mobile data, Wi-Fi, and tethering are blocked.	DO: Samsung Knox 3.0 or higher
Application execution blacklist(Android)	Use the blacklist for running DeX applications.	

Policy	Description	Supported devices
> Application execution blacklist	Prohibits launching the specified applications. When this policy is enabled and applied, the icons of the blocked applications will disappear so that users cannot launch them. However, the applications are not deleted. The icons will reappear once the policy is changed or EMM is disabled. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** Any applications that already have been added to the Application whitelist cannot be added to the Application blacklist.	DO: Samsung Knox 3.0 or higher

Dual DAR (Android Enterprise-Samsung Knox)

This policy is supported in the Work Profile on company-owned type. To use the Dual DAR area for Fully Managed or Work Profile on company-owned devices, select “Yes” for Dual DAR when adding users or organizations. Also, to activate the device as a Work Profile on company-owned type, select “Yes” for Work Profile on company-owned.

Fully Managed will be referred to as DO (Device Owner).

Work Profile will be referred to as PO (Profile Owner).

IT admins can also choose to turn on the Highlight Work Profile on company-owned Devices Profile Only setting to show the available policies highlighted in blue.
The policies are supported only on devices running Android 12 or higher for Fully Managed DAR, and are supported only on devices Android 11 or higher for Work Profile on company-owned Dual DAR.
The personal area on a Work Profile on company-owned device is called WP-C.

Policy	Description	Supported devices
Data Lock Timeout (Minutes)	Sets the data lock timeout. Sets data lock timeout on Fully Managed or Dual DAR Work Profile area. The Dual DAR Workspace will be changed to the data lock state when the set time elapses after screen lock. For Fully Managed (DO) types: • The minimum time for the setting is 5 minutes. The default setting is unlimited and devices are unlocked. For the Work profile on company-owned (WP-C) type: • The minimum time you can set is 1 minute. The default setting is unlimited, and devices are unlocked. **NOTE** • When setting the Dual DAR area data lock function, the device and Work Profile password policies should be set. You must set the passwords in **Android Enterprise** > **Security** > **Device Password** and **Android Enterprise** > **Security** > **Work Profile Password**. • The Dual DAR data lock function is Smart Lock and it is impossible to lock the data unless the screen is locked in either the Fully Managed or Dual DAR Work Profile area. You must set it up in **Android Enterprise** > **Security** > **Work Profile** > **Block functions on lock screen** > **Trust Agent.** • When Dual DAR data lock is activated, biometric authentication is disabled. When you set a policy, be aware that the fingerprint/iris lock function is not available.	DO/PO: Samsung Knox 3.3 or higher
Restrict DE Storage Access	Sets the access restriction of an application to DE (Device Encrypted) space when the Fully Managed or Dual DAR Work Profile area is locked.	DO/PO: Samsung Knox 2.0 or higher

Policy	Description	Supported devices
Whitelisted Apps for Data Lock and DE Storage Access	When locking Dual DAR data, all general applications will stop working due to Knox security policies. Sets a whitelist to allow certain applications to access even when data is locked. Applications on the whitelist can access a DE space even if **Restrict DE Storage Access** is restricted. **NOTE** • If you use the Dual DAR for a third party encryption app, the app will be automatically included on the whitelisted apps list. • To apply the changed policies, send a device command in **Device Command > Apply the Latest Profiles** and reboot the device.	
> Whitelisted Apps	Add an application to allow it to run. EMM applications are automatically registered on the whitelist. • To add an application, click **Add**, and then select applications in the "Select Application" window. • To delete applications, click 🗑 next to the added application.	DO/PO: Samsung Knox 2.0 or higher

APN (Android Enterprise-Samsung Knox)

You can add more APN policy sets by clicking ⊕.

NOTE APN policies are not supported on Work Profile (PO) areas of devices with Android 13 or higher.

Policy	Description
Configuration ID	Enter an APN name to be displayed on the device.
Description	Enter a description for an APN.
Remove available	Allows users to delete APN settings in the EMM Client only. If you choose **Disallow**, then the button used to delete APN settings is disabled.
Access Point Name (APN)	Enter the name of the access point.
APN Type	Select the type of the access point. • **Default**: default type. • **MMS**: Multimedia Messaging Service. • **Supl**: IP-based protocol to receive GPS satellite signals.
Mobile Country Code (MCC)	Enter the country code for the APN.

Policy	Description
Mobile Network Code (MNC)	Enter the carrier network code for the APN.
MMS Server (MMSC)	Enter the server information for sending multimedia messages. • **MMS Proxy Server**: Enter the information of the proxy server for sending multimedia messages. • **MMS Proxy Server Port**: Enter the port number of the proxy server for sending multimedia messages.
Server	Enter the WAP gateway server name.
Proxy Server	Enter the information of the proxy server.
Proxy Server Port	Enter the port number of the proxy server.
Access Point User Name	Enter the user name of the access point. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Access Point Password	Enter the password of the access point. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Authentication Method	Select an authentication method. • **None**: Disables authentication. • **PAP**: Requires a user name and password for authentication. • **CHAP**: Uses encryption with a Challenge string for authentication. • **PAP or CHAP**: Uses the PAP or CHAP authentication method.
Set as Preferred APN	Applies APN settings to the device.

Configuring Android Legacy Policies

Create a profile and register policies for Android Legacy devices.

You can configure the policies below for Android Legacy devices. The availability of each policy varies depending on the OS version.

→ System (Android Legacy)

Provides backup and restore settings, developer options, and other features. Updates the operating system on a device.

→ Interface (Android Legacy)

Allows the use of GPS and controls the network settings, such as Bluetooth, Wi-Fi Direct, and tethering.

→ Security (Android Legacy)

Configures the security settings, such as the password and lock screen.

→ Kiosk (Android Legacy)

Configures Kiosk applications on a Kiosk device and controls the device settings.

→ Application (Android Legacy)

Configures options for application controls such as installation, verification, and permission.

→ Location (Android Legacy)

Collects location data from a device.

→ Browser (Android Legacy)

Allows the use of the default web browser and configures the settings for it.

→ Phone (Android Legacy)

Configures the phone settings, such as airplane mode, the microphone, and the cellular network settings.

→ Firewall (Android Legacy)

Configures the IP or a domain firewall policy for each application.

→ Logging (Android Legacy)

Allows performing logging and configuring the settings.

→ DeX (Android Legacy)

Allows the use of DeX mode, an interface to use a mobile device like a desktop.

→ Wi-Fi (Android Legacy)

Configures the Wi-Fi settings, such as SSID, security type, and proxy. Android 13 and later, this policy is no longer support.

→ Exchange (Android Legacy)

Configures the Microsoft Exchange ActiveSync account to synchronize email, calendar, contacts, and tasks from the Exchange account.

→ Email Account (Android Legacy)

Configures the POP/SMTP server in order to view the incoming and outgoing emails through the email account used on the device.

→ Bookmark (Android Legacy)

Configures the bookmark settings such as the icons and URL that will be displayed on devices.

→ APN (Android Legacy)

Configures the APN (Access Point Name) settings. Android 13 and later, this policy is no longer support.

→ Knox VPN (Android Legacy)

Configures a VPN (Virtual Private Network) on Samsung Galaxy devices. Android 13 and later, this policy is no longer support.

→ VPN (Android Legacy)

Configures a VPN (Virtual Private Network) on Android devices. Android 13 and later, this policy is no longer support.

→ Certificate (Android Legacy)

Set the certificate and the user authentication method on devices for when device users authenticate. Android 13 and later, this policy is no longer support.

System (Android Legacy)

Policy	Description	Supported devices
Factory reset	Allow users to factory reset devices in the Settings menu. • **Disallow**: Factory reset using the hardware button is prevented. However, factory reset using the firmware update utility cannot be prevented.	Samsung Knox 1.0 or higher
Power off	Allows powering off the device. • **Disallow**: The power off option menu does not appear even with the use of a power button. However, powering off by separating the battery cannot be prevented. Factory reset is prohibited if this policy is disallowed.	Samsung Knox 1.0 or higher
Backup	Allows backup of the device data.	Samsung Knox 1.0 or higher
OTA upgrade	Allows an OTA upgrade for the device.	Samsung Knox 1.0 or higher
Settings	Allow users to change of device settings from the Settings menu.	Samsung Knox 1.0 or higher
System app close	Allows force closing system applications.	Samsung Knox 1.0 or higher
App crash report to Google	Allows reporting the application error occurrence information to Google.	Samsung Knox 1.0 or higher
Multiple users	Allow registering additional users to the device.	Samsung Knox 1.0 or higher
Expand status bar	Allows the expansion of the status bar.	Samsung Knox 1.0 or higher
Change wallpaper	Allows changing the home and the lock screens.	Samsung Knox 1.0 or higher
Automatic Date and Time	Allows changing the date and time. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Camera	Allows using the camera. **NOTE** • If the camera in the general area is restricted, the camera in the Knox Workspace is also restricted. • It is not supported on devices other than Samsung Android 10(SDK29) or higher. • If the firmware of a non-Samsung is upgraded to Android 10(SDK29) or higher, the camera policy already applied to the device is maintained, but it is not applied even if the administrator changes or remove the policy. The camera policy can be canceled only by deactivating the device.	Samsung Knox 1.0 or higher, Android 9.0 or higher
> Face recognition camera	Allows use of the camera for face unlock even when the camera is disabled in the Camera policy. This policy is available when **Camera** is set to **Disallow all**.	Samsung Knox 3.2.1 or higher
Screen capture	Allows use of the screen capture function, which is already set as default.	Samsung Knox 1.0 or higher
Clipboard	Allows the clipboard feature throughout the entire system. • **Allow within the same app**: Allows using the clipboard feature only within the same application.	Samsung Knox 1.0 or higher
Share via apps	Allows the share app function.	Samsung Knox 1.0 or higher
S Beam	Allows using Android Beam which transfers data via NFC.	Samsung Knox 1.0 or higher
Encryption for storage	Specifies the encryption of the device's system storage or the external SD card.	Samsung Knox 1.0 or higher, Android 4.1 or higher
> Storage encryption	Check the checkbox to select the storage to be encrypted. **NOTE** External SD card encryption is applicable to Samsung Galaxy devices only.	
External SD Card	Allows using the external SD card.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Write to external SD card	Allows writing to an external SD card. **NOTE** If the external SD card policy is allowed but the Write to external SD card policy is not, then external SD cards can only be read and do not have reset control.	Samsung Knox 1.0 or higher
Unauthorized SD Card	Allows using unauthorized SD cards.	Android 1.0 (SDK1 or higher)
If compromised OS is detected	Select the control function to be triggered if device OS tampering is detected. • **Lock device**: Locks the device. **NOTE** Android 10 (Q) or higher devices are not supported. • **Lock Email**: Locks email use. • **Factory reset + Initialize SD card**: Simultaneously factory resets the user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. **NOTE** The factory reset function is unsupported in Android 2.0 or lower. To reset the device, select the Factory reset + Initialized SD card option.	Samsung Knox 1.0 or higher
Smart Select	Allows using the Smart Select, which is one of the Samsung device features. It allows users to clip a content by drawing a circle with the S pen. Clipped contents can be used on notes or anywhere else.	Samsung Knox 2.2 or higher

Policy	Description	Supported devices
Device Administrators to install and activate apps	Specifies to run or install EMM applications such as AirWatch MDM other than the EMM application. • **Allow**: Allow the installation and activation of device administrator apps. • **Disallow installation**: Disallow installation of device administrator apps. If Disallow Installation is selected, specific apps can be added to exceptions for installation. • **Disallow activation**: Disallow activation of device administrator apps. If Disallow Activation is selected, specify apps can be added to exceptions for activation. **NOTE** App installation and activation cannot be controlled if a similar app that controls the device is enrolled in the device administrator before configuring the policy.	Samsung Knox 2.0 or higher
> Exceptional app whitelist	Allows installing or activating select EMM applications by adding them to the whitelist. This policy is available only when the Device Administrator to Install and Activate apps policy is set to **Disallow installation** or **Disallow activation**. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. • **Disallow installation**: Only the whitelisted applications are allowed to be installed. • **Disallow activation**: Only the whitelisted applications are allowed to be activated.	Samsung Knox 2.0 or higher
Developer mode	Allows using the developer mode.	
> Background process limitation	Allows setting the default number of background processes. If this policy is disabled, the number of background processes will be set at the maximum number.	Samsung Knox 1.0 or higher
> Quit application upon killing activities	Enables closing all running applications when the user logs out of the device. If this policy is disabled, the activation setting is disabled on the device and the user cannot control the device settings.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Mock location	Allows using the mock location, which specifies an arbitrary location for development or test purposes. Use this policy if location information from the Update Device Information of the Send Device Command seems incorrect.	Samsung Knox 1.0 or higher
Safe mode	Allows using Safe Mode. This policy retains device control functions such as camera control, but not EMM applications and preloaded applications.	Samsung Knox 1.0 or higher
Reboot banner	Allows using the reboot banner which appears on the user's device when the device reboots.	Samsung Knox 1.0 or higher
> Reboot banners stationery	Enter the text for the reboot manager. You can enter up to 1000 bytes. **NOTE** You can customize banners for Samsung Knox 2.2 or higher devices. For Samsung Knox 1.0 devices, only the message or banner registered by the manufacturer is displayed.	Samsung Knox 2.2 or higher
Domain blacklist Settings	Allows using the domain blacklist.	Samsung Knox 1.0 or higher
> Domain blacklist	Enter a domain blacklist that should not be used when registering an Exchange or email account. • To add a domain, enter the domain name in the field, and click **Add**. • To delete a domain, click 🗑 next to the added domain name.	
NTP Settings	Allows using the NTP (Network Time Protocol) server. If NTP server is registered, the time information of the server can be applied to the device. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.5 or higher
> Server address	Enter the NTP server address.	Samsung Knox 2.5 or higher
> Maximum number of attempts	Set the maximum number of attempts for connecting to the NTP server to retrieve the time information. The value can be between 1 – 100 times.	Samsung Knox 2.5 or higher
> Polling cycle (hr)	Set the cycle to reconnect to the server via NTP. The value can be between 1 – 8760 hours (8760 = 1 year).	Samsung Knox 2.5 or higher

Policy	Description	Supported devices
> Short polling cycle (sec)	Set the cycle to re-connect to the NTP server after experiencing a timeout. The value can be between 1 – 1000 seconds.	Samsung Knox 2.5 or higher
> Timeout (sec)	Set the connection timeout on the NTP server. The value can be between 1 – 1000 seconds.	Samsung Knox 2.5 or higher
Set Notifications from an event to On.	Sets the device to display notifications when an event for device control is applied. • **User Defined**: Users can set event notifications on the device from the Settings menu of the EMM Agent. • **Show notification**: Displays the notification when an event for device control is applied. • **Hide notifications**: Hides the notification when an event for device control is applied.	Samsung Knox 1.0 or higher, Android 1.0 or higher
Set Notifications from an event to Off.	Sets the device to display the notifications when an event for device control is disengaged. • **User Defined**: Users can set event notifications on the device from the Settings menu of the EMM Agent. • **Show notification**: Displays a notification when an event for device control is disengaged. • **Hide notifications**: Hides a notification when an event for device control is disengaged.	Samsung Knox 1.0 or higher, Android 1.0 or higher
Fix Event Notification	Set the removal of the notification from the device Quick panel. • **User Defined**: Users can remove notification on the device from the settings menu of the EMM Agent. • **Disallow to Remove Notification**: Users cannot remove notifications on the device Quick Panel. • **Allow to Remove Notification**: Users can remove notifications on the device Quick Panel.	Samsung Knox 1.0 or higher, Android 1.0 or higher
Control Power saving mode	Allows power saving control on the device.	Samsung Knox 2.8 or higher
Firmware download mode control	Allows using the hardware key on the device to update firmware. • **Disallow**: Disallows updating firmware with the hardware key and performing a factory reset.	Samsung Knox 2.0 or higher
Samsung Keyboard settings control	Allows accessing the settings key from the Samsung keyboard.	Samsung Knox 5.0 or higher

Policy	Description	Supported devices
Data saver mode	Allows the setting of a device in **Settings** > **Connections** > **Data saver**. If you use the data saver mode, apps running in the background (e.g., EMM Agent) on the device cannot use mobile data. **NOTE** • If the data saver mode policy is disallowed on the devices running Android 9 (Pie), all apps previously selected as “Allow app while Data saver on” will be removed from the target. • If the data saver mode policy is disallowed on the devices running Android 7, all apps selected as “Use without data restriction” will be removed from the target. However, if the data saving mode policy is allowed, apps that were previously selected as “Use without data restriction” will be displayed again.	Samsung Knox 2.7.1 or higher

Interface (Android Legacy)

Policy	Description	Supported devices
Wi-Fi	Allows using Wi-Fi. If the Wi-Fi policy has not been applied successfully, the device will try to apply it again 30 minutes later after EMM is activated. **NOTE** • When a new device is enrolled, this policy is applied after internal applications with their installation types set as **Automatic (Non-removable)** are installed. • Non-Samsung devices running Android 10(SDK29) or higher the Wi-Fi On/Off prohibition policy. • Android 13 and later, this policy is no longer support. • **Allow**: Allows using Wi-Fi. • **Disable On**: Disallows turning on Wi-Fi. It is turned off at all times. • **Disable Off**: Disallows turning off Wi-Fi. It is turned on at all times.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Wi-Fi Direct	Allows use of the Wi-Fi Direct (Wi-Fi P2P) connection. **NOTE** • Set the Wi-Fi policy to **Allow** or **Disable Off** before using this policy. • Depending on the device type, the direct connection of the two devices may cause the function or the menu to get controlled.	Samsung Knox 1.0 or higher
Wi-Fi hotspot	Allows use of the Wi-Fi hotspot. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher, Android 2.3 or higher

Policy	Description	Supported devices
Wi-Fi SSID whitelist setting	Allows using the Wi-Fi SSID whitelist. Devices can only connect to the Wi-Fi APs on the whitelist. **NOTE** • For non-Samsung devices with Android 8.0 or a higher version, this policy can only be applied when it has been agreed to grant access to location information. • In order to use this policy, Wi-Fi SSID for EMM login should be added in the Wi-Fi SSID Whitelist. If not, the device will fail to login when the Wi-Fi SSID is not white-listed. • Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Wi-Fi SSID whitelist	Add Wi-Fi APs to the whitelist. This policy is irrelevant to adding or deleting the Wi-Fi setting profile. • To add a Wi-Fi AP, enter a Wi-Fi SSID and click **Add**. • To add all Wi-Fi APs, click **Add all** to access the Wi-Fi list. • To delete a Wi-Fi AP, select a Wi-Fi SSID and click 🗑.	Android 1.0 (SDK1) or higher Samsung Knox 1.0 or higher
Wi-Fi SSID Blacklist setting	Allows using the Wi-Fi SSID blacklist. Devices cannot connect to Wi-Fi APs on the blacklist. **NOTE** • For non-Samsung devices with Android 8.0 or a higher version, this policy can only be applied when it has been agreed to grant access to location information. • Android 13 and later, this policy is no longer support.	
> Wi-Fi SSID Blacklist	Add Wi-Fi APs to the blacklist. This policy is irrelevant to adding or deleting the Wi-Fi setting profile. • To add a Wi-Fi AP, enter a Wi-Fi SSID and click **Add**. • To add all Wi-Fi APs, click **Add all** to access the Wi-Fi list. • To delete a Wi-Fi AP, select a Wi-Fi SSID and click 🗑.	Samsung Knox 1.0 or higher, Android 1.0 or higher
Wi-Fi auto connection	Allows automatic connection to Wi-Fi SSID already stored in the device. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Wi-Fi minimum security level setting	Set a minimum security level for Wi-Fi. The security level increases in the following ascending order: OPEN < WEP < WPA < LEAP, PWD < FAST, PEAP < TSL, TTLS, SIM, AKA, AKA' **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher
Bluetooth	Allows using Bluetooth. • **Allow**: Allows using Bluetooth. • **Disable On**: Disallows turning on Bluetooth. It is turned off at all times. • **Disable Off**: Disallows turning off Bluetooth. It is turned on at all times. **NOTE** Samsung devices running Android 13 or higher do not support the **Disable Off** option, and non-Samsung devices do not support the **Disable On/Off** options.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Desktop PC connection	Allows Desktop PC connections with the user's device via Bluetooth. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher
> Data transfer	Allows data exchanges with other devices via Bluetooth connection.	Samsung Knox 1.0 or higher
> Search mode	Allows device search via Bluetooth.	Samsung Knox 1.0 or higher
> Bluetooth tethering	Allows Bluetooth tethering to share the internet connection with another device.	Samsung Knox 1.0 or higher, Android 4.2 or higher
Bluetooth UUID Black/Whitelist	Select a method to connect Bluetooth devices based on their Universal Unique Identifier (UUID). • **Blacklist configuration**: Set a device to block Bluetooth connections from certain devices. • **Whitelist configuration**: Set a device to allow Bluetooth connections to certain devices.	

Policy	Description	Supported devices
> Bluetooth UUID blacklist	Select devices to block Bluetooth connections with. Click the checkboxes for **Audio**, **File transfer**, **Phonebook**, **Headsets**, or **Hands-free**. **NOTE** When updating the policy, current Bluetooth connection gets disconnected. Users must reconnect.	Samsung Knox 1.0 or higher
> Bluetooth UUID whitelist	Select devices to allow Bluetooth connections with. Click the checkboxes for **Audio**, **File transfer**, **Phonebook**, **Headsets**, or **Hands-free**. **NOTE** When updating the policy, current Bluetooth connection gets disconnected. Users must reconnect.	Samsung Knox 1.0 or higher
NFC control	Allows NFC (Near Field Communication) control. **NOTE** • Samsung Knox 2.4 or higher is supported for Knox Workspace devices.	Samsung Knox 1.0 or higher
PC connection	Allows connecting user's device to PC.	Samsung Knox 1.0 or higher, Android 1.0 or higher
USB tethering	Allows USB tethering.	Samsung Knox 1.0 or higher, Android 1.0 or higher
USB host storage (OTG)	Allows a device connection via OTG (On the Go). OTG controls only the storage items and not the non-storage items, such as a keyboard or mouse. **NOTE** To use DeX when the USB host storage (OTG) policy is disallowed, enable DeX in the Set USB exception allowed list policy. Then configure the Allow DeX mode policy to Allow.	Samsung Knox 1.0 or higher
> Set usb exception allowed list	Specify the use for the exception allowed list once the USB host storage (OTG) policy is disallowed.	Samsung Knox 3.0 or higher
> USB exception allowed list	Select the USB interface to use if the USB host storage (OTG) policy is disallowed.	Samsung Knox 3.0 or higher

Policy	Description	Supported devices
USB debugging	Allows USB debugging.	Samsung Knox 1.0 or higher
Microphone	Allows use of the microphone.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Recording	Allows the use of microphone recording.	Samsung Knox 1.0 or higher
> S Voice	Allows the use of S Voice.	Samsung Knox 1.0 or higher
GPS	Allows using GPS. • **Allow**: Allows using GPS. • **Disable On**: Disallows turning on GPS. It is turned off at all times. • **Disable Off**: Disallows turning off GPS. It is turned on at all times. **NOTE** To use this policy, the GPS type on the user device must be set as one of the three types: High accuracy, Sleep, and GPS.	Samsung Knox 1.0 or higher
Wearable equipment policy inheritance	Set to use the existing Mobile policy for the Gear policy.	Samsung Knox 2.6 or higher

Security (Android Legacy)

Policy	Description	Supported devices
Device Password	Set the password for the device screen lock. Use of the camera is prohibited when the device is screen locked. **NOTE** • When a user has forgotten their screen lock password, an administrator needs to send the Reset screen password device command, and then the user needs to enter a temporary password. A temporary password is generated randomly according to the set Device Password policies. For more information, see the screen lock password in Viewing the device details. • The device password policy is not supported on devices running Android 10 (SDK29) or higher. • The device password policy is not supported on devices running Android 12(SDK31) or higher. • If the firmware is upgraded to Android 10(SDK 29) for non-Samsung devices and Android 12 (SDK 31) for Samsung devices, the policy already applied to the device is maintained and cannot be removed or changed. • For Knox Workspace devices with a One Lock password, the password policy which is stronger between the Android Legacy and Knox Workspace area will be applied.	
Device Password	**NOTE** • Certificates registered in the device will be deleted in the following cases: - when the EMM is activated on a device that has no password set. - if the minimum strength of the password is set with a pattern, or no password policy is set, in a device that requires more than a certain number of digits for the password.	

Policy	Description	Supported devices
> Minimum strength	Set the minimum password strength on the screen. The password strength increases in the following ascending order: Pattern < Numeric < Alphanumeric < Complex. • **Pattern**: Set the password using a pattern or a password with a higher degree of complexity. • **Numeric**: Set the password using numbers or a password with a higher degree of complexity. • **Must be alphanumeric**: Set the password using alphanumeric characters or a password with a higher degree of complexity. • **Must include special characters**: Set it so that the passwords must include alphanumeric and special characters. **NOTE** To set the password for a user certificate, select **Must be alphanumeric** or **Must include special characters**.	Samsung Knox 2.0 or higher, Android 2.2 or higher
>> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before access is restricted. The value can be between 1 - 10 times. **NOTE** • You can set this only when **Numeric**, **Must be alphanumeric**, or **Must include special characters** is selected. • Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher, Android 2.2 or higher

Policy	Description	Supported devices
>>> If maximum failed login attempts exceeded	Select the action to be performed when the maximum number of failed attempts is reached. **NOTE** • Samsung Knox 1.0 or higher is supported for Knox Workspace devices. • Android 13 and later, this policy is no longer support. • **Lock device**: Locks the device. **NOTE** Android 10 (Q) or higher devices are not supported. • **Factory reset + Initialize SD card**: Simultaneously resets the user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. This option is not applicable for devices with Android 2.0 or lower. To reset the device, select **Factory reset + Initialize SD card**.	Samsung Knox 2.0 or higher, Android 2.2 or higher
>> Minimum length	Set the minimum length of the password. The value can be between 4 - 16 characters. **NOTE** • If Minimum strength is set to Pattern, setting Minimum length does not apply. • Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher, Android 2.2 or higher
>> Expiration after (days)	Set the maximum number of days before the password must be reset. The value can be between 0 - 365 days. **NOTE** • Samsung Knox 2.0 or higher is supported for Knox Workspace devices. • Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher, Android 3.0 or higher

Policy	Description	Supported devices
>> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 0 - 10 times. **NOTE** • If the password is 'Knox123!' and the minimum value is set as 10, the user must use ten other passwords before reusing 'Knox123!' as password. • Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher, Android 3.0 or higher
>> Maximum length of sequential numbers	Set the maximum number of consecutive numeric characters allowed in a password. The value can be between 1 - 10 words.	Samsung Knox 1.0 or higher
>> Maximum length of sequential characters	Set the number of consecutive letters allowed in a password. The value can be between 1 - 10 words.	Samsung Knox 1.0 or higher
>> Block function setting on lock screen	Allows blocking functions on the lock screen. **NOTE** • The visibility of the notifications on the lock screen depends on the options you set in the application. • Samsung Knox 2.4 - 2.9 is supported for Knox Workspace devices. • The block function setting on lock screen policy is not supported on devices running Android 10 (SDK29) or higher.	Android 5.0 or higher

Policy	Description	Supported devices
>>> Block functions on lock screen	Select the function to be blocked on the lock screen when a password policy is set on a device. • **All**: Blocks all functions on the lock screen. • **Camera**: Blocks direct camera control on lock screen. • **Trust Agent**: Trust Agent notifies the system whether the device is in a safe condition. If you block the Trust Agent, the Smart Lock function will be blocked, which automatically unlocks the screen in certain conditions. • **Fingerprint**: Blocks the fingerprint unlock function. • **Previews in pop-ups**: Displays notifications on the lock screen but hides private content set in the application. • **Notifications**: All notifications are hidden via the lock screen. **NOTE** • This policy can be implemented only when the password level is set to pattern or higher. • For devices activated prior to EMM 1.6, you must agree to the additional Android authorization agreement. • The devices running Android 10 (SDK29) or higher do not support other policies except for the Trust Agent policy. • If the firmware is upgraded to Android 10 (SDK29) or higher, the policy already applied to the device is maintained, and can be canceled by changing the policy to not set.	
> Maximum screen timeout	Set the maximum screen timeout for when a user is not using or working with the applications on the device. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher, Android 2.2 or higher

Policy	Description	Supported devices
> Delay Time for Device Lock	Set the amount of time it takes for the device to be locked after the screen is turned off. The sum of the Screen timeout and Auto lock when screen turns off set on the device is the maximum delay time that can be set on the device. (Auto lock when screen turns off: The time required for a password when the screen is turned on again after being turned off) The maximum delay time varies depending on the device model, and the Delay Time for Device Lock may differ depending on the set value of Screen timeout. **NOTE** • The following situations can occur even if this policy is applied to the device. - The user can change the set value of Auto lock when screen turns off in the Settings menu of the device. - The set values of the Auto lock when screen turns off and the Delay Time for Device Lock set on the device may be different from the one applied to the profile. - If the device is unlocked by Smart Lock, the set Delay Time for Device Lock does not apply to the device.	Android 2.3 or higher
EMM Guardian	Allows devices that have been factory reset but not unenrolled by the administrator to reconnect to the EMM Server. When this policy is activated, the following functions are not available: the camera, SD card, MTP, Bluetooth, Wi-Fi tethering, USB debugging, and screen capture.	Samsung Knox 2.0 or higher
Connection attempt between server and device	Allows EMM to retry connecting according to the value that you specified when the device is disconnected from EMM. If not specified, communication will be reattempted twice every 15 minutes.	

Policy	Description	Supported devices
> Communication retry count	Set a retry count when a device is disconnected from EMM and EMM retries connecting to the device in 1 minute intervals. If the device is disconnected continuously despite retrying on the specified count, EMM will retry connecting according to the **Communication retry interval (min)** below. The value can be between 1 - 60 times.	Android 1.0 (SDK 1) or higher
> Communication retry interval (min)	Set a retry interval for when a device is disconnected from EMM. If EMM receives the event that the device is available, the server will try to connect immediately despite the waiting time. The value can be between 1 to 60 minutes.	Android 1.0 (SDK 1) or higher
CRL confirmation	Allows the CRL (Certificate Revocation List) to check the certificate conditions. You have to set the policy for the CC Mode. **NOTE** When applying the CC mode settings on a device which supports CC mode, the CC mode is activated if the following terms are fulfilled. • Encryption of the device memory and external SD card • When the following policy is set on an allocated device management profile. - In **Security** > **Maximum Failed Login Attempts**, when the set number of attempts is reached, it is reset to factory defaults. - In **Security** > **Manage password history**, set it to Default (No value) or 0 (zero). - **Allow** is selected in **Security** > **CRL Confirmation**. - In **System** > **Encryption for storage**, set **System storage** and **External SD card**.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Smartcard Browser Authentication	Allows Smartcard Browser Authentication within the internet browser. When the policy is allowed, the Bluetooth security mode is applied while the device is connected to the smart card reader and will not accept other Bluetooth connections. **NOTE** • To use this policy, Bluetooth smart card-related applications must be installed on the device and the smartcard must be registered in the Settings menu of the device. • Android 10 (Q) or higher devices are not supported.	Samsung Knox 1.0 or higher
Certificate deletion	Prevents users from deleting the certificate in the Settings menu of the device.	Samsung Knox 1.0 or higher
Certificate verification during installation	Set the system to validate the certificate during installation. If the certificate fails validation, it cannot be installed.	Samsung Knox 1.0 or higher
Attestation	Communicates with the attestation server to determine whether the user's device is forged. If no option is selected, attestation will not be processed.	Samsung Knox 1.0.1 or higher
> Action when verification fails	Set the measure for when forgery of the device firmware is detected. If detected, the creation of a new Knox Workspace and the use of the existing Knox Workspace are prohibited. • **Lock Knox Workspace**: Locks the Knox Workspace. • **Delete Knox Workspace**: Deletes the Knox Workspace. • **Lock device**: Locks the device. **NOTE** Android 10 (Q) or higher devices are not supported. • **Factory reset + Initialization SD Card**: Simultaneously factory resets the user's device and the SD card. • **Factory reset**: Resets the user device but not the SD card.	Samsung Knox 1.0.1 or higher
Google Android security update Policy	Allows the user to select whether to receive updates on the device. • **Forced use**: Set to receive security updates by default.	Samsung Knox 2.6 or higher

Kiosk (Android Legacy)

Policy	Description	Supported devices
Kiosk app settings	Select a Kiosk feature to use on a device. • **Single app**: Runs a single application on the device's home screen. • **Multi app**: Runs multiple applications that are developed using the Kiosk Wizard. • **Kiosk Browser**: Opens webpages that are specified by the administrator. **NOTE** • To set a Kiosk Browser to use, it has to be registered in **Setting** > **EMM Application and Policy** > **EMM Application**. • Kiosks are not available with non-Samsung Android Legacy devices.	Samsung Knox 1.0 or higher
> Set application	Click **Select** and select a single Kiosk application from the list. Alternatively, click **Add** and manually add applications. For more information about adding single applications, see Creating a Single App Kiosk.	Samsung Knox 1.0 or higher
>Set application	Click **Select** and select multiple Kiosk applications from the list. Alternatively, click **New** and create a Multi App Kiosk the Kiosk Wizard. For more information To learn how to use the Kiosk Wizard, see Exploring Kiosk Wizard.	Samsung Knox 1.0 or higher
> Set Kiosk Browser	When setting up the Kiosk Browser, the package name of the application registered as the Kiosk Browser will be automatically selected.	
> Default URL	Set the default page URL to call in the Kiosk Browser. You can enter a URL that is up to 128 bytes including alphanumeric characters and some special characters (_,., -, *, /).	
> Screen Saver	Use the screen saver for the Multi App Kiosk and the Kiosk Browser. When no user activity has been sensed for a certain amount of time, set it in the Auto Screen Off or Session Timeout settings on the device, the registered images or video files will be activated on the device display. **NOTE** • The Screen Saver only runs while the device is charging. • The Screen Saver for the Kiosk Browser only runs while the device is connected to a power source.	

Policy	Description	Supported devices
>> Screen Saver Type	Select either an image or video type screensaver.	
>>> Image	Select image files for the screen saver. You can add up to 10 image files in the PNG, JPG, JPEG, or GIF format (animated files are not supported). Each image file must be less than 5 MB. • To upload an image file, click **Add** and select a file. • To delete an image file, click next to the name of the uploaded image file. **NOTE** The device command must be transferred to the device to apply an image file to it.	
>>> Video	Select a video file for the screen saver. You can add only one video file in the MP4 or MKV format. The video file must be less than 50 MB. • To upload a video file, click **Add** and select a file. • To delete a video file, click next to the name of the uploaded video file. **NOTE** The device command must be transferred to the device to apply a video to it.	
> Session timeout	Allows the use of the session timeout feature for the Kiosk Browser. If the user does not use the device for a set time, the device deletes user information, such as the cache and cookies, in the device Kiosk Browser and goes to the main page URL: • **Apply**: Enable the session timeout feature for the browser.	
>> Time (sec)	Set the session timeout in seconds for the Kiosk Browser. The value must be between 10 - 3600 secs (default is 1800).	
> Text Copy	Allows the copying of text strings in the Kiosk Browser.	
> Javascript	Allows the running of the JavaScript contained in websites.	
> Http Proxy	Allows the use of an HTTP proxy for communications in the Kiosk Browser.	
>> IP/ Domain:Port	Set the HTTP proxy server IP or domain address, and Port. When not entered, the Port number is automatically set to 80.	

Policy	Description	Supported devices
> User agent settings key value	Set the key value to be added to the user agent. Allow the Kiosk Browser to access the Web server and the user agent key values contained in the HTTP header. User agent key settings can be used to detect access to non-Kiosk Browsers on the web server.	
> File Upload	Allows the attaching of files to a website through the Kiosk Browser. Kiosk Browser does not support pop-up windows, so cloud attachment is not possible.	DO: Samsung Knox 1.0 or higher Non-Samsung DO: Android 9.0 or higher
Delete Kiosk app when policy is removed	Allows deleting applications along with policies from the device when the applied policy is deleted.	Samsung Knox 1.0 or higher
Task manager	Allows the use of the Task Manager. **NOTE** You can use the function to disable the hardware key on SDK 2.5 or later.	Samsung Knox 1.0–2.4 or higher
System bar	Use the System bar which refers to the Status bar in the Notifications area at the top of the device and the Navigation bar in the Buttons area at the bottom. For non-Samsung devices, even if you selected either **Allow status bar only** or **Allow navigation bar only**, both the status bar and the navigation bar will be disabled.	Samsung Knox 1.0 or higher
Prohibit hardware key	Specify the hardware keys to disallow in Default and Kiosk mode.	Samsung Knox 1.0 or higher
> Disallow hardware key(s)	Select hardware keys to disallow. The type of hardware keys may vary depending on the device. If you set the task manager to Disallowed, the task manager is not launched even if you tap the left menu key on the navigation bar at the bottom the screen.	Samsung Knox 1.0 or higher
Multi windows	Allows the use of multiple windows. This is available for devices that provide the functionality of multiple windows.	Samsung Knox 1.0 or higher
Air command	Allows the use of Air command. Air command is a function provided on Samsung devices. Menu items appear when the user brings an S pen close to the screen.	Samsung Knox 2.2 or higher
Air view	Allows the use of Air view. Air view is a function provided on Samsung devices. Users can preview a picture or email when they bring the S pen or finger close to the picture or other content.	Samsung Knox 2.2 or higher
Edge screen	Allows the use of the Edge screen of the device. The Edge screen allows users to create shortcuts on the edges of the screen panel to frequently used applications, favorite contacts, or the camera.	Samsung Knox 2.5 or higher

Application (Android Legacy)

Policy	Description	Supported devices
Installation of application from untrusted sources	Allows the installation of applications from untrusted sources instead of just the Google Play Store. **NOTE** Android 8.0 or higher is supported for Knox Workspace devices.	Samsung Knox 1.0 or higher
Play Store	Allows using the Google Play Store.	Samsung Knox 1.0 or higher
YouTube	Allows using YouTube.	Samsung Knox 1.0 or higher
Application black/ whitelist settings	Set to control the application installation policies. • **Application blacklist settings**: Blacklist is the list of applications that should not be installed or run on the user devices. You can specify the **Application installation blacklist** and the **Application execution blacklist**. • **Application whitelist settings**: Whitelist is the list of applications that could be installed or run on the user devices. You can specify the **Application installation whitelist** and the **Application execution whitelist**. • **Application black/whitelist settings**: You can apply both blacklist and whitelist policy at the same time. If an application is registered both on the black and whitelist, the whitelist has priority.	

Policy	Description	Supported devices
> Application installation blacklist	Add applications to prohibit their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click next to the added application. **NOTE** • Applications that are installed before applying this policy and are not on the whitelist will be removed. • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Blacklisted applications cannot be installed and will be deleted even if they were previously installed. • An application that has been added on the **Application installation whitelist** cannot be added.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Application installation whitelist	Add applications to allow their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click next to the added application. **NOTE** • Applications that are installed before applying this policy and are not on the whitelist will be removed. • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Any applications not on the whitelist are deleted, even if they are not on the blacklist. • An application that has been added on the **Application installation blacklist** cannot be added. • Samsung Knox 2.0 or higher is supported for Knox Workspace devices.	Samsung Knox 1.0 or higher
> Application execution blacklist	Add applications to prevent their execution. Icon of the blacklisted application disappears and users cannot run the application. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** An application that has been added on the **Application installation whitelist** cannot be added.	Samsung Knox 1.0 or higher, Android 2.2 or higher

Policy	Description	Supported devices
> Application execution whitelist	Add applications to allow their execution. Icons of applications that are not on the whitelist disappear automatically. EMM and the preloaded applications are automatically registered on the whitelist. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** An application that has been added on the **Application installation blacklist** cannot be added.	Samsung Knox 1.0 or higher, Android 2.2 or higher
Application force stop prohibition list setting	Set to prohibit applications from force stop.	
> Force stop blacklist	Add applications to prohibit from force stop.	Samsung Knox 1.0 or higher
Application execution prevention list setting	Set to prevent applications from executing.	
> Application execution prevention list	Add applications to be displayed but not executable. Listed applications can be installed and the icons will be displayed, but they will not be executed. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 2.0 or higher
Application uninstallation prevention list setting	Set to prevent applications from uninstalling.	
> Application uninstallation prevention list	Add applications to prevent their uninstallation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Action when apps are compromised	Select from among the actions below to take if an internal or a kiosk application is compromised: • **Disallow running**: Prohibits the application's execution. • **Uninstall**: Deletes an application. • **Lock device**: Locks the user's device. **NOTE** Android 10 (Q) or higher devices are not supported. • **Notify Alert**: The compromised status of the device is reported on the **Dashboard**. • **Factory reset + Initialize SD card**: Simultaneously resets a user device and the SD card. • **Factory reset**: Resets the user device but not the SD card. **NOTE** • Actions such as lock device, factory reset, and the notify alert will be applied but only for general Android devices and not for Samsung Galaxy and LG Electronic devices. • This option is not applicable for devices with Android 2.0 or lower. To reset the device, select **Factory reset + Initialize SD card**.	Samsung Knox 1.0 or higher
Show ProgressBar when installing apps	Specify whether to display the ProgressBar when users are installing an app.	Samsung Knox 1.0 or higher, Android 1.0 or higher
Battery optimization exceptions	Set to exempt applications from the battery optimization function. This policy may cause battery loss. **NOTE** This policy is for devices running Android (Nougat) or later.	
> Apps excluded battery optimization	Add applications to exempt them from the battery optimization function.	Samsung Knox 2.7 or higher

Location (Android Legacy)

Policy	Description	Supported devices
Report device location	Allows collecting location data. • **User consent**: Allows location data collection only with the user's consent. • **Allow**: Allow collection of location information. **NOTE** • When this policy is set to **User consent**, location data can only be collected after the user allows collection of device location data in the permission pop-up. The Report device location policy has a higher priority than the GPS policy or Collect current location device command. • When this policy is set to **User consent** or **Allow**, EMM v2.5.5 or later devices must agree to the location permission. • The report device location interval will be deprecated after EMM v2.5.0. From EMM v2.5.0 or later, you can set the policy in Setting > Location Report Interval.	Android 5.0 or higher
> Report device location interval	Set an interval period to save the location data of the device. **NOTE** To set the collection interval, select either Allow or User Consent for the Report device location policy.	
High Accuracy Mode	Set to use for collecting accurate GPS locations of the devices.	Android 2.3 or higher

Browser (Android Legacy)

Browsers must be closed and opened again to apply the changes.

Policy	Description	Supported devices
Android browser	Allows using the Android browser. **NOTE** The disallowed setting or blacklist setting takes priority over others. If the disallowed setting is configured in any of the Android browser or the application blacklist policies, the Samsung Internet browser cannot be launched.	Samsung Knox 1.0 or higher
> Cookies	Allows cookies in the Android browser. **NOTE** If cookies are not allowed, you cannot access websites that authenticate users with cookies.	Samsung Knox 1.0 or higher
> JavaScript	Allows JavaScript in the Android browser.	Samsung Knox 1.0 or higher
> Autofill	Allows auto-completion of information that you enter on websites in the Android browser.	Samsung Knox 1.0 or higher
> Pop-up block	Allows blocking pop-ups in the Android browser.	Samsung Knox 1.0 or higher
Browser proxy URL	Set the proxy server address for the Android browser in the general area. Enter the value in the form of IP:port or domain:port in the fields. **NOTE** • The Chrome browser and Samsung S browser are supported. • The supported version for Chrome is Knox 4.0.1 - 5.6.	Samsung Knox 1.0.1 or higher

Phone (Android Legacy)

Policy	Description	Supported devices
Airplane mode	Allows the use of airplane mode.	Samsung Knox 2.0 or higher
Cellular data connection	Allows the use of a cellular data connection. **NOTE** This policy is applied after internal applications that have been set as **Automatic (Non-removable)** are installed. If the cellular data connection policy is not applied successfully, the device tries again to apply this policy 30 minutes later after EMM is activated.	Samsung Knox 1.0 or higher
Prohibit voice call	Prohibits incoming and outgoing voice calls.	Samsung Knox 1.0 or higher
> Voice call	Specifies the types of voice call to block: • **Incoming**: Blocks incoming voice calls only. • **Outgoing**: Blocks outgoing voice calls only If both are selected, only emergency calls can be received or made.	
Data usage limit	Allows the limiting of data usage.	Samsung Knox 1.0 or higher
Data usage restrictions	Limits the maximum data usage for user devices. If data usage exceeds the limit set on a device, data use is no longer available. To get precise information on the amount of usage, changing the date and time must not be allowed.	Samsung Knox 1.0 or higher
> Maximum usage	Set the maximum data amount for user devices for 1 day, 1 week, or 1 month. **NOTE** • Daily usage is calculated at 12:00 p.m. each day, weekly usage on Sundays, and monthly usage on the first day of each month. • When the maximum data amount is reached, the data network will be blocked. But if the user allows the data network, the data usage of the user device will be reset.	
Data connection during roaming	Allows data connection when roaming.	Samsung Knox 1.0 or higher
WAP push during roaming	Allows WAP push communication while using roaming.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Data sync during roaming	Allows data synchronization while roaming.	Samsung Knox 1.0 or higher
Voice calls during roaming	Allows voice calls while roaming.	Samsung Knox 1.0 or higher
Disallow SMS/MMS	Prohibits sending and receiving SMS/MMS messages.	Samsung Knox 1.0 or higher
> Disallow Incoming/ Outgoing SMS/ MMS	Specifies the types of SMS/MMS messages to block. **NOTE** At least one of the types should be selected.	
> Incoming SMS blacklist	Add phone numbers to the blacklist to block incoming SMS/MMS messages. • To add a phone number, enter it in the field and click  . • To delete a phone number, click  next to it.	
> Outgoing SMS blacklist	Add phone numbers to the blacklist to block outgoing SMS/MMS messages. • To add a phone number, enter it in the field and click  . • To delete a phone number, click  next to it.	
Use SIM card locking	Prevents the use of the SIM card on a user device. To use this policy, the default PIN of the SIM card should be entered. Then, the new PIN number for the SIM card should be entered. If the locked SIM card is registered to another device, the device is locked and the user must enter a valid PIN to unlock it. **NOTE** eSIM does not support the **Use SIM card locking** policy.	Samsung Knox 1.0 or higher
> Default SIM PIN	Enter the default PIN found on the SIM card. The value is a 4 - 8 digit number. **NOTE** This policy is designed for use by Corporate-Owned, Personally Enabled (COPE) devices and is only applied if the PIN found on SIM card matches the default PIN.	
> New SIM PIN	Enter the new PIN number for the SIM card. The new PIN number can be found next to **SIM PIN Number** in the “Network“ tab of the “Device Detail” page. The value is 4 - 8 digit numbers.	

Policy	Description	Supported devices
Set app voice recording whitelist	Allows recording phone conversations. **NOTE** If unspecified, voice recording is not allowed.	Samsung Knox 3.0 or higher
> App voice recording whitelist	Add applications that are allowed to record phone conversations to the whitelist. **NOTE** • The registered voice recording applications cannot be deleted after being activated. To remove the registered applications, you must factory reset the device. • If the registered voice recording applications are activated on a device, the device USB connection is blocked.	Samsung Knox 3.0 or higher

Firewall (Android Legacy)

Firewall configuration sets rules to block access to the network. You can add more firewall policy sets by clicking +.

Policy	Description	Supported devices
Firewall	Set to use the firewall to set target IP addresses. If the policy is not applied, the firewall is enabled by default. Enable policy is used to set IPs and ports to be excluded from the Disable policy. **NOTE** • If the firewall policy is set incorrectly, communication between the EMM server and the EMM Agent is failed, and device control is not possible. • Samsung Knox 1.0 - 2.4.1 is supported for Knox Workspace devices.	

Policy	Description	Supported devices
> Permitted Policy (IP)	Enter the target IP Address (range) and Port (range) to permit and select the network interface that can access the network. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the IP Address (range) and Port (range). 3. Select the Network Interface. 4. Select the Network Type: • **All** • **Data**: Only mobile network access is enabled. • **Wi-Fi**: Only Wi-Fi network access is enabled. 5. Select Port Range: • **All** • **Local**: Port access from the device is enabled. • **Remote**: Port access from the target server is enabled. 6. Click + to add. **NOTE** • To permit the target IPs, ports, and networks, you must set the IP Address (range) and Port (range) to * in Prohibited policy (IP). • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings. • Samsung Knox 2.5 is supported for Knox Workspace devices.	Samsung Knox 2.5 or higher

Policy	Description	Supported devices
> Prohibited Policy (IP)	Enter the target IP Address (range) and Port (range) to prohibit and select the network interface to prohibit network access. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Enter the IP Address (range) and Port (range). • Enter a wildcard character (*) as an IP Address to prohibit the use of the bandwidth. 3. Select the Network Interface. 4. Select Network Type: • **All** • **Data**: Mobile network access is disabled. • **Wi-Fi**: Wi-Fi network access is disabled. 5. Select Port Range: • **All** • **Local**: Port access from the device is disabled. • **Remote**: Port access from the target server is disabled. 6. Click + to add. **NOTE** • When entering the IP address, you can use a wildcard character (*) to disabled the bandwidth usage. • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings. • Samsung Knox 2.5 is supported for Knox Workspace devices.	Samsung Knox 2.5 or higher

Policy	Description	Supported devices
> Permitted Policy (Domain)	Input values to permit the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** • To allow specific domains only, you must set all domains in the **Prohibited policy (Domain)** using the wildcard then allow specific domains. • Use a wildcard character (*) to allow the use of a specific domain. The wildcard must be placed before or after the address and not in the middle. e.g.) *android.com / www.samsung* • Samsung Knox 2.6 is supported for Knox Workspace devices.	Samsung Knox 2.6 or higher
> Prohibited policy (Domain)	Input values to disable the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** • Use a wildcard character (*) to disable a specific domain. • Samsung Knox 2.6 is supported for Knox Workspace devices.	Samsung Knox 2.6 or higher
> DNS setting	Input values to specify the domain server address of all applications or registered applications. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input DNS values. • **DNS1**: Primary DNS. • **DNS2**: Secondary DNS. **NOTE** Only one DNS per application can be set and it is effective only when there are no VPN or Proxy policies assigned to the application.	Samsung Knox 2.7 or higher

NOTE

- If there are multiple firewalls, restricted firewalls have a higher priority.
- If a firewall is configured to all applications as well as in specific applications, the policy for each application has a higher priority.
- For example, specify firewall Enable/Disable policies as follows to allow only specific domains in Chrome:
  - Enable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *.samsungknox.com
  - Disable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *
- Firewall settings supports IPv6 for SDK 2.6 or later. Even if IPv4 and IPv6 addresses refer to a physically identical address, each must be configured separately.

Logging (Android Legacy)

Policy	Description	Supported devices
Save logs	Set to enable the save logs feature. • **Enable**: Set to perform logging. This is the default value. • **Disable**: Cannot record device logs. **NOTE** If this policy is not specified, the EMM performs logging with the **DEBUG** level.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Log level	Select a log level. • **DEBUG**: Logs detailed device information for the developers. • **INFO**: Logs device information for the administrators. • **WARNING**: Logs information that are not errors, but the ones that require special attention for the administrators. • **ERROR**: Logs error information. • **FATAL**: Logs critical error information, such as system interruption.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Maximum log size (MB)	Enter value for the maximum log size. The value can be between 1 - 20 MB.	Samsung Knox 1.0 or higher, Android 1.0 or higher
> Maximum days for storage (day)	Enter value for the maximum days for log storage. The value can be between 1 – 30 day.	Samsung Knox 1.0 or higher, Android 1.0 or higher

DeX (Android Legacy)

Samsung DeX is an accessory that extends the functionalities of a mobile device. By connecting a monitor, keyboard, and mouse to a Dex docking station, the mobile device can function as a desktop computer

In EMM, you can allow the use of DeX mode and control applications according to the Application execution blacklist setting.

Policy	Description	Supported devices
Allow DeX mode	Allows the use of DeX mode. • **Disallow**: The DeX station will not function even if a mobile device is mounted on it.	Samsung Knox 3.0 or higher
Allow Ethernet only	Allows ethernet only for DeX. Mobile data, Wi-Fi, and tethering are blocked.	Samsung Knox 3.0 or higher
Application execution blacklist(Android)	Use the blacklist for running DeX applications.	Samsung Knox 3.0 or higher
> Application execution blacklist	Prohibits launching the specified applications. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** • Any applications that already have been added to the Application whitelist cannot be added to the Application blacklist. • When this policy is enabled and applied, the icons of the blocked applications will disappear so that users cannot launch them. However, the applications are not deleted. The icons will reappear once the policy is changed or EMM is disabled.	

Wi-Fi (Android Legacy)

You can add more Wi-Fi policy sets by clicking ＋.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for each Wi-Fi setting.
Description	Enter a description for each Wi-Fi setting.
Network Name (SSID)	Enter an identifier of a wireless router to connect to. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Remove available	Allows users to delete the Wi-Fi settings.
Security type	Specifies the access protocol used and whether certificates are required.
> WEP	Set a WEP KEY index from WEP KEY 1 to 4.
> WPA/WPA2-PSK	Enter a password.

Policy	Description
> 802.1xEAP	Configure the following items: • **EAP Method**: Select an authentication protocol from among PEAP, TLS, and TTLS. • **2-step authentication**: Select one from PAP, MSCHAP, MSCHAPV2, or GTC as a secondary authentication method. This is available when EAP Method is set to TTLS or TLS. • **User information input method**: Select an input method for entering user information. - **Manual Input**: Enter the user ID and Password for the Wi-Fi connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. - **Connector interworking**: Choose a connector from the User Information Connector. - **User Information**: Use the user information registered in EMM to access Wi-Fi. • **User certificate input method**: Select a user certificate confirmation method. - **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. - **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. **User certificate Connector**: Select a connector to use from the User certificate Connector list.

Policy	Description
> 802.1xEAP	- **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service. • **CA certificate**: Select a root certificate. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **Wi-Fi** and the Type set as **Root** will appear on the list.
Proxy configuration	Select a proxy server configuration method. You can use the server to route through the proxy server when the device is connected to Wi-Fi.
> Manual	Configure the proxy server manually. • **Proxy host name**: Enter the host name of the IP address of the proxy server • **Proxy port**: Enter the port number used by the proxy server • **Proxy exception**: Enter the IP address or domain address that cannot be accessed through the proxy server. If server authentication is required to use the proxy server, check the **Server authentication** check box. • **User name**: Enter the username for the proxy server. • **Password**: Enter the password for the proxy server.
> Proxy automatic configuration	Configure the proxy server automatically. You should enter a PAC web address in the **PAC web address** field, the URL of the PAC file that automatically determines which proxy server to use.

Exchange (Android Legacy)

You can add more Exchange policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each exchange setting.
Description	Enter a description for each exchange setting.
Remove available	Allows users to delete the exchange settings.
Office 365	Allows to configure the Exchange settings by automatically filling out the Exchange server address and the SSL option as 'Use'.
User information input method	Select an input method for entering user information.
> Manual Input	Select to manually enter the email address, account ID, and password of a user. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
> Connector interworking	Select to choose a connector from the User Information Connector list. **NOTE** All the connectors are listed in **System** > **Connector** > **Directory**.
> User Information	Select to access the exchange server using the registered EMM email and ID. The password must be entered from the user's device.
Domain	Enter a domain address for the exchange server. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Exchange server address	Enter the exchange server information such as IP address, host name or URL. **NOTE** If **Office365** is selected, outlook.office365.com will be automatically entered.
Sync measure for the early data	Select the interval period to sync the past emails. The sync interval and synchronization are in accordance with the email application settings.
User certificate input method	Select an input method for entering certificate information.
> EMM Management Certificate	Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **User Certificate**: Select a certificate to use from the User Certificate list.

Policy	Description
> Connector interworking	Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. • **User certificate Connector**: Select a connector to use from the User certificate Connector list.
> Issuing external CA	Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. • **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Sync calendar	Syncs schedules on a calendar from an Exchange server or a mail server to a device.
Sync contacts	Syncs contact information in a phone book from a server to a device.
Sync task	Syncs tasks items from a server to a device.
Sync notes	Syncs notes from a server to a device.
SSL	Set to use SSL for email encryption. **NOTE** If **Office365** is selected, the SSL option is automatically set to 'Use'.
Signature	Enter the email signature to use.
Notification	Notifies the user of new emails.
Always vibrate on notification	Notifies the user of new emails with a vibration.

Policy	Description
Silent notification	Mutes email notifications. **NOTE** **Always vibrate on notification** and **Silent notification** cannot be used at the same time.
Attachment capacity (byte)	Enter the email attachment file size limit in bytes. The value can be between 1-52428800(50MB).
Maximum Size of Email Body (Kbyte)	Select a maximum value for the email body size. This is only set once during the initial Exchange ActiveSync setup.
> Default Size of Email Body (Kbyte)	Select the default value for the email body size. This is only set once during the initial Exchange ActiveSync setup.

Email Account (Android Legacy)

You can add more email account policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each email account setting.
Description	Enter a description for each email account setting.
Remove available	Allows users to delete the email account settings.
Default Account	Specifies to use the default account.
User information Input Method	Select an input method for entering user information.
> Manual Input	Select to manually enter the email address, server ID and password of a user. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
> Connector interworking	Select a connector from the user information connector list. **NOTE** The connectors are listed in **System** > **Connector** > **Directory**.
> User information	Select to access the relevant mail server using the registered EMM email, ID and password. **NOTE** The password must be entered from the user's device.
Incoming Server Protocol	Select between the POP3 (pop3) and IMAP (imap) protocol.
Outgoing Server Protocol	Entered automatically as SMTP.
Incoming Server Address/ port	Enter the Incoming Server address/port in a provided format.

Policy	Description
Incoming Server ID	Enter an incoming server ID to log in to the incoming mail server manually. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. **NOTE** This protocol is only available when **Manual Input** is selected.
Incoming Server Password	Enter an incoming server password to manually log in to the incoming mail server. **NOTE** This protocol is only available when **Manual Input** is selected.
Incoming SSL	Select to use SSL for encryption.
Outgoing Server Address/ port	Enter the outgoing server address/port and port in a provided format.
Outgoing Server ID	Enter an outgoing server ID to manually log in to the outgoing mail server. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. **NOTE** This protocol is only available when **Manual Input** is selected.
Outgoing Server Password	Enter an outgoing server password to manually log in to the outgoing mail server **NOTE** This protocol is only available when **Manual Input** is selected.
Incoming SSL	Select to use SSL for encryption.
Outgoing SSL	Select to use SSL for encryption.
Notification	Select an email notification method. • **Enable Notification**: Activates email notification. • **Enable 'Always notify by vibrate mode'**: Notifies the user of new emails with a vibration. • **Disable Notification**: Deactivates email notification.
All incoming certificates	Allows receiving certificates.
All outgoing certificates	Allows sending certificates.
Signature	Enter an email signature to use.
Account Name	Assign an account name.
Sender Name	Assign a sender name.

Bookmark (Android Legacy)

You can add, modify, or delete the bookmarks in the Samsung S browser, the default browser on Samsung Galaxy devices. You can add more bookmark policy sets by clicking +.

NOTE

- Browsers must be closed and opened again to apply the changes.
- Even if a user modifies a registered bookmark or registers a bookmark with the same URL and name, it will not be deleted when the bookmark setting is deleted.
- Even if a user manually deletes the set bookmark, due to the limitations of Samsung devices, the application may still appear to be installed. In this case, you have to delete the bookmark in the profile, and then recreate the bookmark.
- The auto-installation of Bookmark settings is supported on devices running Android 6.0 Marshmallow or Android 7.0 Nougat, and only when **BookMark** is chosen in the Installation area.

Policy	Description
Configuration ID	Assign a unique ID for each bookmark setting.
Description	Enter a description for each bookmark setting.
Installation area	Specifies a location to install the bookmark. • **BookMark**: Saves a bookmark in the S browser. • **ShortCut**: Creates a shortcut for the bookmarked address on the home screen of the device. Shortcut icons are created based on the Samsung Launcher. - If a **Shortcut** has been selected, auto installation is not supported. - Shortcut icons may not be able to be created depending on the type of launcher set by the user. An administrator cannot delete the shortcut icon, but the user can delete it manually.
Bookmark page URL	Enter a website address to go to when a bookmark is selected.
Bookmark name	Enter the bookmark name to be displayed as a title in the bookmark.

APN (Android Legacy)

You can add more APN policy sets by clicking +.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Enter an APN name to be displayed on the device.
Description	Enter a description for an APN.
Remove available	Allows users to delete APN settings in the EMM Client only. If you choose **Disallow**, then the button used to delete APN settings is disabled.
Access Point Name (APN)	Enter the name of the access point.
APN Type	Select the type of the access point. • **Default**: default type. • **MMS**: Multimedia Messaging Service. • **Supl**: IP-based protocol to receive GPS satellite signals.
Mobile Country Code (MCC)	Enter the country code for the APN.
Mobile Network Code (MNC)	Enter the carrier network code for the APN.
MMS Server (MMSC)	Enter the server information for sending multimedia messages. • **MMS Proxy Server**: Enter the information of the proxy server for sending multimedia messages. • **MMS Proxy Server Port**: Enter the port number of the proxy server for sending multimedia messages.
Server	Enter the WAP gateway server name.
Proxy Server	Enter the information of the proxy server.
Proxy Server Port	Enter the port number of the proxy server.
Access Point User Name	Enter the user name of the access point. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Access Point Password	Enter the password of the access point. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Authentication Method	Select an authentication method. • **None**: Disables authentication. • **PAP**: Requires a user name and password for authentication. • **CHAP**: Uses encryption with a Challenge string for authentication. • **PAP or CHAP**: Uses the PAP or CHAP authentication method.
Set as Preferred APN	Applies APN settings to the device.

Knox VPN (Android Legacy)

Knox VPN settings are provided to help you set up a VPN on a Samsung Galaxy device more easily. You can add more Knox VPN policy sets by clicking +.

NOTE Android 13 and later, this policy is no longer support.

Refer to the following for configuring Knox VPN policy sets.

- You can set up a VPN to use for an application or the device.
- You can set up a Knox VPN to use in the Knox Workspace area under Android Legacy > Knox VPN.
- VPN chaining creates a pair of inner and outer VPNs. When the outer VPN runs, the inner VPN also runs automatically. In this case, the data secured by the first VPN is double-secured by the second VPN, but the connection speed may slow down. When you run the outer VPN, the inner VPN also runs automatically. When you stop the outer VPN, the inner VPN also stops automatically. Two different VPN vendors are used for Knox VPN, and the two vendor's VPN Client applications are installed in the same area.
- VPN switching registers the information of several VPN servers as Knox VPN policy sets, so that when the first VPN is disconnected, another VPN connects. EMM only supports the switching of chained VPNs. Chained VPNs can be switched by users' stopping or starting VPN manually on their devices.

When switching VPNs, communications outside of the VPN are disconnected. Thus, the following restrictions occur if a firewall is configured.

- When switching VPNs, communications outside of the VPN are disconnected. Thus, the following restrictions occur if a firewall is configured.
- If Knox VPN does not restart after stopping, communications will be disconnected.
- If communication is disconnected due to the Knox VPN stopping, the firewall policy in the profile will not be applied. When Knox VPN restarts, the firewall policy will be applied.
- If the Knox VPN settings have never been started or if they restart after stopping, communications will not be disconnected.
- Deleting the Knox VPN set in the stopped Knox VPN profile removes the disconnections of communications.
- Using Knox VPN that is not chained does not disconnect communication through the firewall.
- Using EMM Agent and Knox VPN does not disconnect communication.

NOTE You can set the name of the application or package that will use the VPN into the Knox Workspace area and the General area.

Policy	Description
Configuration ID	Assign a unique ID for the Knox VPN setting.
VPN name	Enter a VPN name to display on the user device.
Description	Enter a description for the Knox VPN setting.
Remove available	Allows users to delete the Knox VPN settings.
VPN vendor name	Select a VPN vendor from among **Cisco**, **StrongSwan**, and **User defined**. Input fields vary depending on the selected VPN vendor name. **NOTE** Select **User defined** to set up a different vendor's VPN service, such as the Sectra mobile VPN. For more information, see Entering a VPN vendor manually.
VPN client vendor package name	Entered automatically according to the selected VPN vendor name. If **User defined** is selected, you must manually enter this protocol.
VPN type	Entered automatically when you select **StrongSwan**. If **Cisco** or **User defined** is selected, you must manually select this protocol.
Entering methods for Knox VPN	Select an entering method for Knox VPN information. • **Manual Input**: Only allowed for **StrongSwan** and **Cisco**. For more information, see Configuring a Knox VPN profile manually. • **Upload profile**: Allowed for all VPN vendors. **NOTE** Input fields vary depending on the selected VPN vendor and the entering method.
Upload Knox VPN profile	Allows uploading a Knox VPN profile when you set **Entering methods for Knox VPN** to **Upload profile**. You can upload a text file in the JSON format. JSON varies depending on the VPN vendor and VPN type. For more information about sample files, see the sample file of a Sectra Mobile VPN configuration in Entering a VPN vendor manually.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
CA Certificate	Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **Knox VPN** and the Type set as **Root** will appear on the list.
Server certificate	Select a certificate to use from the certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose has been set as **Knox VPN** and the Type set as **User** will appear on the list.
FIPS mode	Allows the use of FIPS mode. FIPS (US Federal Information Processing Standards) encrypts all data with FIPS-140-2 authentication modules between the server and client.

Policy	Description
Auto Re-connection	Allows connecting automatically when an error occurs.
VPN route type by application (General Area)	Select the following options from the list to use the VPN for the selected application or all applications in the General area: • **Per Application**: VPN is applied to the selected application. Click the **Select** button to select an application or enter the paged name directory. • **All packages**: VPN is applied to all applications in the General area or Knox Workspace area.
VPN route type by application (Knox Workspace Area)	Select the following options from the list to use the VPN for the selected application or all applications in the Knox Workspace area: • **Per Application**: VPN is applied to the selected application. Click the **Select** button to select an application or enter the paged name directory. • **All packages**: VPN is applied to all applications in the Knox Workspace area. **NOTE** • You must select **User defined** for **VPN vendor name** to set VPN Route Type of the General Area and Knox Workspace Area together. • When Knox Workspace is created on a device activated with COPE type, VPN route type by application (Knox Area) should not be set. The admin should select the option'-' to prevent errors from occurring.
Setting VPN	Configure the outer VPN and the inner VPN to use for VPN chaining. Do not configure it if you want to use a solitary Knox VPN setting. For example, configure Knox VPN as the outer VPN in Setting 1, and then configure the inner VPN in Setting 2. Click Select in the Setting 2's VPN chaining setting and designate Setting 1 as the outer VPN. Then, the VPN chaining will be set. In this case, the Setting 1's VPN chaining setting will be automatically filled as Setting 2 selected. If another VPN is selected in Setting 2, VPN chaining will be automatically cut. • Click **Select**, and in the "Select VPN Configuration" window, click the VPN's **Configuration ID** to connect. If the VPN is the inner VPN, only the outer VPN will be displayed, and the VPNs already paired will not be displayed on the list.

Entering a VPN vendor manually

To use a VPN provided by a vendor other than StrongSwan or Cisco, select **User defined** in the **VPN vendor name** field. Then upload a text profile in the JSON format. The VPN Client must be installed on the device before using a VPN.

For example when a Sectra VPN is used, set the options as below:

1. Enter `com.sectra.mobilevpn` in the **VPN client vendor package name** field.
2. Set **VPN type** to **SSL**.
3. Click **Add** next to **Upload Knox VPN profile** and upload a configuration file with the Sectra Mobile VPN configuration parameters set.
   - Upload a file in the JSON format to fully integrate the Sectra Mobile VPN in the EMM Admin Portal.
   - Set the parameters as shown in the example below.

Parameter	Description	Example
profileName	The name of the VPN configuration profile that will be listed on the EMM application and the VPN client GUI.	Sectra Mobile VPN

servers	A list of 1 – 6 VPN servers with IP addresses and a network port. This list will be in an order of priority, with the default VPN server being the first on the list. The remaining VPN servers will be used only if the default server is damaged.	`[`
		`{"address":"1.1.1.1", "port":443}`
		`{"address":"2.2.2.2", "port":444}`
		`{"address":"3.3.3.3", "port":445}`
		`]`

pkcx12BaseUrl	A download server's HTTP/S URL, where the encrypted key materials are downloaded to.	http://download.server.com/certs/
mtuSize	The MTU (Magnetic Tape Unit) is a size used on EMM's virtual network interface. It is the maximum size for the outgoing UDP (User Datagram Protocol) tunnel packets before being fragmented The value must be between 576 – 1500 bytes.	1300

Parameter	Description	Example
UseDtle	Determines whether a DTLS tunnel is used. A DTLS tunnel should be used if sensitive data is being transmitted in real-time. E.g.) When streaming video and/or using VoIP calls. The value must be either True or False. If unsure, set to True.	True
diffServe	Tunnel packets' QoS (Quality of Serve) tag sent from a client. Differentiated service is part of an IP header. The value must be between 0 – 63. 0 means disabled.	0
tcpKeepAlive	Timer value for the interval of a KeepAlive packet sent from a TCP tunnel. The value must be between 1 – 18000. • Sectra recommends to set this value as 1200 seconds since is compatible with most mobile networks. **NOTE** This is an important parameter that needs to be selected with caution.	1200
dtlsInactivityTimeout	The timer value for the standby period of a DTLS tunnel that determines how long it idles without receiving any data before it goes inactive. The value must be between 1 – 300 seconds. **NOTE** Sectra does not recommend setting this value to 300 seconds.	30

trarricProfiles	1 – 3 traffic profiles the users can choose, for when a normal configuration is not sufficient. Traffic profiles can change the following configuration parameters: mtuSize, useDtls, diffServ, tcpKeepAlive and/or dtlsInactivityTimeout. The traffic profile also requires the name of the profile which is shown in the client GUI.	`[ {"profileName": "BadNetworkProfile","mtuSize":800, "tcpKeepAlive":600},`
		`{"profileName":" RealTimeProfile" ,"mtuSize":1500, "useDtls":"true", "diffServ":63}`
		`]`

The following is a sample file of a Sectra Mobile VPN configuration:

```
{
     "KNOX_VPN_PARAMETERS":{
           "profile_attribute":{
                 "profileName":"Sectra Mobile VPN",
                 "vpn_type":"ssl",
                 "vpn_route_type":1
           },
           "knox":{
                 "connectionType":"keepon"
           },
            "vendor":{
                 "connection":{
                       "servers": [
                             {"address":"1.1.1.1", "port":443},
                             {"address":"2.2.2.2", "port":444},
                             {"address":"3.3.3.3", "port":555}
                       ],
                       "ssl": {
                             "basic": {
                                 "pkcs12BaseUrl":"http://download.server.com/
certs/",
                                 "mtuSize":1300,
                                 "useDtls":true,
                                 "diffServ":0,
                                 "tcpKeepalive":1200,
                                 "dtlsInactivityTimeout":30
                             }
                       }
                 },
                 "trafficProfiles": [
                       {
                             "profileName": "BadNetworkProfile",
                             "mtuSize":800,
                             "tcpKeepAlive":600
                       },
                       {
                             "profileName":"RealTimeProfile",
                             "mtuSize":1500,
                             "useDtls":"true",
                             "diffServ":63
                       }
                 ]
           }
      }
}
```

Configuring a Knox VPN profile manually

You can manually enter a profile only when the VPN vendor is StrongSwan or Cisco. Select **Manual Input** in the **Entering methods for Knox VPN** field. Then set the options as below:

1. Enter the IP address, host name, or URL of the VPN server in the **Server address**.
   - The VPN route type, which enables the use of VPN tunneling, is automatically entered.
2. Select to use **User authentication**.
3. Enter the user information for authentication depending on the selected **Entering methods for user information**:

Method	Description
Manual Input	Enter the user ID and Password for the VPN connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Connector interworking	Choose a connector from the **User certificate Connector**. All the connectors are listed in **System** > **Connector** > **Directory**.

4. Select a **Connection type** and enter the parameters. The required parameters vary depending on the selected connection type.

Item	Description
PPTP	Select whether to use **PPP Encryption (MPPE)**.
L2TP/IPSec PSK	Enter the **L2TP Secret Key**, **Identifier**, and **Pre-shared Key**.
L2TP/IPSec RSA	Enter the **L2TP Secret Key**.
IPSec Xauth PSK	Enter the **IPSec Identifier** and **Pre-shared Key**.
IPSec Xauth RSA	Enter the **User certificate input method**, **CA Certificate**, and **Server Certificate**.
IPSec Hybrid RSA	Enter the **CA Certificate** and **Server Certificate**
IPSec IKE2 PSK	Enter the **Identifier** and **Pre-shared Key**.
IPSec IKE2 RSA	Enter the **User certificate input method**, **OCSP URL**, **CA Certificate**, and **Server Certificate**.

5. Configure the advanced option.

Item	Description
DNS search domain	Enter the DNS name.
DNS server	Enter the DNS address according to the IP pattern.
Forwarding route	Entered automatically when **Subnet Bits** is selected
Subnet Bits	Select **None** or **/1** from **/30**.

6. Select a VPN **connection type**.
   - **Keep On**: Keep the VPN connection.
   - **On Demand**: Connect to the VPN upon request.
7. Select the **chaining** type.
8. Select to use the **UID PID**.

The following is a sample file with Cisco as the VPN vendor and IPSec as the VPN type:

```
{
     "KNOX_VPN_PARAMETERS":{
          "profile_attribute":{
               "profileName":"c1",
               "host":"12.3.456.78",
               "isUserAuthEnabled":true,
               "vpn_type":"ipsec",
               "vpn_route_type":1
          },
          "ipsec":{
               "basic":{
                    "username":"",
                    "password":"",
                    "authentication_type":1,
                    "psk":"",
                    "ikeVersion":1,
                    "dhGroup":0,
                    "p1Mode":2,
                    "identity_type":0,
                    "identity":"test@sta.com",
                    "splitTunnelType":0,
                    "forwardRoutes":[
                         {
                              "route":""
                         }
                    ]
               },
               "advanced":{
                    "mobikeEnabled":false,
                    "pfs":true,
                    "ike_lifetime":"10",
                    "ipsec_lifetime":"25",
                    "deadPeerDetect":true
               },
               "algorithms":{
               }
          },
          "knox":{
               "connectionType":"keepon",
               "chaining_enabled":"-1",
               "uidpid_search_enabled":"0"
          },
          "vendor":{
               "setCertCommonName":"space",
               "SetCertHash":"pluto",
               "certAuthMode":"Automatic"
          }
     }
}
```

The following is a sample file with Cisco, as the VPN vendor, and SSL, as the VPN type:

```
{
     "KNOX_VPN_PARAMETERS":{
          "profile_attribute":{
               "profileName":"c3",
               "host":"cisco-asa.gnawks.com",
               "isUserAuthEnabled":true,
               "vpn_type":"ssl",
               "vpn_route_type":1
          },
          "ssl":{
               "basic":{
                    "username":"demo",
                    "password":"samsung",
                    "authentication_type":1,
                    "splitTunnelType":0,
                    "forwardRoutes":[
                         {
                              "route":""
                         }
                    ]
               },
               "algorithms":{
                    "ssl_algorithm":0
               }
          },
          "knox":{
               "connectionType":"keepon",
               "chaining_enabled":"-1",
               "uidpid_search_enabled":"0"
          },
          "vendor":{
               "setCertCommonName":"space",
               "SetCertHash":"pluto",
               "certAuthMode":"Automatic"
          }
     }
}
```

VPN (Android Legacy)

You can configure the VPN settings to connect to a private network through a public network. You can add more VPN policy sets by clicking +.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for the VPN setting.
VPN Name	Enter a VPN name to display on the user device.
Description	Enter a description for the VPN setting.
Remove available	Allows users to delete the VPN settings.
Connection type	Select a connection type and enter the parameters. Required parameters vary depending on the selected connection type. • **PPTP**: Set if PPP should be encrypted (MPPE). • **L2TP/IPSec PSK**: Enter parameters in the **L2TP Secret Key, IPSec Identifier**, and **IPSec Pre-shared Key** fields. • **L2TP/IPSec RSA, IPSec Xauth RSA, IPSec Hybrid RSA**: Select a root certificate from IPSec CA Certificates. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **VPN** and the Type set as Root will appear on the list. • **IPSec Xauth PSK**: Enter parameters in the **IPSec Identifier** and **IPSec Pre-shared Key** fields.
Server address	Enter the IP address, host name, or URL of the VPN server that the device needs to access.
User information input method	Select an input method for entering user information. • **Manual Input**: Enter the user ID and Password for the VPN connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. • **Connector interworking**: Choose a connector from the **User information Connector**. All the connectors are listed in **System** > **Connector** > **Directory**. • **User Information**: Use the user information registered in EMM to access the VPN.
PPP Encryption (MPPE)	Allows to encrypt data for the VPN connection.
DNS search domain	Enter the DNS name.
DNS server	Enter the DNS server address.
Forwarding route	This is automatically entered when **Subnet Bits** is selected.
Subnet Bits	The value can be set as none or select from /1 to /30.

Certificate (Android Legacy)

You can install a user certificate on a device and use the certificate through Wi-Fi or on websites. You can add more certificate policy sets by clicking +.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration	Assign a unique ID for each certificate setting.
Description	Enter a description for each certificate setting.
Automatic Installation	Select whether to install each certificate automatically. The default value is **Use**. However, if you set only one certificate, it will be automatically installed. **NOTE** • Certificates are installed per the setting values of the automatic installation only when devices have EMM Agent v2.5.5 and the server is EMM v2.5.5 or higher. • For certificate settings created on lower versions than EMM v2.5.5, the automatic installation value will be displayed as **Do not use**.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Certification category	Select a certification category when **EMM Management Certificate** is selected in **User certificate input method**, • **CA certificate**: Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **CA Cert** and the Type set as **Root** will appear on the list. • **User certificate**: Select a certificate to use from the User Certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose has been set as **CA Cert** and the Type set as **User** will appear on the list.

Configuring Knox Workspace Policies

Create a profile and register policies for Knox Workspace devices.

You can configure the policies below for Knox Workspace devices. The availability of each policy varies depending on the OS version.

→ System (Knox Workspace)

Allows various features, such as screen capture, clipboard, and share via apps.

→ Interface (Knox Workspace)

Allows adding a new Wi-Fi network or using a microphone and other features.

→ Security (Knox Workspace)

Configures the security settings, such as passwords and lock screen.

→ Application (Knox Workspace)

Configures options for application controls such as installation, blacklist/whitelist, and execution prevention.

→ Browser (Knox Workspace)

Allows the use of the Android browser and configuring the settings for it.

→ Firewall (Knox Workspace)

Configures the IP or a domain firewall policy for each application.

→ Container Data (Knox Workspace)

Allows data transfers between the Knox Workspace area and the general area.

→ Dual DAR(Knox Workspace)

You can set policies for Dual DAR Workspace such as data lock or application access restriction.

→ Exchange ActiveSync (Knox Workspace)

Configures the Microsoft Exchange ActiveSync account to synchronize email, calendar, contacts, and tasks from the Exchange account.

→ Email Account (Knox Workspace)

Configures the POP/SMTP server in order to view the incoming and outgoing emails through the email account used on the device.

→ Bookmark (Knox Workspace)

Configures the bookmark settings such as the icons and URL that will be displayed on devices.

→ Knox VPN (Knox Workspace)

Configures the VPN (Virtual Private Network) on a Knox Workspace. Android 13 and later, this policy is no longer support.

→ Certificate (Knox Workspace)

Set the certificate and the user authentication method on devices for when device users authenticate. Android 13 and later, this policy is no longer support.

System (Knox Workspace)

Policy	Description	Supported devices
Screen capture	Allows using the screen capture function in the Knox Workspace.	Samsung Knox 1.0 or higher
Clipboard	Allows the clipboard feature. • **Allow within the same app**: The clipboard function can only be used within the same application.	Samsung Knox 1.0 or higher
Share via apps	Allows the share app function in the Knox Workspace.	Samsung Knox 1.0 or higher
Google account synchronization	Allows Google account synchronization in the Knox Workspace.	Samsung Knox 2.0 or higher
App crash report to Google	Report application error occurrence information to Google in the Knox Workspace.	Samsung Knox 1.0 or higher
System app close	Allows forceful system application shutdowns in the Knox Workspace.	Samsung Knox 1.0 or higher
Trusted Boot Verification	Allows Trusted Boot.	Samsung Knox 2.0 or higher
Third Party Keyboard	Allows the use of third Party Keyboards. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
Add Email Account	Allows adding accounts from the default email application on the device.	Samsung Knox 1.0 or higher
Domain whitelist setting	Set to use the email domain whitelist setting. **NOTE** • The Add email account policy has a higher priority than the Domain whitelist setting policy. • The Domain whitelist setting policy does not apply if the Add email account policy is set to Disallow.	
> Domain Whitelist	Enter the email domain whitelist to add. • To add a domain, enter the domain name in the field, and click **Add**. • To delete a domain, click 🗑 next to the added domain name.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Allow Remote Control	Allows remote control within the Knox Workspace via Remote Support. Remote Support should be installed in the general area. **NOTE** • Policy changes using Remote Support in the Knox Workspace do not apply to the Remote Support Viewer immediately. In this case, reload the Knox Workspace area. • This policy is not available for the high security version.	Samsung Knox 2.2 or higher

Interface (Knox Workspace)

Policy	Description	Supported devices
Add a new Wi-Fi network	Allows adding a new Wi-Fi network connection in the Knox Workspace.	Samsung Knox 1.0 - 2.4.1
Microphone	Allows the controls for Microphone use in the Knox Workspace. **NOTE** If this policy is disallowed, video recording is also disallowed.	Samsung Knox 1.0 or higher
> Recording	Allows using microphone recording in the Knox Workspace.	Samsung Knox 1.0 or higher
Camera	Allows using the camera in the Knox Workspace. • **Disallow all**: Allows taking pictures but disables video recording. This option is available only for Samsung devices. **NOTE** If the camera policy in the General area is disallowed, camera use in the Knox Workspace is also prohibited.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Allow USB access	Allows using USB devices, such as printers and scanners, via OTG in the Knox Workspace. • **Disallow** is the default value. **NOTE** • This policy is only allowed for non-storage USB devices in USB accessary mode. • Devices from Verizon, the United States telecommunications provider, are not supported. • Android 13 and later, this policy is no longer support.	Samsung Knox 2.5 or higher
> Allow access of USB devices	Set USB products to use in a specific application. 1. Enter the Package Name. 2. Select the Vendor ID. 3. Enter the Product ID. • Only 4-digit, hexadecimal characters can be entered. • Multiple inputs should be separated by commas. • Only the product ID for the selected vendor can be entered. 4. Click + to add, or click 🗑 to delete.	Samsung Knox 2.1 or higher
Bluetooth Low Energy	Allows use of the Bluetooth Low Energy feature in the Knox Workspace. To use this policy, set the Bluetooth connections in the general area to Allow.	Samsung Knox 2.4 or higher
Phone Book Access Profile (PBAP) via Bluetooth	Allows use of the Phone Book Access Profile (PBAP). Contacts on the Knox Workspace are sent to the connected device if this policy is allowed.	Samsung Knox 2.7 or higher
NFC control	Allows control of the NFC (Near Field Communication). **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.4 or higher

Security (Knox Workspace)

Policy	Description	Supported devices
Knox Container Password	Set the password for the Knox Workspace screen lock. **NOTE** • For devices with a One Lock password, the password policy that is stronger between Android Legacy and the Knox Workspace area will be applied. • When a user has forgotten their Knox Workspace password, the administrator needs to send the **Reset screen password** device command, and then the user needs to enter a temporary password. For more information, see the Knox password in Viewing the device details. • If the Prohibited words policy has been set, then the password cannot be reset with a temporary password containing the specified prohibited words. If this happens, you will need to disable the Prohibited words policy, save the relevant profile again, and then apply it. • Allow this policy to set the password for a Knox Workspace on devices running Android 8.0 (Oreo) or higher. If you allow this policy, the password setup screen will appear after the Knox Workspace is created.	
> Enterprise Identity Authentication	Controls Knox Workspace unlock with an enterprise ID. • **Use**: Allows the choice to use an enterprise ID to log in. • **Forced use**: Forces the use of an enterprise ID to log in.	Samsung Knox 2.4 or higher
>> Domain Address	Enter the domain address of the enterprise identity server. The http(s) prefix can be omitted.	Samsung Knox 2.4 or higher
>> Setup file	Select a file to install inside the Knox Workspace for enterprise ID authentication. **NOTE** You can select an application such as Samsung SSO Authenticator (com.sec.android.service.singlesignon), from the application list. Applications must be pre-enrolled either on **Application** > **Internal application** or **Application** > **Public application**.	Samsung Knox 2.4 or higher

Policy	Description	Supported devices
>> Enable FIDO	Use FIDO (Fast ID Online) authentication in a Knox Workspace when using an enterprise ID.	Samsung Knox 2.7 or higher
>>> Request URL	Set the URL to request for FIDO authentication.	Samsung Knox 2.7 or higher
>>> Response URL	Set the URL to respond to FIDO authentication	Samsung Knox 2.7 or higher
>>> FIDO App Installed List	Manage the applications to use for FIDO authentication. **NOTE** The essential applications required for FIDO authentication are automatically added to the list. You can add an additional application if needed.	Samsung Knox 2.7 or higher
> Minimum strength	Set the minimum password strength on the screen. • **Pattern**: Set the password using a pattern or any other password with a higher degree of complexity, such as **Numeric**, **Must be alphanumeric**, or the **Must include special characters** options. • **Numeric**: The password must consist of a 4 digit number or be more complex. The screen can be locked using the **Numeric**, **Must be alphanumeric**, and **Must include special characters** types of passwords. • **Must be alphanumeric**: Both letters and numbers must be included. The screen can be locked using with the **Must be alphanumeric** and **Must include special characters** types of passwords. • **Must include special characters**: Set so that the passwords must include alphanumeric and special characters.	Samsung Knox 2.0 or higher
>> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before access is restricted. The value can be between 0 - 10 times. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher

Policy	Description	Supported devices
>>> Action for failing allowed count to retry password	Select the action to be taken when the maximum number of failed attempts is reached. A Workspace control command must be sent to unlock the Knox Workspace. • **Lock Knox Workspace**: When the set number of password attempts has been reached, the Knox Workspace is locked. • **Wipe Knox Workspace**: When the set number of password attempts has been reached, the Knox Workspace is deleted. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 1.0 or higher
>> Expiration after (days)	Set the maximum number of days before the password must be reset. The value can be between 0 - 365 days. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 0 - 10 times. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Minimum length	Set the minimum length of the password. • If the **Minimum strength** is set to **Pattern**, at least more than one stroke is required. • In the case of **Must include special characters**, it must be equal to or greater than the sum of the **Minimum number of letters** and **Minimum number of non-letters**. The value can be between 4 - 16 characters for **Numeric** or **Must include special characters**. The value can be between 6 - 16 characters for **Must include special characters**. **NOTE** • If Minimum strength is set to Pattern, setting Minimum length does not apply. • Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher

Policy	Description	Supported devices
>> Minimum number of letters	Set the minimum number of password letters. • If the **Minimum strength** is set to **Must include special characters**, the number 1 must be entered. • In the case of **Must include special characters**, the default value is the number 3. If you want to enter another number, the number must be equal or greater than the sum of the **Minimum number of lowercase letters** and the **Minimum number of capital letters**: The value can be between 4 – 10 characters. The default value is 1 character for **Must be alphanumeric**. The default value is 3 characters for **Must include special characters**. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Minimum number of lowercase letters	Set the minimum number of lowercase letters required in the password. The value can be between 1 - 10 characters. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Minimum number of capital letters	Set the minimum number of uppercase letters required in the password. The value can be between 1 - 10 characters. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Minimum number of non-letters	Set the minimum number of numbers and special characters required in the password. If **Minimum strength** is set to **Must be alphanumeric**, the default value is the number 2. If you want to enter another number, the number must be equal or greater than the sum of **Minimum number of numeric characters** and **Minimum number of special characters**. The value can be between 1 - 10 characters. The default value is 2 characters for **Must include special characters**. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher

Policy	Description	Supported devices
>> Minimum number of numeric characters	Set the minimum number of numeric characters allowed in the password. The value can be between 1 - 10 characters. The default value is 2 characters for **Must include special characters**. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Minimum number of special characters	Set the minimum number of special characters required in the password. The value can be between 1 -10 characters. The default value is 1 character for **Must include special characters**. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
>> Maximum length of repeated characters	Set maximum number of duplicated characters. The value can be between 1 -10 characters.	Samsung Knox 1.0 or higher
>> Maximum length of sequential numbers	Set the maximum number of consecutive numeric characters allowed in a password. The value can be between 1 - 10 words.	Samsung Knox 1.0 or higher
>> Maximum length of sequential characters	Set the number of consecutive letters allowed in a password. The value can be between 1 - 10 words.	Samsung Knox 1.0 or higher
>> Minimum length of character change	Set the minimum length of letters that users must change from the previous password. If the **Minimum strength** is set to **Numeric**, **Must be alphanumeric**, or **Must include special characters**, it must be less than the Minimum length. The value can be between 1 - 10 words.	Samsung Knox 1.0 or higher
>> Prohibited words	Allows the use of prohibited words in a password.	
>>> Set prohibited words	Set prohibited words in a password. • To add a word, enter the word the field and click +. • To delete a word, click 🗑 next to the added word.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Maximum screen timeout	Set the maximum time limit that a user can linger before screen timeout. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
Password visibility settings	Shows the password when entering it.	Samsung Knox 1.0 or higher
Pattern lock visibility settings	Shows the password when entering it.	Samsung Knox 1.0 or higher
Smartcard Browser Authentication	Allows Smartcard Browser Authentication within the internet browser. When the policy is allowed, the Bluetooth security mode is applied while the device is connected to the smart card reader and will not accept other Bluetooth connections. **NOTE** • To use this policy, Bluetooth smart card-related applications must be installed on the device and the smartcard must be registered in the Settings menu of the device. • Android 10 (Q) or higher devices are not supported.	Samsung Knox 1.0 or higher
Unlock with fingerprint	Allows the use of the fingerprint unlock control. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.1 or higher
Unlock with iris	Allows the use of the iris unlock control. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.2 or higher

Policy	Description	Supported devices
Enforce Multi factor Authentication	Allows the use of two-step authentication. • **Use**: Forces the screen lock to release via fingerprint or iris recognition. • **Do not use**: Disables the two-step authentication settings via your fingerprint or iris recognition. **NOTE** When the Knox Workspace is created, it is set to select only two factor authentication on the password setup stage. Even when the manager chooses to disable 'Unlock with fingerprint' or 'Unlock with Iris, you can still use your fingerprint or iris for two-step verification.	Samsung Knox 2.2 or higher
Block function setting on lock screen	Blocks the function set in the lock screen.	
> Block functions on lock screen	Set the lock screen function options. • **Trust Agent**: Set whether to use the Knox Quick Access on the lock screen.	Samsung Knox 2.4 - 2.9

Application (Knox Workspace)

Policy	Description	Supported devices
Installation of application from untrusted sources	Allows the installation of applications from untrusted sources instead of just the Google Play Store.	Samsung Knox 1.0 or higher
Application black/ whitelist settings	Set to control the application installation policies on the Knox Workspace. • **Application blacklist settings**: Blacklist is the list of applications that should not be installed or run on the user devices. You can specify the **Application installation blacklist** and the **Application execution blacklist**. • **Application whitelist settings**: Whitelist is the list of applications that could be installed or run on the user devices. You can specify the **Application installation whitelist** and the **Application uninstallation prevention list**. • **Application black/whitelist settings**: You can apply both blacklist and whitelist policy at the same time. If an application is registered both on the black and whitelist, the whitelist has priority. If this policy is not set for any applications, then no applications other than EMM application such as EMM Client and Secure Browser can be executed and installed.	
> Application installation blacklist	Add applications to prohibit their installation on the Knox Workspace. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Previously installed blacklisted applications will also be removed. • An application that has been added on the **Application installation whitelist** policy cannot be added.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
> Application installation whitelist	Add applications to allow their installation on the Knox Workspace. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Any applications not on the whitelist are deleted, even if they are not on the blacklist. • An application that has been added to the **Application installation blacklist** policy cannot be added. • Applications that are installed before applying this policy and are not on the whitelist will be removed.	Samsung Knox 2.0 or higher
> Application execution blacklist	Add applications to prevent their execution in Knox Workspace. Icon of the blacklisted application disappears and users cannot run the application. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** An application that has been added to the **Application installation whitelist** policy cannot be added.	Samsung Knox 1.0 or higher
> Application execution prevention list	Add applications to be displayed but not executable on the Knox Workspace. Listed applications can be installed and the icons will be displayed, but they will not be executable. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	Samsung Knox 2.0 or higher

Policy	Description	Supported devices
> Application uninstallation prevention list	Add applications to prevent their uninstallation on Knox Workspace. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 1.0 or higher
App installation authority whitelisting settings	Set the applications with installation permissions on Knox Workspace.	
> Application installation whitelist	Add applications to allow installation on the Knox Workspace. Selected applications will be added to the View list with the package name of the applications. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 1.0 or higher
GMS application	Allows Google Mobile Service (GMS) application installation. If the GMS application policy is disallowed, the basic applications provided by Google do not appear.	Samsung Knox 1.0 or higher
TIMA CCM profile whitelist	Allows the use of the TIMA Client Certificate Manager (CCM) profile on Knox Workspace. • **Entire application**: Applications in the Knox Workspace can access TIMA CCM. • **Whitelist Application**: Only the added applications on the whitelist can access TIMA CCM.	
> TIMA CCM profile application whitelist	Add applications to access the TIMA CCM on the Knox Workspace. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 2.1 or higher
TIMA CCM profile app access restriction exception list settings	Allows only the set applications to access the TIMA CCM profile even when the Knox Workspace is locked.	

Policy	Description	Supported devices
> TIMA CCM profile app access restriction exception list	Add applications to access the TIMA CCM profile even when the Knox Workspace is locked. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** • If **Whitelist Application** is selected in the **TIMA CCM profile whitelist** policy, only the whitelisted applications can access TIMA CCM. • If **Entire application** is selected in the **TIMA CCM profile whitelist** policy, the access restrictions of the applied applications are excluded.	Samsung Knox 2.1 or higher
Settings for whitelisting apps allowing external SD card	Allows the use of an external SD card in Knox Workspace. The external SD card cannot be used by default in the Knox Workspace.	
> Whitelisted apps for external SD card	Add applications that can use an external SD card. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 2.2 or higher
Battery optimization exceptions	Set to exempt applications from the battery optimization function. This policy may cause battery loss.	
> Apps excluded from battery optimization	Add applications to exempt from the battery optimization function on Knox Workspace. Applications specified as exceptions can continue to run freely during the battery optimization process. This feature is available on devices running Android 7.0 (Nougat) or higher. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 2.7 or higher
Set General area app installation	Allows the applications installed in the general area to be installed in the Knox Workspace area.	

Policy	Description	Supported devices
> General area app installation list	Add the applications in the general area to be installed in the Knox Workspace area. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** A list of Android platform applications is displayed in **Profile** > **Manage Control App**.	Samsung Knox 2.1 or higher
App Data deletion control setting	Allows control of the deletion of the internal application data inside Knox Workspace.	
> App Data deletion prevention list	Add applications to protect the internal application data from being deleted. The internal data delete button is disabled to block users from arbitrarily deleting application data. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application. **NOTE** Add the registered application to the **App Data deletion protection list** policy with a wildcard character in the package name. Then the application data for the specific registered package cannot be deleted. e.g.) com.*.SDS EMM / com.sds.* / com.*.SDS EMM.*	Samsung Knox 1.0 or higher
> App Data deletion protection exception list	Add applications to delete the internal application data. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application.	Samsung Knox 1.0 or higher
Application force stop prohibition list setting	Set to prohibit application from force stop.	
> Force stop blacklist	Add applications to prohibit force stop. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	Samsung Knox 1.0 or higher

Policy	Description	Supported devices
Show ProgressBar when installing apps	Set to display the ProgressBar, which displays the progress of the application downloads made in EMM.	Android 6.0 or higher

Browser (Knox Workspace)

Browsers must be closed and opened again to apply the changes.

Policy	Description	Supported devices
Android browser	Allows using the Android browser in the Knox Workspace.	Samsung Knox 1.0 or higher
> Cookies	Allows cookies in the Android browser of the Knox Workspace.	Samsung Knox 1.0 or higher
> JavaScript	Allows JavaScript in the Android browser of the Knox Workspace.	Samsung Knox 1.0 or higher
> Autofill	Allows auto-completion of information that you enter on websites in the Android browser of the Knox Workspace.	Samsung Knox 1.0 or higher
> Pop-up block	Allows blocking pop-ups in the Android browser of the Knox Workspace.	Samsung Knox 1.0 or higher
Browser proxy URL	Set the proxy server address for the Android browser in the Knox Workspace. Enter the value in the form of IP:port or domain:port in the fields. **NOTE** • The Chrome browser and Samsung S browser are supported. • The supported version for Chrome is Knox 1.0.1 - 2.6.	Samsung Knox 1.0.1 or higher

Firewall (Knox Workspace)

Firewall configuration sets rules to block access to the network. You can add more firewall policy sets by clicking +.

Policy	Description	Supported devices
Firewall	Set to use the firewall to set target IP addresses. If the policy is not applied, the firewall inside the Knox container is enabled by default. Enable policy is used to set IPs and ports to be excluded from the Disable policy. **NOTE** If the firewall policy is set incorrectly, communication between the EMM server and the EMM Agent is failed, and device control is not possible.	Samsung Knox 1.0 - 2.4.1
> Firewall type	Select and configure the firewall type to use in Knox Workspace. • **All Packages**: Input values for Permission policy and Prohibition policy. **NOTE** • Samsung Knox 1.0 - 2.4.1 is supported for Knox Workspace devices. • **By Application**: Input values for Permission policy (IP), Prohibition policy (IP), Permitted policy (Domain), Prohibited policy (Domain), and DNS setting. • You can use a wildcard character (*) to set the firewall of all applications.	

Policy	Description	Supported devices
>> Permission policy	Input values to permit access through the firewall. 1. Enter a Host Pattern and Port. 2. Select a Network Type: • **All** • **Data**: Only mobile network access is enabled. • **Wi-Fi**: Only Wi-Fi network access is enabled. 3. Select Port Range: • **All** • **Local**: Port access from the device is enabled. • **Remote**: Port access from the target server is enabled. 4. Click + to add. **NOTE** Before setting this policy, disable all IPs and ports by entering a wildcard character (*) to the **Prohibited policy (IP)** ranges	Samsung Knox 1.0 - 2.4.1
>> Prohibition policy	Input values to prohibit access through the firewall. 1. Enter a Host Pattern and Port. 2. Select Network Type: • **All** • **Data**: Only mobile network access is disabled. • **Wi-Fi**: Only Wi-Fi network access is disabled. 3. Select Port Range: • All • **Local**: Port access from the device is disabled. • **Remote**: Port access from the target server is disabled. 4. Click + to add.	Samsung Knox 1.0 - 2.4.1

Policy	Description	Supported devices
>> Permitted policy (IP)	Enter the target IP Address (range) and Port (range) to permit and select the network interface that can access the network. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the IP Address (range) and Port (range). 3. Select the Network Interface. 4. Select the Network Type: • **All** • **Data**: Only mobile network access is enable. • **Wi-Fi**: Only Wi-Fi network access is enable. 5. Select Port Range: • **All** • **Local**: Port access from the device is enable. • **Remote**: Port access from the target server is enable. 6. Click + to add. **NOTE** • To permit the target IPs, ports, and networks, you must set the IP Address (range) and Port (range) to * in Prohibited policy (IP). • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings. • Samsung Knox 2.5 is supported for Knox Workspace devices.	Samsung Knox 2.5 or higher

Policy	Description	Supported devices
>> Prohibited policy (IP)	Enter the target IP Address (range) and Port (range) to prohibit and select the network interface to prohibit network access. Configure the following: 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Enter the IP Address (range) and Port (range). • Enter a wildcard character (*) as an IP Address to prohibit the use of the bandwidth. 3. Select the Network Interface. 4. Select Network Type: • **All** • **Data**: Mobile network access is disable. • **Wi-Fi**: Wi-Fi network access is disable. 5. Select Port Range: • **All** • **Local**: Port access from the device is disable. • **Remote**: Port access from the target server is disable. 6. Click + to add. **NOTE** • When entering the IP address, you can use a wildcard character (*) to disable the bandwidth usage. • For devices less than Samsung Knox 3.6, if the network interface for which options are set is included in the firewall settings, the firewall settings are not applied. If you want to apply the firewall settings, select Network Interface as No settings.	Samsung Knox 2.5 or higher

Policy	Description	Supported devices
>> Permitted policy (Domain)	Input values to permit the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** • To allow specific domains only, you must set all domains in the **Prohibited policy (Domain)** using the wildcard then allow specific domains. • Use a wildcard character (*) to allow the use of a specific domain. The wildcard must be placed before or after the address and not in the middle. e.g.) *android.com / www.samsung*	Samsung Knox 2.6 or higher
>> Prohibited policy (Domain)	Input values to prohibit the target domain address. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input the Domain address (range). **NOTE** Use a wildcard character (*) to disable a specific domain.	Samsung Knox 2.6 or higher
>> DNS setting	Input values to specify the domain server address of all applications or registered applications. 1. Enter the Package Name of the application or click **Add** and then select applications in the “Select Application” window. 2. Input DNS values. • **DNS1**: Primary DNS. • **DNS2**: Secondary DNS. **NOTE** Only one DNS per application can be set and it is effective only when there are no VPN or Proxy policies assigned to the application.	Samsung Knox 2.4 or higher

NOTE

- If there are multiple firewalls, restricted firewalls have a higher priority.
- If a firewall is configured to all applications as well as in specific applications, the policy for each application has a higher priority.
- For example, specify firewall Enable/Disable policies as follows to allow only specific domains in Chrome:
  - Enable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *.samsungknox.com
  - Disable Policy (Domain)
    Package Name: com.android.chrome, Domain Address: *
- Firewall settings supports IPv6 for SDK 2.6 or later. Even if IPv4 and IPv6 addresses refer to a physically identical address, each must be configured separately.

Container Data (Knox Workspace)

Policy	Description	Supported devices
Moving an application to container	Allows moving applications from the general area to the Knox Workspace. **NOTE** Android 10 (Q) or higher devices are not supported.	Samsung Knox 2.0 or higher
Moving a file to Knox area	Allows moving files from the general area to the Knox Workspace. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
Moving a file to General area	Allows moving files from the Knox Workspace to the general area. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
Calendar sync setting	Allows syncing calendar data between the general area and the Knox Workspace. **NOTE** Android 13 and later, this policy is no longer support.	Samsung Knox 2.0 or higher
> Calendar data sync	Set how the calendar data is synced between the general area and the Knox Workspace: • **Allow Import**: Allows to import the calendar data of the general area to the Knox Workspace. • **Allow Export**: Allow to export the calendar data of the Knox Workspace to the general area.	Samsung Knox 2.0 or higher
Contacts sync setting	Allows syncing contact data between the general area and the Knox Workspace. **NOTE** Android 13 and later, this policy is no longer support.	
> Contacts data sync	Sets Data Loss Protection (): • **Allow Import**: Allows to import the contact data of the general area to the Knox Workspace. • **Allow Export**: Allows to export the contact data of the Knox Workspace to the general area.	Samsung Knox 2.0 or higher
Copy and Paste Clipboard per Profile	Allows copying and pasting with the clipboard between general area and workspace area.	Android 7.1 or higher

Dual DAR(Knox Workspace)

Policy	Description	Supported devices
Data Lock Timeout (Minutes)	Sets the Dual DAR Workspace data lock time. The Dual DAR Workspace will be changed to the data lock state when the set time elapses after screen lock. The minimum time you can set is 1 minute. **NOTE** • When setting the Dual DAR data lock function, the device and Knox Container password policies should be set. You must set the passwords in **Android (Legacy)** > **Security** > **Device Password** and **Knox Workspace** > **Security** > **Knox Container Password**. • The Dual DAR data lock function is Smart Lock and it is impossible to lock the data unless the screen is locked in both the general area and the Workspace area. You must set it up in **Knox Workspace** > **Security** > **Block functions on lock screen** > **Trust Agent.** • When Dual DAR data lock is activated, biometric authentication is disabled. When you set a policy, be aware that the fingerprint/iris lock function is not available.	Samsung Knox 3.3 or higher
Restrict DE Storage Access	Sets the access restriction of an application to DE (Device Encrypted) space.	Samsung Knox 2.0 or higher
Whitelisted Apps for Data Lock and DE Storage Access	When locking Dual DAR data, all general applications will stop working due to Knox security policies. Sets a whitelist to allow certain applications to access even when data is locked. Applications on the whitelist can access a DE space even if **Restrict DE Storage Access** is restricted.	
> Whitelisted Apps	Add an application to allow it to run. EMM applications are automatically registered on the whitelist. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete applications, click 🗑 next to the added application.	Samsung Knox 2.0 or higher

Exchange ActiveSync (Knox Workspace)

You can add more Exchange ActiveSync policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each Exchange setting.
Description	Enter a description for each Exchange setting.
Remove available	Allows users to delete the Exchange settings in Knox Workspace.
Office 365	Allows to configure the Exchange settings. **NOTE** This policy will automatically fill out the Exchange server address and the SSL option as 'Use'.
User information input method	Select an input method for entering user information.
> Manual Input	Select to manually enter the email address, account ID, and password of a user. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
> Connector interworking	Select to choose a connector from the User Information Connector list. **NOTE** All the connectors are listed in **System** > **Connector** > **Directory**.
> User Information	Select to access the exchange server using the registered EMM email and ID. The password must be entered from the user's device.
Domain	Enter a domain address for the Exchange server. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Exchange server address	Enter the Exchange server information such as IP address, host name or URL.
Sync measure for the early data	Select the interval period to sync the past emails. The sync interval and synchronization are in accordance with the email application settings.
Email sync Interval	Select the interval period to sync the past emails. **NOTE** The sync interval and synchronization are in accordance with the email application settings.
User certificate input method	Select an input method for entering certificate information.

Policy	Description
> EMM Management Certificate	Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Certificate**: Select a certificate to use from the User Certificate list.
> Connector interworking	Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. • **User certificate Connector**: Select a connector to use from the User certificate Connector list.
> Issuing External CA	Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. • **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Sync calendar	Syncs schedules on a calendar from a server to a device.
Sync contacts	Syncs contact information in a phone book from a server to a device.
Sync task	Syncs tasks items from a server to a device.
Sync notes	Syncs notes from a server to a device.
SSL	Set to use SSL for email encryption. **NOTE** If **Office365** setting is used, the SSL option is automatically set to 'Use'.
Signature	Enter the email signature to use.

Policy	Description
Notification	Notifies the user of new emails.
Always vibrate on notification	Notifies the user of new emails with a vibration.
Silent notification	Mutes email notifications. **NOTE** **Always vibrate on notification** and **Silent notification** cannot be used at the same time.
Attachments capacity (byte)	Enter the email attachment file size limit in bytes. The input value ranges from 1 to 52428800 (50MB).
Maximum Size of Email Body (Kbyte)	Select a maximum value for the email body size. This is only set once during the initial Exchange ActiveSync setup.
> Default Size of Email Body (Kbyte)	Select the default value of the email body size. **NOTE** Select this setting after the **Maximum Size of Email Body (Kbyte)** setting.

Email Account (Knox Workspace)

You can add more email account policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each email account setting.
Description	Enter a description for each email account setting.
Remove available	Allows users to delete the email account settings in Knox Workspace.
Default Account	Specifies to usage of the default account.
User Information input method	Select an input method for entering user information.
> Manual Input	Select this to enter the email address manually. You can also enter the incoming server ID, incoming server password, outgoing server ID, and outgoing server password for the email connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be entered automatically.
> Connector interworking	Select a connector from the user information connector. **NOTE** The connectors are listed in **System** > **Connector** > **Directory**.
> User Information	Select to access the relevant mail server using the registered EMM email, ID, and password. The password must be entered from the user's device.

Policy	Description
Incoming Server Protocol	Select between the POP3 (pop3) and IMAP (imap) protocol.
Outgoing Server Protocol	Entered automatically as SMTP.
Incoming Server Address/ port	Enter the Incoming Server address/port in a provided format.
Incoming Server ID	Enter an incoming server ID to log in to the incoming mail server manually. This protocol is only available when **Manual Input** is selected. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be entered automatically.
Incoming Server Password	Enter an incoming server password to log in to the incoming mail server manually. This protocol is only available when **Manual Input** is selected.
Outgoing Server Address/ port	Enter the outgoing Server address/port in a provided format.
Outgoing Server ID	Enter an outgoing server ID to log in to the outgoing mail server manually. This protocol is only available when **Manual Input** is selected. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be entered automatically.
Outgoing Server Password	Enter an outgoing server password to manually log in to the outgoing mail server. This protocol is only available when **Manual Input** is selected.
Incoming SSL	Select this to use SSL encryption.
Outgoing SSL	Select this to use SSL encryption.
Notification	Select an email notification method. • **Enable Notification**: Activates email notification. • **Enable 'Always notify by vibrate mode'**: Notifies the user of new emails with a vibration. • **Disable Notification**: Deactivates email notification.
All incoming certificates	Allows receiving certificates.
All outgoing certificates	Allows sending certificates.
Signature	Enter an email signature to use.
Account Name	Assign an account name.
Sender Name	Assign a sender name.

Bookmark (Knox Workspace)

You can add, modify, or delete the bookmarks in the Samsung S browser, the default browser on Samsung devices. You can add more bookmark policy sets by clicking +.

NOTE

- Browsers must be closed and opened again to apply the changes.
- Even if a user modifies a registered bookmark or registers a bookmark with the same URL and name, it will not be deleted when the bookmark setting is deleted.
- Even if a user manually deletes the set bookmark, due to the limitations of Samsung devices, the application may still appear to be installed. In this case, you have to delete the bookmark in the profile, and then recreate the bookmark.

Policy	Description
Configuration ID	Assign a unique ID for each bookmark setting.
Description	Enter a description for each bookmark setting.
Bookmark page URL	Enter a website address to go to when a bookmark is selected.
Bookmark name	Enter a bookmark name to be displayed as the title in a bookmark.

Knox VPN (Knox Workspace)

Knox VPN settings are provided to help you set up a VPN on a Knox Workspace more easily. You can add more Knox VPN policy sets by clicking +.

NOTE

- Only one Knox VPN can be set on a device regardless of the Know Workspace area or General area.
- Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for the Knox VPN setting.
VPN name	Enter a VPN name to display on the user device.
Description	Enter a description for the Knox VPN setting.
Remove available	Allows users to delete the Knox VPN setting.
VPN vendor name	Select a VPN vendor among **F5**, **Juniper**, **Cisco** and **User defined**. Input fields vary depending on the selected VPN vendor name. **NOTE** Select **User defined** to set up a different vendor's VPN service, such as Sectra mobile VPN. For more information, see Entering a VPN vendor manually.

Policy	Description
VPN client vendor package name	Entered automatically according to the selected VPN vendor name. If **User defined** is selected, you must manually enter this protocol.
VPN type	Entered automatically when you selected **F5**. If other vendors are selected, you must manually select this protocol.
Entering methods for Knox VPN	Select an entering method for Knox VPN information. • **Manual Input**: Allowed for all VPN vendors except for **User defined**. For more information, see Configuring a Knox VPN profile manually. • **Upload profile**: Allowed for all VPN vendors. **NOTE** Input fields vary depending on the selected VPN vendor and the entering method.
Upload Knox VPN profile	Allows uploading a Knox VPN profile when you set **Entering methods for Knox VPNs** to **Upload profile**. You can upload a text file in the JSON format. JSON varies depending on the VPN vendor and VPN type. For more information about sample files, see Entering a VPN vendor manually.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. **NOTE** All users share this one certificate for each network setting. Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Authentication Method	Select an authentication method. • **Not Applicable**: Disables authentication. • **Certificate-based Authentication**: Uses certificates for authentication in the Knox VPN setting. • **CAC-based Authentication**: Uses two-factor authentication provided by CAC (Common Access Card).
CA Certificate	Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **Knox VPN** and the Type set as **Root** will appear on the list.

Policy	Description
Server certificate	Select a certificate to use from the certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose has been set as **Knox VPN** and the Type set as **User** will appear on the list.
FIPS mode	Allows the use of FIPS mode. FIPS (US Federal Information Processing Standards) encrypts all data with FIPS-140-2 authentication modules between the server and client.
Auto Re-connection	Allows connecting automatically when an error occurs.
VPN route type by application	Select to use a VPN for selected applications or for all applications in the General area. • **By Application**: Click **Add** next to **The VPN applied package name per app**, select applications, and then click **Save**. • **All packages of general area**: All applications in the General area are subject to a VPN.

Configuring a Knox VPN profile manually

You can manually enter a profile when **Manual Input** is selected in the **Entering methods for Knox VPN** field. Set the options as below:

1. Enter the IP address, host name, or URL of the VPN server in the **Server address**.
   - The VPN route type, which enables the use of VPN tunneling, is automatically entered.
2. Select to use user authentication.
3. Enter the user information for authentication depending on the selected method of entering user information:

Method	Description
Manual Input	Enter the user ID and Password for the VPN connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Connector interworking	Choose a connector from the **User information Connector**. All the connectors are listed in **System** > **Connector** > **Directory**.
User Information	Use the user information registered in EMM to access a VPN.

4. Select a VPN type and enter the parameters. Required parameters vary depending on the selected VPN type.
   - If the VPN type is set to **SSL**, enter the SSL algorithm that the server requires for the **SSL algorithm** section.
5. If the VPN type is seConfigure the advanced option.

Item	Description
DNS search domain	Enter the DNS name.
DNS server	Enter the DNS address according to the IP pattern.
Forwarding route	Entered automatically when **Subnet Bits** is selected
Subnet Bits	Select **None** or **/1** from **/30**.

6. Select a VPN connection type.
   - **KEEP ON**: Keep the VPN connection.
   - **On Demand**: Connect to the VPN upon request.
7. Select the chaining type.

8. Select to use the UID PID.
9. Select to use the Logon mode.
    - Logon mode is used when the VPN vendor name is set to **F5**.

Certificate (Knox Workspace)

You can add more certificate policy sets by clicking +.

NOTE Android 13 and later, this policy is no longer support.

Policy	Description
Configuration ID	Assign a unique ID for each certificate setting.
Description	Enter a description for each certificate setting.
Automatic Installation	Select whether to install each certificate automatically. The default value is **Use**. However, if you set only one certificate, it will be automatically installed. **NOTE** • Certificates are installed per the setting values of the automatic installation only when devices have EMM Agent v2.5.5 and the server is EMM v2.5.5 or higher. • For certificate settings created on lower versions than EMM v2.5.5, the automatic installation value will be displayed as **Do not use**.

Policy	Description
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. **NOTE** All users share this one certificate for each network setting. Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Certificate category	Select a certification category when **EMM Management Certificate** is selected in **User certificate input method**, • **CA certificate**: Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as CA Cert and the Type set as Root will appear on the list. • **User certificate**: Select a certificate to use from the User Certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as CA Cert and the Type set as User will appear on the list.

Configuring iOS Policies

Create a profile and register policies for iOS devices.

You can configure the policies below for iOS devices. The availability of each policy varies depending on the OS version.

→ System (iOS)
Allows features such as camera, screen capture, and Siri.

→ Security (iOS)
Configures the password settings.

→ Application (iOS)
Allows using Gamer Center, iMessage, and YouTube, and also enables configuring options for application controls, such as installation and blacklist/whitelist.

→ Phone (iOS)
Configures the phone settings such as video calling and voice dialing.

→ Share (iOS)
Allows the use of AirDrop and the transferring of data between managed applications and unmanaged applications.

→ Browser (iOS)
Allows using the Safari browser and configuring its settings.

→ iCloud (iOS)
Configures the iCloud settings, such as backup, iCloud photo library, and photo sharing.

→ Media (iOS)
Enables selecting a country to choose the level of media content, such as movies, TV shows, and applications

→ Wi-Fi (iOS)

Configures Wi-Fi settings, such as SSID, security type, and proxy.

→ Exchange (iOS)

Configures the Microsoft Exchange ActiveSync account to synchronize email, calendar, contacts, and tasks from the Exchange account.

→ VPN (iOS)

Configures VPNs (Virtual Private Network) on iOS devices.

→ Certificate (iOS)

Set the certificate and the user authentication method on devices for when device users authenticate.

→ SSO (iOS)

Configures the SSO (Single Sign On) settings for one-click access to all applications.

→ Cellular (iOS)

Configures the cellular network settings, such as AttachAPN and APNs.

→ AirPrint (iOS)

Configures the AirPrint settings to enable computers to automatically detect an AirPrint printer.

→ Font (iOS)

Allows the delivering of new fonts to devices.

→ WebClip (iOS)

Configures the display of web shortcuts on an iOS device.

→ App Lock (iOS)

Configures the functions of an application that is locked down on a supervised device

→ Global HTTP Proxy (iOS)

Configures a global HTTP proxy to direct all HTTP traffic through a designated proxy server.

→ AirPlay (iOS)

Configures the AirPlay settings to allow iOS devices to share content.

→ Web Content Filter (iOS)

Configures the settings for the Web content filter to control accessing specific URLs on a web browser.

→ Managed domains (iOS)

Specifies URLs or subdomains to allow downloading content from these domains without any restrictions.

→ Network Usage Rules (iOS)

Configures network usage rules to control which applications can access data or when the device is roaming.

System (iOS)

Policy	Description	Supported devices
Camera	Allows using the camera.	iOS 4.0 or higher
> Use Camera from Lock Screen	Even if the camera policy is set to disallow, you can select whether to use the camera on the lock screen. If you disallow this policy, using the camera on the lock screen is disabled. The policy is valid at the time of initial application and after that, the settings in the camera policy take precedence.	iOS 4.0 or higher
Screen capture	Allows use of the screen capture function, which is already set as default.	iOS 4.0 or higher
Siri	Allows using Siri.	iOS 5.0 (iPhone 4S) iOS 6.0 (iPad 3)
> Siri on lock screen	Allows using Siri on the lock screen.	iOS 5.1 (iPhone 4S) iOS 6.0 (iPad 3)
> Web search result on Siri	Allows displaying the web search results on Siri.	iOS 7.0 or higher Supervised
> Profanity filter on Siri	Select to use the Profanity filter on Siri. • **Forced use**: Users are forced to use the Profanity filter on Siri. • **User selection**: Users are allowed to select whether to use the Profanity filter on Siri.	iOS 5.0 (iPhone 4S) iOS 6.0 (iPad 3) or higher Supervised
Submission of diagnosis and usage details	Allows submitting diagnostic results and usage information to the manufacturer.	iOS 6.0 or higher
Passbook on lock screen	Allows using the Passbook on the lock screen.	iOS 6.0 or higher
Control center on lock screen	Allows using the Control center on the lock screen.	iOS 7.0 or higher
Display notifications on lock screen	Allows displaying the notifications on the lock screen.	iOS 7.0 or higher
Display Today view on lock screen	Allows displaying the Today view on the lock screen.	iOS 7.0 or higher
Manual installation for profile	Allows manual installation of the Apple Configuration Profile.	iOS 6.0 or higher Supervised
Control editing account information	Allows editing the account information.	iOS 7.0 or higher Supervised

Policy	Description	Supported devices
Automatic updates of certificate trust settings	Allows automatic updates of the certificate trust settings.	iOS 7.0 or higher
Encryption for iTunes backup	Select to encrypt the iTunes backup. • **Forced use**: Users are forced to encrypt. • **User selection**: Users are allowed to select whether to encrypt.	iOS 7.1 or higher
iTunes pairing	Allows iTunes connection with unauthorized PCs.	iOS 7.0 or higher Supervised
Limited Ad tracking	Select to use the Limit Ad tracking. • **Forced use**: Users are forced to use Limit Ad tracking. • **User selection**: Users are allowed to select whether to use Limit Ad tracking.	iOS 7.0 or higher
Factory reset	Allows a device to factory reset.	iOS 8.0 or higher Supervised
Result of web search with Spotlight	Allows displaying the web search results from Spotlight search.	iOS 8.0 or higher Supervised
Block configuration	Allows users to configure any restrictions on the menus by activating the block menu function. If the policy is prohibited, the users cannot configure the device via the block menu function.	iOS 8.0 or higher Supervised
Change device name	Select to automatically change the device name to a mobile ID when updating the profile. For this policy, you can send a device command to set the device name as the mobile ID.	iOS 8.0 or higher Supervised
Allow Bluetooth Modification	Allows modifying Bluetooth settings on the device.	iOS 11.0 or higher Supervised

Security (iOS)

Policy	Description	Supported devices
Password policies	Set to apply the password policy when the screen is locked.	
> Password strength	Set the password strength on the screen. • **None**: Set the password with a four digit number. • **Numeric**: Set the password using numbers • **Alphanumeric**: Set the password using alphanumeric characters. • **Complex**: Set it so that the passwords must include alphanumeric and special characters.	iOS 4.0 or higher
> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before resetting the device to its factory settings. The value can be between 0 - 10 times.	iOS 4.0 or higher
> Minimum length	Set the minimum length of the password. The value can be between 0 - 16 characters.	iOS 4.0 or higher
> Expiration after (days)	Set the maximum number of days before the password must be reset. The value can be between 0 - 730 days.	iOS 4.0 or higher
> Manage password history (times)	Set the minimum number of new passwords that must be used before a user can reuse the previous password. The value can be between 0 - 50 times.	iOS 4.0 or higher
> Screenlock time (min)	Set the maximum inactive time before the screen of the device is locked. The maximum allowed time varies by device-type. **NOTE** 1, 3, and 4 minute intervals are available with iPhone. 10 and 15 minute intervals are available with iPad.	iOS 4.0 or higher
> Screenlock grace period (min)	Set the time duration for device lock after turning off a device screen without entering the password. **NOTE** Select 0 to lock the device immediately.	iOS 4.0 or higher
> Screen unlock with Touch ID	Allows screen unlock with Touch ID.	iOS 7.0 or higher

Application (iOS)

Policy	Description	Supported devices
Application installation	Allows the installation of applications. **NOTE** Applications can be installed using MDM but cannot be installed using iTunes.	iOS 4.0 or higher Supervised (iOS 13 or higher)
> Allow App Store to install Apps	Allows using the App Store for application installation. **NOTE** Applications can be installed using MDM but cannot be installed using iTunes.	iOS 9.0 or higher Supervised
Application uninstallation	Allows applications to be deleted.	iOS 4.2.1 or higher Supervised
iTunes Store	Allows using the iTunes Store.	iOS 4.0 or higher Supervised (iOS 13 or higher)
> Explicit content on music and podcasts	Allows the purchase of explicit content from the iTunes Store.	iOS 4.0 or higher Supervised
> Require iTunes password for every purchase	Select to require the iTunes Store password for every purchase made in the iTunes Store.	iOS 5.0 or higher
Game Center	Allows using Game Center.	iOS 6.0 or higher Supervised
> Adding friends in Game Center	Allows adding friends in Game Center.	iOS 4.2.1 or higher Supervised (iOS 13 or higher)
> Multiplayer games	Allows multiplayer games in Game Center.	iOS 4.1 or higher Supervised
iBookstore	Allows iBookstore.	iOS 6.0 or higher Supervised
Inappropriate content download on iBookstore	Allows downloading unrated media content. **NOTE** iOS 6 or lower only applies when you allow iBookStore policies	iOS 6.0 or higher
iMessage	Allows using the messaging application.	iOS 6.0 or higher Supervised
YouTube	Allows using YouTube.	iOS 5.1 or lower

Policy	Description	Supported devices
Find friends	Allows the **Find My Friends** function.	iOS 7.0 or higher Supervised
In-app purchase	Allows in-app purchases.	iOS 4.0 or higher
Application black/ whitelist Settings	Set to control the application installation policies. Both the **blacklist** and **whitelist** policies can be applied at the same time. **NOTE** If the **Application black/whitelist Settings** policy is set with no applications, then no other applications except for the EMM applications such as EMM client and Secure Browser will be allowed to be executed and installed.	iOS 4.0 or higher Supervised (iOS 13 or higher)
> Application installation blacklist	Add applications to prohibit their installation. Blacklisted applications will be deleted even if they were previously installed. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** An application that has been added on the **Application installation whitelist** cannot be added.	iOS 4.0 or higher Supervised (iOS 13 or higher)
> Application installation whitelist	Add applications to allow their installation. Any applications not on the whitelist are deleted, even if they are not on the blacklist. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application. **NOTE** An application that has been added on the **Application installation blacklist** cannot be added.	iOS 4.0 or higher Supervised (iOS 13 or higher)
Autonomous single app mode	Set to use Autonomous Single App Mode, which enables applications to use Single App Mode on request. This policy grants a permission to perform the Application Lock function.	iOS 7.0 or higher Supervised

Policy	Description	Supported devices
> List of apps allowing auto single app mode	Add applications to autonomously enable or disable Single App Mode. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click 🗑 next to the added application.	iOS 7.0 or higher Supervised
To trust company app	Allows the trusted Company applications. Company applications installed before the policy has been set can still be executed.	iOS 9.0 or higher

Phone (iOS)

Policy	Description	Supported devices
Modification of cellular data settings for each application	Allows modifying cellular data usage per application.	iOS 7.0 or higher Supervised
Video calling	Allows video calling.	iOS 4.0 or higher Supervised (iOS 13 or higher)
Voice dialing	Allows video dialing.	iOS 4.0 or higher
Background fetch for roaming	Allows background fetch when roaming.	iOS 4.0 or higher

Share (iOS)

Policy	Description	Supported devices
Data transfer from managed to unmanaged applications	Allows transferring data from managed applications installed by EMM to unmanaged applications installed by users.	iOS 7.0 or higher
Data transfer from unmanaged to managed applications	Allows transferring data from unmanaged applications installed by users to managed applications installed by EMM.	iOS 7.0 or higher
AirDrop	Allows the use of AirDrop.	iOS 7.0 or higher Supervised

Policy	Description	Supported devices
Consider AirDrop not managed	Allows the sharing of managed documents when using AirDrop on the device.	iOS 9.0 or higher Supervised

Browser (iOS)

Policy	Description	Supported devices
Safari	Allows using Safari, the default iOS browser.	iOS 4.0 or higher Supervised (iOS 13 or higher)
Cookies	Set the cookies permission in Safari. • **Disallow**: Disallows accepting cookies. • **Currently only connected websites are allowed**: Allows accepting cookies from the currently connected sites. • **Only visited websites are allowed**: Allows accepting cookies from the visited sites. • **Always**: Always allows cookies.	iOS 4.0 or higher
JavaScript	Allows JavaScript in Safari.	iOS 4.0 or higher
Autofill	Allows auto-completion of information that you enter on websites in Safari.	iOS 4.0 or higher Supervised (iOS 13 or higher)
Block pop-ups	Allows blocking pop-ups in Safari.	iOS 4.0 or higher
Untrusted TLS certificate	Allows to accept untrusted TLS certificates.	iOS 5.0 or higher
Web forgery warning	Shows a warning message about potentially fraudulent websites. • **Forced use**: Safari is forced to display a warning message. • **User selection**: Users are allowed to select whether to use web forgery warning.	iOS 4.0 or higher

iCloud (iOS)

Policy	Description	Supported devices
Backup	Allows backing up the device data on iCloud.	iOS 5.0 or higher
Document synchronization	Allows synchronizing device documents on iCloud.	iOS 5.0 or higher Supervised (iOS 13 or higher)
iCloud Photo Library	Allows use of the iCloud Photo Library for uploading photos and videos on iCloud.	iOS 9.0 or higher
Photo stream	Allows using Photo Stream for storing personal photos on iCloud.	iOS 5.0 or higher
Photo sharing	Allows using Photo Sharing for sharing personal photos through iCloud.	iOS 6.0 or higher
Keychain synchronization	Allows synchronizing Keychain Synchronization on iCloud, which helps users to have consistent access to their user account, name, password, credit card number, email, contracts, schedule, and other user information on all their devices.	iOS 7.0 or higher
Managed app synchronization	Allows synchronizing managed applications installed by the EMM server to save data on iCloud.	iOS 8.0 or higher
Handoff	Allows the use of Handoff, one of the Apple's Continuity features, to move and continue performing the same tasks seamlessly between devices through iCloud.	iOS 8.0 or higher

Media (iOS)

Policy	Description	Supported devices
Rating for each country	Select a country to set a rating level for media content, such as movies, TV shows, and applications, from below: • United States/United Kingdom/New Zealand/Japan/ Ireland/Germany/France/Canada/Australia.	iOS 4.0 or higher
> Movies	Set the maximum allowable movie rating.	iOS 4.0 or higher
> TV Shows	Set the maximum allowable TV show rating.	iOS 4.0 or higher
> Apps	Set the advertisement tracking restriction on the device.	iOS 4.0 or higher

Wi-Fi (iOS)

You can add more Wi-Fi policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each Wi-Fi setting.
Description	Enter a description for each Wi-Fi setting.
Network name (SSID)	Enter the identifier of a wireless router to connect to. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Security Type	Specifies the access protocol used and whether certificates are required.
> WEP	Set a password.
> WPA/WPA2	
> For all individuals	
> Enterprise WEP	Configure the following items: • **Protocol** - **Permitted EAP Type**: Select the EAP types to permit. You can select multiple types. - **EAP-FAST**: Configure the EAP-FAST options. Enable the next options by clicking the previous one. - **A dynamic trust decision by the user**: Select whether to use the option. - **Allow direct connection(Proxy URL)**: Select whether to use the option. • **Authentication** - **One-time password for connection**: Check to enable. - **Manual Input**: Enter the user ID and Password for the Wi-Fi connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. - **Connector interworking**: Choose a connector from the **User information Connector**. • **Trust** - **Root Certificate**: Select a Root Certificate to use.
> Enterprise WPA/WPA2	
> For all enterprises	
Hotspot Availability	Check to enable Hotspot usage and configure its settings. If this policy is enabled, the device will be connected to Wi-Fi access points that support Hotspot 2.0.
> Hotspot Domain Name	Assign an identifier to the Wi-Fi hotspot service displayed on a device.
> Operator Name	Assign the name of the network provider shown on the device.

Policy	Description
> Roaming Consortium OI	Add a Roaming Consortium organization ID to connect to.
> Network Access ID	Add an ID to authenticate network access.
> Hotspot Operator Code	Add both the Mobile Country Code (MCC) and the Mobile Network Code (MNC). **NOTE** For SK Telecom (a South Korean wireless telecom operator) devices, enter 45005.
Hidden Network	Check the checkbox to hide the network from the list of available networks on the device. The SSID does not broadcast.
Auto Connect (iOS 5 and above)	Check the checkbox to use an automatic Wi-Fi connection. **NOTE** This setting is for iOS 5 or higher.
Protocol	Specifies the permitted protocol for the Wi-Fi network. **NOTE** This tab is enabled if the **Security Type** is selected as Enterprise WEP, Enterprise WPA/WPA2, or for all enterprises.
> Permitted EAP Type	Select more than one permitted protocol: TLS, LEAP, EAP-FAST, TTLS, PEAP, and EAP-SIM. **NOTE** If TTLS is checked, select an extra protocol from the Internal Authentication Protocol.
> EAP-FAST	Select PAC protocols to use from the following: • **Use PAC**: Determines whether to use PAC. • **PAC Deployment**: Check the **Use PAC** option to enable it. • **Anonymous PAC Deployment**: Check **PAC Deployment** to enable it.
> A dynamic trust decision by user	Allows using a dynamic trust decision by the user protocol.
> Allow direct connection (Proxy URL)	Allows using the direct connection protocol.
Authentication	Specifics the authentication of the Wi-Fi users. **NOTE** This tab is enabled if the **Security Type** is selected as Enterprise WEP, Enterprise WPA/WPA2, or for all enterprises.

Policy	Description
> One-time password for connection	Select to ask users to enter the password whenever Wi-Fi is connected. • If checked, the Auto Connect setting is automatically disabled. • If unchecked, the Auto Connect is automatically activated. **NOTE** This setting is for iOS 5 or higher.
> User information input method	Specifies the user information used and whether certificates are required. Select an input method as follows: • **Manual Input**: Enter the user ID and Password for the Wi-Fi connection. • **Connector interworking**: Choose a connector from the User information Connector. You can also click **Lookup** to open the reference items list and select an item from it when entering an ID for the **Manual Input**. The reference value will be automatically entered.
> External ID	Assign an external ID for **Manual Input**. **NOTE** This setting is available when either TTLS, PEAP, or EAP-FAST is selected.

Policy	Description
> User Certificate Type	Select the user certificate type. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. - **User certificate Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. - **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Trust	Specifies the required certificates. This tab is enabled if the **Security Type** selected is Enterprise WEP, Enterprise WPA/WPA2, or for all enterprises.
> Trusted certificate name	Add the name of the Trusted certificate.
> Root Certificate	Select a Root Certificate.
Proxy	Select a proxy server settings method. **NOTE** This setting is for iOS 5 or higher.

Policy	Description
> Manual	Configure the proxy server manually. • **Proxy IP Address and Port**: Enter the IP address of the proxy server and the port number used by the proxy server. • **User name**: Enter the username for the proxy server. • **Proxy Authenticated User Password**: Enter the password for the proxy server.
> Auto	Configure the proxy server automatically. • **Proxy Server URL**: Enter the URL of the proxy server.

Exchange (iOS)

You can add more Exchange policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each Exchange setting.
Description	Enter a description for each Exchange setting.
Office365	Allows to configure the Exchange settings. **NOTE** This policy will automatically fill out the Exchange server address and the SSL option as 'Use'.
User information input method	Select an input method for entering user information.
> Manual Input	Select to manually enter the email address, account ID, and password of a user. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
> Connector interworking	Select to choose a connector from the User Information Connector list. **NOTE** All the connectors are listed in **System** > **Connector** > **Directory**.
> User information	Select to access the exchange server using the registered EMM email and ID. The password must be entered from the user's device.
Domain	Enter a domain address for the Exchange server. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Host	Enter the host name of the email server.

Policy	Description
SSL	Set to use SSL for email encryption. **NOTE** If **Office 365** setting is used, the SSL option is automatically set to 'Use'.
User certificate input method	Select an input method for entering certificate information.
> EMM Management Certificate	Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **User Certificate**: Select a certificate to use from the User Certificate list.
> Connector interworking	Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. • **User certificate Connector**: Select a connector to use from the User certificate Connector list.
> Issuing external CA	Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. • **Issuing external CA**: Select an external CA to use from the Issuing external CA list. **NOTE** To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.
Sync Interval	Select the interval period to sync the past emails. **NOTE** The sync interval and synchronization are in accordance with the email application settings.

Policy	Description
Do not move message to other accounts	Select to use the policy.
Available only on mail app	Select to use the policy.
Do not sync the recently used email address	Select to use the policy.
Activate S/MIME	Check to activate and configure S/MIME functions for email security.
> S/MIME signing certificate input method	Select EMM Management Certificate or Connector interworking. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user.
> S/MIME Signing Certificate	Available only when **EMM Management Certificate** is selected. Choose the signing certificate according to the S/MIME signing certificate input method.
> S/MIME signing certificate connector	Available only when **Connector interworking** is selected Choose the signing certificate connector according to the S/MIME signing certificate input method.

Policy	Description
> S/MIME encryption certificate input method	Select EMM Management Certificate or Connector interworking. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. All users share this one certificate for each network setting. **NOTE** Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user.
> S/MIME Encryption Certificate	Available only when **EMM Management Certificate** is selected. Choose the Encryption Certificate according to the S/MIME encryption certificate input method.
> S/MIME signing certificate connector	Available only when **Connector interworking** is selected Choose the signing certificate connector according to the S/MIME signing certificate input method.
> S/MIME Enable Per Message Switch	Check the checkbox to enable S/MIME per message.

VPN (iOS)

You can configure the VPN settings to connect to a private network through a public network. You can add more VPN policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for the VPN setting.
Description	Enter a description for the VPN setting.

Policy	Description
Connection type	Select a connection type and enter the parameters. Required parameters vary depending on the selected connection type. • **L2TP**: Set the **Shared Security** and **Send All Traffic** options. • **PPTP**: Set the **Encryption Step** and **Send All Traffic** options. • **IPSec (Cisco)**: Enter the items depending on the selected device authentication type: – If **Device Authentication** is set to **certificate**, set **Domain/Host Pattern**, and **Action** for it. And then, select a **User certification input method** and set to **Include User PIN** when a device is authenticated. – If **Device Authentication** is set to **Shared Security/Group Name**, set **Group Name** and **Shared Security** options. And then, set to **Use mixed authentication** and **Password Request** when a device is connected with VPN. • **Cisco AnyConnect**: Set the **Group Name** option. • **Juniper SSL**: Set the **Realm** and **Role** options. If this is selected, Pulse secure VPN, a new VPN, is supported and previous Juniper Pulse versions will not be supported. • **SonicWALL Mobile Connect**: Set the **Login Group** or **Domain** options. • **IKEv2**: For IKEv2, see Configuring VPN IKEv2 connection.
Server address	Enter the IP address, host name, or URL of the VPN server that the device needs to access.
VPN Application Allocation	Select applications that will be allowed to connect to a VPN automatically. Click **Add** and select applications. And then, click **OK**.
Safari Domain	Select URLs that will be allowed to connect to a VPN automatically on Safari. Enter a domain address, and then click +.
VPN type for each app	Select a VPN type for each application. • **packet-tunnel**: for app-layer tunneling • **app-proxy**: for packet-layer tunneling
User Connection Authentication Type	Select an authentication type for user connection between **Password** and **RSA SecurID**.
User information input method	Select an input method for entering user information. • **Manual Input**: Enter the user ID and Password for VPN connection. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. • **Connector interworking**: Choose a connector from the **User information Connector**. All the connectors registered in **System** > **Connector** > **Directory** are listed in the User information Connector. • **User Information**: Use the user information registered in EMM to access VPN.

Policy	Description
ID	Set an ID for the VPN settings. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Password	Set a password for the VPN settings. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
User certificate input method	Select an input method for entering certificate information. • **EMM Management Certificate**: Register an external certificate on the EMM server for each network setting, and then verify each network setting using that certificate. **NOTE** All users share this one certificate for each network setting. Navigate to **Advanced** > **Certificate** > **External Certificate** to register network settings for each purpose. – **User certificate**: Select a certificate to use from the User Certificate list. • **Connector interworking**: Verifies network settings using the user information obtained by applying the filter set for the connector. To verify the network settings on the device, you should set the Service Type as **Profile Configuration (Certification)** when you register a connector in **System** > **Connector** > **Directory**. To learn more about how to add a directory connector, see Adding a directory connector. When you search for a user using the filter set for the connector, the user certificate (.p12 or .pfx) corresponding to the obtained user information is applied along with a profile, allowing you to use this certificate to verify the user. – **User Information Connector**: Select a connector to use from the User certificate Connector list. • **Issuing external CA**: Register a certificate obtained from an external certificate authority to **Advanced** > **Certificate** > **Certificate Template**. Then, you register a certificate template for each network setting, and verify it as a user certificate. To learn more about how to add an external certificate, see Adding external certificates. – **Issuing External CA**: Select an external CA to use from the Issuing external CA list. **NOTE** • User certificate input method appears only when certificate is selected in the user connection authentication type or in the device authentication. • To install a certificate on the Trusted Anchor database for Android, the minimum strength of the device password must be set to **Numeric** or stronger. When the device reboots, the user must enter the password to access the certificate for the EMM service.

Policy	Description
Proxy Settings	Select the setting for the proxy server. • **Manual**: Enter the proxy IP address and port number. Then, assign a user name and proxy authenticated user password. • **Auto**: Enter the proxy server URL address.

Configuring VPN IKEv2 connection

If the connection type is set to **IKEv2**, you can configure the setting as follows:

1. Set the **VPN auto connection** settings.
   - **VPN auto connection (Only devices allowed by director)**: Keeps VPN activated on the device.
   - **Allow users to deactivate auto connection**: Allows users to deactivate auto connection on the device.
   - **Use the same tunnel for both cellular and Wi-Fi**: Configure the VPN connection information to be used by both networks. To use different tunnels for configurations for cellular and Wi-Fi, click the **Cellular** and **Wi-Fi** tabs and enter the VPN connection information.
   - If a profile has more than two VPN settings with **VPN auto connection** checked, the profile will not be installed on the device.
2. Enter the information below:

Item	Description
Server address	Enter the IP address, host name, or URL of the VPN server.
Local identifier	Enter the value to identify the IKEv2 client in the format below: • FQDN, UserFQDN, Address, and ASN1DN
Remote identifier	Enter the value in the format below: • FQDN, UserFQDN, Address, and ASN1DN
System authentication	Select a VPN authentication method: • **Security sharing**: Enter the security sharing password. • **Certificate**: Select a user certificate input method. Then enter the common name of the server certificate issuer and the common name of the server certificate.
EAP activation	Determines if EAP is activated. If activated, select • **Certificate**: Select a user certificate input method. • **Password**: Enter the user ID and Password.

Item	Description
Dead Peer Detection speed	Set the interval for checking the usability of the VPN equipment. **NOTE** Check whether the resource should change or the content should be modified.
Encryption algorithm	Choose the Encryption algorithm. • **IKE SA**: DES, 3DES, AES-128, AES-256, AES-128-GCM, AES- 256 GCM • **Sub SA**: DES, 3DES, AES-128, AES-256, AES-128-GCM, AES-256-GCM
Integrity algorithm	Choose the Integrity algorithm. • **IKE SA**: SHA1-96, SHA1-160, SHA2-256, SHA2-384, SHA2-512 • **Sub SA**: SHA1-96, SHA1-160, SHA2-256, SHA2-384, SHA2-512
Diffie Hellman group	Select the group to be used for Diffie Hellman algorithm. • **IKE SA**: 0, 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21 • **Sub SA**: 0, 1, 2, 5, 14, 15, 16, 17, 18, 19, 20, 21
Time(min)	Enter the session expiration period. • **IKE SA**: Between 10 and 14440. The default value is 14440. • **Sub SA**: Between 10 and 14440. The default value is 14440.
Enable NAT keepalive while the device is in sleep mode	Enable NAT Keepalive and set the interval for Keepalive. **NOTE** This item is for iOS 9 or higher.
NAT keepalive interval	Set NAT KeepAlive intervals in seconds. The default value is 20 seconds. **NOTE** This item is for iOS 9 or higher.
Use IPv4/IPv6 internal subnet properties	Select to use the IPv4/IPv6 internal subnet attribute of IKEv2. **NOTE** This item is for iOS 9 or higher.
Disable portability and multi-homing	Select to deactivate portability and multi-homing (MOBIKE). **NOTE** This item is for iOS 9 or higher.
Disable redirect	Select to disable IKEv2 connection redirection. **NOTE** This item is for iOS 9 or higher.
Enable a perfect forward secrecy	Select to enable PFS (Perfect Forward Secrecy) **NOTE** This item is for iOS 9 or higher.

Item	Description
Voice mail box / AirPrint	Select the allowed traffic range when using Voicemails and AirPrint. • Allow traffic to goes through tunnel/Allow traffic outside tunnel/Drop traffic
Captive web sheet traffic outside of VPN tunnel	Allows captive web sheet traffic outside the VPN tunnel.
Captive Network App bundle identifier	Enter the Captive Network App bundle identifier to allow and click + to disallow this item.

Certificate (iOS)

You can add more certificate policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each certificate setting.
Description	Enter a description for each certificate setting.
Certificate category	Select a certification category. • **CA Certificate**: Select a certificate to use from the CA certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **CA Cert** and the Type set as **Root** will appear on the list. • **User certificate**: Select a certificate to use from the User Certificate list. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **CA Cert** and the Type set as User will appear on the list.

SSO (iOS)

SSO (Single Sign On) service offers one-click access to all of the applications without additional authentication. You can add more SSO policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each SSO setting.
Description	Enter a description for each SSO setting.
Account Name	Enter the name that appears on the device.
Principal Name	Enter the principal name.
Realm	Enter a domain name that is able to use SSO. You must enter the name in upper case letters.

Policy	Description
URL Prefixes	Enter a URL to be accessed with SSO. Click ⌄, enter a URL, and then click +.
App Identifier	Enter the bundle ID of an application that you can use through SSO. If there is no application added on the list, SSO can be used for all applications. Click ⌄, enter the bundle ID of an application, and then click +.

Cellular (iOS)

Configure the cellular network settings and control how the device accesses the cellular network. If an APN has already been set, the cellular configuration will not be applied. You can add more cellular policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each cellular setting.
Description	Enter a description for each cellular setting.
AttachAPN	Configure the settings for an Attach APN. • **Name**: Enter the name for the setting. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. • **Authentication Method**: Choose PAP or CHAP. • **Username**: Enter the user name for user authentication. • **Password**: Enter the password for user authentication.
APNs	Configure the setting for an APN. • **Name**: Enter the name for the setting. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered. • **Authentication Method**: Choose PAP or CHAP. • **Username**: Enter the user name for user authentication. • **Password**: Enter the password for user authentication. • **Proxy Server**: Enter the IP address of a proxy server. • **Proxy Server Port**: Enter the port number of a proxy server.

AirPrint (iOS)

You can add a printer to the AirPrint list on the device and configure devices and printers that exist on different networks conveniently. You can add more AirPrint policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each setting.
Description	Enter a description for each setting.
AirPrint Printer List	Add printers that support AirPrint. Click , enter an IP address and a resource path, and then click . For the resource path, you can enter what's below: • printers/Canon_MG5300_series • printers/Xerox_Phaser_7600 • ipp/print • Epson_IPP_Printer

Font (iOS)

You can add more font policy sets by clicking .

Policy	Description
Configuration ID	Assign a unique ID for each font setting.
Description	Enter a description for each font setting.
Font	Add a font to use on the device. Click **Add** and add a font.

WebClip (iOS)

You can add more WebClip policy sets by clicking .

Policy	Description
Configuration ID	Assign a unique ID for each web clip setting.
Description	Enter a description for each web clip setting.
Label	Enter a web clip name to be displayed on the device home screen.
URL	Enter a web clip URL address.
Removable	Check the checkbox to allow users to delete the web clip account settings.
Icon	Click **Add**, and then click **Browse** to select an icon that will be displayed on the user's device home screen. Then click **OK** to add. • The icon must be 59 x 60 px and in the PNG file format. • A white square image will be displayed if no icon is selected.

App Lock (iOS)

You can add more App Lock policy sets by clicking ⊕.

Policy	Description
Configuration ID	Assign a unique ID for each application lock setting.
Description	Enter a description for each application lock setting.
App Bundle ID	Enter the application bundle ID to identify applications.
Options	Check the box to configure the application lock options.
> Touch Screen	Allows device touchscreen mode.
> Screen Rotation	Enables using the landscape or portrait mode of the device screen.
> Volume Button	Enables adjusting the volume.
> Ringer Switch	Enables the easy on and off ringer mode through a ringer switch.
> Power Button	Allows turning the device on or off through the power button.
> Auto Lock	Enables automatically locking the device after a fixed amount of time through auto lock.
> VoiceOver	Turn on voice over for a screen-reading feature.
> Zoom In/Out	Turn on the zoom feature to configure easy zooming on the screen display.
> Invert Colors	Turn on color inversion to show colors on the device screen as their complementary colors.
> Assistive Touch	Allows virtual home button to perform multiple actions on the screen with a simple tab.
> Speak Selection	Turn on say optional item to select a text to be read aloud.
> Mono Audio	Turn on Mono Audio to play both audio channels in one ear using a headset.
User Enabled Options	Check the box to configure user enabled options.
> VoiceOver	Enables Voice over for the screen-reading feature.
> Zoom In/Out	Allows for configuring the easy zoom in and out feature on the display.
> Invert Colors	Allows color inversion to display colors on the device screen as their complementary colors.
> Assistive Touch	Allows virtual home button to perform multiple actions on the screen with a simple tab.

Global HTTP Proxy (iOS)

You can add more global HTTP policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each global HTTP proxy setting.
Description	Enter a description for each global HTTP proxy setting.
Proxy Type	Select and enter the corresponding items depending on the proxy type.
> Manual	• **Proxy Server and Port**: Enter the IP address of a proxy server and the port number of the proxy server. • **Username**: Enter the username for user authentication • **Password**: Enter the password for user authentication.
> Auto	• **Proxy PAC URL**: Enter the URL of the PAC file that defines the proxy configuration. • **Proxy PAC Fallback Allowed (iOS 7 or above)**: Check the checkbox to allow a direct connection from the user device if the PAC connection fails.
Proxy Captive Login Allowed (iOS 7 or above)	Check the checkbox to allow the device to bypass the proxy server to display the login page for captive networks.

AirPlay (iOS)

These policies support devices with iOS 7 or above. You can add more AirPlay policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each AirPlay setting.
Description	Enter a description for each AirPlay setting.
Whitelist (Supervised)	Add an AirPlay device ID to the whitelist so that it is displayed on the user's device. Click ⌄, enter a device ID, and then click +.
Passwords	Add an AirPlay device password. Click ⌄, enter a device name and password, and then click +.

Web Content Filter (iOS)

You can add a specific URL to the whitelist or blacklist. These policies support devices with iOS 7 or higher in Supervised mode. You can add more web content filter policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each setting.
Description	Enter a description for each setting.
Auto Filter Enabled	Check the checkbox to use the auto filter function.
Blacklisted URLs	Add a URL to allow access to. Click ⌄, enter a URL, and then click +.
Permitted URLs	Add a URL to block access to. Click ⌄, enter a URL, and then click +.
Whitelisted Bookmarks	Add a bookmark to allow for access. Click ⌄, enter a URL, title, and path, and then click +.

Managed domains (iOS)

Set managed domains and protect corporate data. You can control what apps can open documents downloaded from corporate domains using Safari. These policies support the devices with iOS 8 or higher in Supervised mode. You can add more managed domains policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each setting.
Description	Enter a description for each setting.
Email domains	Add a domain to specify as a corporate domain for emails. Click ⌄, enter a URL, and then click +.
Web domains	Add a domain to specify a corporate domain for the web. Click ⌄, enter a URL, and then click +.

Network Usage Rules (iOS)

Configure network usage rules to allow data roaming and cellular data for applications. You can add more network usage rules policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each setting.

Policy	Description
Description	Enter a description for each setting.
Managed app Network Settings	Add an application and allow cellular data and data roaming. Click ⌄, add an application, set the data settings, and then click +.

Configuring Windows Policies

Create a profile and register policies for Windows devices.

You can configure the policies below for Windows devices. The availability of each policy varies depending on the OS version.

→ System (Windows)
Allows the use of features such as factory reset, camera, screen capture and VPN.

→ Interface (Windows)
Controls the network settings, such as Bluetooth, Wi-Fi tethering, and NFC.

→ Security (Windows)
Configures the password settings.

→ Application (Windows)
Allows using the Windows App Store and configuring options for application controls, such as installation and blacklist/whitelist.

→ Phone (Windows)
Allows overseas data roaming.

→ Etc (Windows)
Allows deleting PPKG (Provisioning Package) files or MDM profiles while using them.

→ Wi-Fi (Windows)
Configures the Wi-Fi settings, such as SSID, security type, and proxy.

→ Exchange (Windows)
Configures the Microsoft Exchange ActiveSync account to synchronize email, calendar, contacts, and tasks from the Exchange account.

→ VPN (Windows)
Configures VPNs (Virtual Private Network) on Windows devices.

→ Certificate (Windows)
Configures the EMM Agent Root, user certificates, and server certificates for use on the device.

System (Windows)

Policy	Description	Supported devices
Factory reset	Allows a device factory reset.	Windows 10 (Mobile / Desktop) or higher
Camera	Allows using the camera.	Windows 10 (Mobile / Desktop) or higher
Screen Capture	Allows using the screen capture function.	Windows 10 (Mobile) or higher
VPN	Allows modifying the VPN settings.	Windows 10 (Mobile) or higher

Interface (Windows)

Policy	Description	Supported devices
Wi-Fi	Allows the use of Wi-Fi.	Windows 10 (Mobile / Desktop) or higher
> Wi-Fi Tethering	Allows tethering the Wi-Fi connection.	Windows 10 (Mobile / Desktop) or higher
Bluetooth	Allows the use of Bluetooth.	Windows 10 (Mobile / Desktop) or higher
> Search Mode	Allows using device search via Bluetooth.	Windows 10 (Mobile / Desktop) or higher
NFC	Allows the use of NFC (Near Field Communication).	Windows 10 (Mobile) or higher
USB	Allows USB tethering connections.	Windows 10 (Mobile) or higher

Security (Windows)

Policy	Description	Supported devices
Password policies	Set to apply the password policy when the screen is locked. The camera is disabled in screen lock mode. **NOTE** If you have enabled Samsung SDS EMM for a device with no password, certificates registered in the device will be deleted.	Windows 10 (Mobile) or higher
> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts. The value can be between 3 - 998 times. **NOTE** If you enter the wrong password more than the allowed number of times, a challenge phrase appears, and then the system begins the factory reset operation. A challenge phrase is a particular phrase that is presented to you to disable the autofill feature and protect your information. You need to enter the case sensitive challenge phrase exactly.	Windows 10 (Mobile) or higher
> Minimum length	Set the minimum length of the password. The value can be between 4 - 16 words.	Windows 10 (Mobile) or higher
> Maximum Screen lock grace period (Minutes)	Set an idle time before the screen lock is enabled. The value can be between 0 – 999 minutes.	Windows 10 (Mobile) or higher
> Expiration after (days)	Set the maximum number of days before the password must be reset. The value can be between 0 - 730 days. **NOTE** Set the number to 0 for an indefinite period.	Windows 10 (Mobile) or higher
> Retain history for	Set the number of times that you can reuse the password that you previously used, including the current password. The value can be between 2 - 50 times.	Windows 10 (Mobile) or higher

Application (Windows)

NOTE To set the CSP for an application's black/white lists settings, see Setting CSP.

Policy	Description	Supported devices
Windows App store access control	Allows access to the Windows App Store.	Windows 10 (Mobile) or higher
Add App Install Black/Whitelist	Set the Windows application policies based on the blacklist or the whitelist.	Windows 10 (Mobile/Desktop) or higher
> Add Preloaded App Automatically	Set to automatically add preloaded applications. **NOTE** This policy available only when **Application whitelist settings** is selected.	Windows 10 (Mobile/Desktop) or higher
> App Install/Run Whitelist	Add applications to allow their installation. Any applications not on the whitelist are deleted, even if previously installed. • To add an application, click **Add**, and then select applications in the "Select Application" window. • To delete an application, click 🗑 next to the added application. **NOTE** The EMM Agent is automatically registered on the list.	Windows 10 (Mobile/Desktop) or higher
> App Install/Run Blacklist	Add applications to prohibit their installation. Blacklisted applications will be deleted even if they were previously installed. • To add an application, click **Add**, and then select applications in the "Select Application" window. • To delete an application, click 🗑 next to the added application. **NOTE** An application that has been added on the **App Install/Run Whitelist** cannot be added.	Windows 10 (Mobile/Desktop) or higher

Phone (Windows)

Policy	Description	Supported devices
Data connection during roaming	Allows overseas data roaming	Windows 10 (Mobile/Desktop) or higher

Etc (Windows)

Policy	Description	Supported devices
Delete PPKG	Allows users to delete provisioning package (PPKG) files while using them.	Windows 10 (Mobile/Desktop) or higher
MDM Client Unenrollment	Allows users to delete MDM profiles while using them.	Windows 10 (Mobile/Desktop) or higher

Wi-Fi (Windows)

You can add more Wi-Fi policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each Wi-Fi setting.
Description	Enter a description for each Wi-Fi setting.
Network Name (SSID)	Enter the identifier of a wireless router to connect to. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Security type	Specifies the access protocol used.
> Open	Allows a Wi-Fi connection without a password.
> WEP	Set a password in the **Password** field.
> WPA2 Personal	Set a password in the **Password** field.
> EAP	Enter an EAP XML configuration code. **NOTE** The EAP XML tab is enabled only when EAP is selected for the Security type.
Auto connection	Check to use an automatic Wi-Fi connection.
Hide Network	Check the checkbox to hide the network from the list of available networks on the device. The SSID does not broadcast.
Proxy Server and Port	Enter the IP address of a proxy server and the port number of the proxy server.

Exchange (Windows)

You can add more Exchange policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each Exchange setting.
Description	Enter a description for each Exchange setting.
User information input method	Select an input method for entering user information.
> Manual Input	Select to manually enter the email address, account ID, and password of a user. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
> Connector interworking	Select to choose a connector from the User Information Connector list. **NOTE** All the connectors are listed in **System** > **Connector** > **Directory**. The email account that is registered is the one registered in the connected directory's information.
> User Information	Select to access the exchange server using the registered EMM email and ID. The password must be entered from the user's device.
Domain	Enter a domain address for the Exchange server. You can also click **Lookup** to open the reference items list and select an item from it. The reference value will be automatically entered.
Server Name	Assign an Exchange server name.
Diagnostic Logging	Select a configuration level for diagnostic logging. • **Logging off**: Does not leave a record in the Event Viewer log. • **Basic logging**: Configure the default diagnostic log information. • **Advanced logging**: Configure the diagnostic log information for the security-related events.
Sync Schedule	Select the interval period to sync the incoming emails.
Sync measure for the early data	Select the interval period to sync the past emails.
Sync calendar	Syncs schedules on a calendar from a server to a device.
Sync contacts	Syncs contact information in a phone book from an Exchange to a device.
Sync Email	Syncs emails from an Exchange to a device.
Sync task	Syncs tasks from an Exchange to a device.
SSL	Set to use SSL for email encryption.

VPN (Windows)

You can add more VPN policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for the VPN setting.
Description	Enter a description for the VPN setting.
VPN vendor name	Select a VPN vendor from among **Pulse Secure VPN**, **F5**, **SonicWall Mobile Connect**, and **Check Point Mobile**.
Server address	Enter the IP address, host name, or URL of the VPN server that the device needs to access.
Customer Configuration	Enter the VPN vendor-specific settings in the XML format and click **Save**.
Remember Credentials	Check to use remember credentials.
Always On	Check to use always on mode.
Lock Down	Check to use lock down mode.
DNS Suffix	Enter a DNS Suffix.
Trusted Network	Enter the IP address, host name, or URL.
Proxy Settings	Select the setting for the proxy server. • **Manual**: Enter the IP address of the proxy server. • **Auto**: Enter the Auto Config URL.

Certificate (Windows)

You can add more certificate policy sets by clicking +.

Policy	Description
Configuration ID	Assign a unique ID for each certificate setting.
Description	Enter a description for each certificate setting.
Certificate category	Select a certification category. • **Root**: Select a certificate to use. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Purpose set as **CA Cert** and Type set as **Root** will appear on the list. • **User**: Select a certificate to use. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Type set as **User** will appear on the list. • **Server**: Select a certificate to use. Among the certificates registered in **Advanced** > **Certificate** > **External Certificate**, those with the Type set as **Server** will appear on the list.

Configuring Tizen Wearable Policies

Create a profile and register policies for Tizen Wearable devices.

You can configure the policies below for Tizen Wearable devices. The availability of each policy varies depending on the OS version.

→ System (Tizen Wearable)
Configures various settings, such as the system settings, firmware recovery, factory reset, Airplane mode, power saving mode, Power off, screen capture, and firmware update.

→ Interface (Tizen Wearable)
Allows adding a new Wi-Fi network or using Bluetooth, NFC, GPS, and other features.

→ Security (Tizen Wearable)
Configures the password settings.

→ Application (Tizen Wearable)
Configures options for application controls such as installation, blacklist/whitelist, and execution prevention.

→ Phone (Tizen Wearable)
Configures the cellular data connection.

→ Logging (Tizen Wearable)
Allows performing logging and configuring the settings.

System (Tizen Wearable)

Policy	Description	Supported devices
Factory reset	Allows a device factory reset from the System Configuration menu on the device.	Samsung Knox 1.0 higher
Settings	Allows the configuration of the System Settings.	Samsung Knox 1.0 higher
Firmware download mode control	Allows using the hardware key on the device to update firmware. • **Disallow**: Disallows updating firmware with the hardware key and performing a factory reset.	Samsung Knox 1.0 higher
Airplane mode	Allows the use of airplane mode.	Samsung Knox 2.2 higher
> Change to Airplane mode	Allows changing to airplane mode.	Samsung Knox 2.2 higher
Control power saving mode	Allows controlling the power saving mode on the device.	Samsung Knox 2.2 higher

Policy	Description	Supported devices
Power off	Allows powering off the device. **NOTE** • If this policy is disallowed, the user cannot turn off the device and cannot perform a factory reset. • The device command from an administrator for factory reset is also blocked.	Samsung Knox 2.2 higher
Screen capture	Allows using the screen capture function.	Samsung Knox 1.0 higher
Firmware update	Allows updating the firmware. This policy is used to allow the user to manually update the firmware from their wearable device's firmware update menu, or from the paired parent device, or disallow such actions.	Samsung Knox 2.2 higher

Interface (Tizen Wearable)

Policy	Description	Supported devices
Wi-Fi	Allows using a Wi-Fi network. If the Wi-Fi policy is not applied successfully, the device tries again to apply the Wi-Fi 30 minutes later after EMM is activated.	Samsung Knox 1.0 higher
Bluetooth	Allows using Bluetooth.	Samsung Knox 1.0 higher
NFC control	Allows using NFC control.	Samsung Knox 1.0 higher
GPS	Allows using the GPS function. **NOTE** Before applying this policy, Tizen Wearable devices are already applied with one of the three GPS modes: high accuracy/sleep/GPS only.	Samsung Knox 1.0 higher
USB debugging	Allows for a connection between a Tizen Wearable device and a PC for debugging.	Samsung Knox 1.0 higher
Wi-Fi SSID whitelist setting	Allows using the Wi-Fi SSID Whitelist. Devices can only connect to the Wi-Fi APs on the whitelist.	Samsung Knox 1.0 higher

Policy	Description	Supported devices
> Wi-Fi SSID whitelist	Add Wi-Fi APs to the whitelist. This policy is irrelevant to adding or deleting the Wi-Fi setting profile. • To add a Wi-Fi AP, enter a Wi-Fi SSID and click **Add**. • To add all Wi-Fi APs, click **Add all** to access the Wi-Fi list. • To delete a Wi-Fi AP, select a Wi-Fi SSID and click 🗑.	Samsung Knox 1.0 higher
Wi-Fi SSID blacklist setting	Allows using the Wi-Fi SSID blacklist. Devices cannot connect to Wi-Fi APs on the blacklist.	Samsung Knox 1.0 higher
> Wi-Fi SSID blacklist	Add Wi-Fi APs to the blacklist. This policy is irrelevant to adding or deleting the Wi-Fi setting profile. • To add a Wi-Fi AP, enter a Wi-Fi SSID and click **Add**. • To add all Wi-Fi APs, click **Add all** to access the Wi-Fi list. • To delete a Wi-Fi AP, select a Wi-Fi SSID and click 🗑.	Samsung Knox 1.0 higher

Security (Tizen Wearable)

Policy	Description	Supported devices
Password policies	Set to apply the password policy when the screen is locked. The camera cannot be used when the screen is locked. **NOTE** If you install the Samsung SDS EMM application on a device that has no set password, the certificate registered to the device will be deleted.	
> Minimum strength	Set the Password strength on the screen: • **None**: Set the password with a four digit number. • **Numeric**: Set the password using numbers • **Must be alphanumeric**: Set the password using both letters and numbers.	Samsung Knox 1.0 higher
> Maximum Failed Login Attempts	Set the maximum number of incorrect password attempts before resetting the device to its factory settings. The value can be between 0 - 10 times.	Samsung Knox 1.0 higher

Policy	Description	Supported devices
> Minimum Length	Set the minimum length of the password. The value can be between 4 - 16 characters for **Numeric** or **Must be alphanumeric**. **NOTE** If the minimum strength is set to pattern, the minimum length policy will not be applied.	Samsung Knox 1.0 higher

Application (Tizen Wearable)

Policy	Description	Supported devices
Application black/ whitelist	Set to control the application installation policies. • **Application blacklist settings**: The Blacklist is the list of applications that should not be installed or run on user devices. You can specify the **Application installation blacklist** and the **Application execution blacklist**. • **Application whitelist settings**: The Whitelist is the list of applications that could be installed or run on the user devices. You can specify the **Application installation whitelist,** the **Application execution blacklist** and the **Applications that cannot be uninstalled**. • **Application black/whitelist settings**: You can apply both a blacklist and whitelist policy at the same time. If an application is registered both on the black and whitelist, the whitelist has priority.	Samsung Knox 1.0 higher

Policy	Description	Supported devices
> Application installation blacklist	Add applications to prohibit their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Blacklisted applications cannot be installed and will be deleted even if they were previously installed. • An application that has been added to the Application installation whitelist cannot be added.	Samsung Knox 1.0 higher
> Application installation whitelist	Add applications to allow their installation. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To add all applications, click **Add all**. • To delete an application, click 🗑 next to the added application. **NOTE** • If a control application registered with a wildcard (*) in the package name is added to this policy, the specific package will not be installed. e.g.) com.*.emm / com.sds.* / com.*.emm.* • Any applications not on the whitelist are deleted, even if they are not on the blacklist. • An application that has been added on the **Application installation blacklist** cannot be added. • Samsung Knox 2.0 or higher is supported on Knox Workspace devices.	Samsung Knox 1.0 higher

Policy	Description	Supported devices
> Application execution blacklist	Add applications to prevent their execution. The icon of the blacklisted application disappears and users cannot run the application. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** An application that has been added on the **Application installation whitelist** cannot be added.	Samsung Knox 1.0 higher
> Application execution whitelist	Add applications to allow their execution. Icons of applications that are not on the whitelist disappear automatically. EMM and the preloaded applications are automatically registered on the whitelist. • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application. **NOTE** An application that has been added on the **Application installation blacklist** cannot be added.	Samsung Knox 1.0 higher
> Applications that cannot be uninstalled	Add applications that should not be removed to the user devices. An application that has already been added on the Application Blacklist or Application installation blacklist cannot be added on the Application removal blacklist: • To add an application, click **Add**, and then select applications in the “Select Application” window. • To delete an application, click next to the added application.	Samsung Knox 1.0 higher

Phone (Tizen Wearable)

Policy	Description	Supported devices
Cellular data connection	Allows the use of a cellular data connection. **NOTE** This policy is applied after internal applications that have been set as **Automatic (Non-removable)** are installed. If the cellular data connection policy is not applied successfully, the device tries to apply this policy again 30 minutes later after EMM is activated.	Samsung Knox 1.0 higher

Logging (Tizen Wearable)

Policy	Description	Supported devices
Save logs	Set to enable the save logs feature. • **Enable**: Set to perform logging. This is the default value. • **Disable**: Cannot record device logs. **NOTE** If this policy is not specified, the EMM performs logging with the **DEBUG** level.	Samsung Knox 1.0 higher
> Log level	Select a log level. • **DEBUG**: Logs detailed device information for the developers. • **INFO**: Logs device information for the administrators. • **WARNING**: Logs information that are not errors, but the ones that require special attention for the administrators. • **ERROR**: Logs error information.	Samsung Knox 1.0 higher
Maximum log size (MB)	Enter value for the maximum log size. The value can be between 1 – 20 MB.	Samsung Knox 1.0 higher
> Maximum days for storage (day)	Enter value for the maximum days for log storage. The value can be between 1 – 30 day.	Samsung Knox 1.0 higher

Applying configurations automatically (Android only)

If you configured device settings for a profile, such as Wi-Fi, APN, VPN, Exchange, Email, and Certification, then the settings can be applied automatically on the device without user action. If two or more values have been configured for the same category on a device, then the user must select a category and apply the settings manually, except for Wi-Fi settings. However, the bookmark settings cannot be applied automatically if the Installation area field is set to Shortcut. The EMM Agent on the user device must be v2.5.5, and the Admin Server must be EMM v2.5.5 to set automatic installation as Use for profile certificates and auto-install more than two certificates.

Refer to the following table for an example:

Category	Value	Application type
Wi-Fi	A	Auto application
	B	
VPN	C	
Exchange	D	Manual application
	F	

Device settings can be applied automatically once EMM is activated and the policies are applied. After the application is complete, you can see the results in a notification message.

Preparations

To apply configurations automatically, do the following:

- When using certificates and VPN settings in the Wi-Fi 802.1xEAP framework, install Credential Storage (CS) so that trusted certificates can be stored in advance. CS installation means locking the screen using an option more secure than a password.
- For the Knox VPN setting, install the Vendor Client in advance.
- For the Email and Exchange settings, install the Samsung Email application and agree to receive notifications from the Email application (Samsung S8 or higher).
- For the Knox workspace, install the VPN Vendor Client in the general area.

Restrictions

In the following cases, manual intervention is still required even configurations are applied automatically.

- The device cannot automatically connect to the Wi-Fi AP, so the user should select a Wi-Fi AP to connect to in the device settings. However, if you set **Automatic Connection** for the **Wi-Fi** setting in the Android Enterprise profile, the device will automatically connect to the Wi-Fi AP.
- To connect a tunnel after installing a VPN or Knox VPN, it must be enabled manually.
- If the user deletes the auto-applied configuration, the deleted configuration is automatically reapplied when the device is manually rebooted or restarted.

Categories of auto application

Configurations applied automatically can be categorized into Cases A, B, and C:

Category	Description	Application order
Case A	Settings that can be applied and updated immediately after EMM is activated and policies are applied. • Application and updates can be performed automatically in the Knox Workspace area once it is created and policies are applied. • The Email and Exchange settings require installation of the Samsung Email application. • For Wi-Fi 802.1xEAP, select PEAP in the EAP Methods, which is an authentication protocol, to prevent the usage of certificates. The user does not need to select a screen lock type and add it when auto-installing Wi-Fi settings, because this doesn't require installation of Credential Storage (CS). • Auto application of the Bookmark settings is supported on devices running Android 6.0 (Marshmallow) or Android 7.0 (Nougat), and only when the Installation area field is set to Bookmark. However, the Bookmark settings cannot be applied automatically on Android Enterprise devices.	APN > Bookmark > Wi-Fi > Exchange > Email

Category	Description	Application order
Case B	Settings that can be applied or updated once a screen lock password is set and additional applications or certifications are installed. • If no screen lock password has been set, configurations will not be applied automatically and a notification message for setting the screen lock password will appear instead. Tap **Set password** on the notification message to open the settings screen of the device.	Wi-Fi > VPN > Knox VPN
Case C	Settings that must be applied manually by the user from EMM.	

NOTE If you set up Exchange with a certificate, it will be categorized as Case B because it requires certificate installation.

For more information, see the table below:

The settings categories with the asterisks(*) are not supported on devices with Android 13 or higher.

Settings category	Android enrollment type	General/ Knox Workspace	Type	CS installation required	Additional application installation required	Automation category
Wi-Fi	Fully managed/ Legacy*	G	None	X	X	Case A
			WEP	X	X	Case A
			WPA/WPA2-PSK	X	X	Case A
			802.1xEAP	X	X	Case A (When a certificate is not in use)
	Legacy*			O	X	Case B
Exchange ActiveSync	Legacy	G/K	N/A	X	O	Case A Case B (When a certificate is in use)
Email	Legacy	G/K	N/A	X	O	Case A
Certificate	Fully managed/ Legacy*	G	N/A	O	X	Case B
APN	Fully managed/ Legacy*	G	N/A	X	X	Case A

Settings category	Android enrollment type	General/ Knox Workspace	Type	CS installation required	Additional application installation required	Automation category
Bookmark	Fully managed	G	N/A	X	X	Case C
	Legacy	G/K	N/A	X	X	Case A
VPN	Legacy*	G	PPTP	O	X	Case B
		G	L2TP/IPSec PSK	O	X	Case B
		G	L2TP/IPSec RSA	O	X	Case B
		G	IPSec Xauth PSK	O	X	Case B
		G	IPSec Xauth RSA	O	X	Case B
		G	IPSec Hybrid RSA	O	X	Case B
Knox VPN*	Fully managed/ Fully managed with Work Profile/ Legacy*	G/K	Cisco	X	O	Case C
		G	Strongswan	O	O	Case C
	Legacy*	K	F5	X	O	Case B
		K	Juniper	X	O	Case B (When a certificate is not in use, auto application is not supported.)

Assigning and applying profiles

Assign a profile to a group or an organization. You must assign a profile before applying the policies that are configured for it.

When multiple profiles are assigned to the same group or organization and there is a conflict within the policies between the profiles, the latest assigned/applied profile has priority. Policies from multiple profiles will be applied if they do not conflict with each other. If a device belongs to a group and an organization at the same time, the policies of the profiles applied to the group have priority.

You have to apply a profile to a group or an organization after assigning it. You must apply a profile to devices so that the profile policies can take effect. Profiles can be applied immediately or at a specific time.

Assigning to groups

To assign a profile to a group, complete the following steps:

1. Navigate to **Profile**.

   You can also assign a profile from the group list by navigating to **Groups** and selecting a group to assign. For more information, see Assigning and applying profiles to groups.

2. On the “Profile” page, click the checkbox for a profile to be assigned.

3. Click **Assign**.

4. On the “Assign Profile” page, click **Group**.

5. Click the checkboxes for groups to be assigned with the selected profile.

   - You can select multiple groups.
   - If a group has already been assigned a profile and it is assigned to another profile, you can preview the conflicting policies from the two profiles by clicking **Preview Policy**.

6. Click **Assign & Apply** to assign and apply the profile to the selected groups at the same time.

   - Click **Assign** to assign the profile to the selected groups and not to apply the profile now.

7. In the “Assign Profile” window, click **OK**.

Assigning to organizations

To assign a profile to an organization, complete the following steps:

1. Navigate to **Profile**.

   You can also assign a profile from the organization list by navigating to **Organization** and selecting an organization to assign. For more information, see Assigning applications to organizations.

2. On the “Profile” page, click the checkbox for a profile to be assigned.

3. Click **Assign**.

4. On the “Assign Profile” page, click **Organization**.

5. Click the checkboxes for organizations to be assigned with the selected profile.

   - You can select multiple organizations.
   - If an organization has already been assigned a profile and it is assigned to another profile, you can preview the conflicting policies from the two profiles by clicking **Preview Policy**.
   - When a profile is assigned to an organization that has sub-organizations, the profile will be applied to all the sub-organizations.
   - If a sub-organization has not been assigned a profile, the profile of the super organization will be inherited, but the inherited profile can be overwritten with a new profile.
   - If a sub-organization has been assigned its own profile, then the profile of the super-organization will not be inherited.

6. Click **Assign & Apply** to assign and apply the profile to the selected organizations at the same time.

   - Click **Assign** to assign the profile to the selected organizations and not apply the profile now.

7. In the “Assign Profile” window, click **OK**.

NOTE Sub-administrators who only have the Profile Managing Permission cannot assign or apply profiles to organizations. In order for sub-administrators to be able to assign or apply profiles to organizations, they need to be given both the Org and Profile Managing Permissions. For more information, see Adding an organization.

Managing profiles on the list

Manage profiles from the profiles list. You can manage applications by package name or set up profile priorities.

Managing applications for specific purposes

You can add applications by package name to control them in a blacklist or whitelist.
When you click **Export to CSV**, you can download a list of control applications as an Excel file.

To add applications, complete the following steps:

1. Navigate to **Profile**.
2. Click **Manage Control App**.
3. In the “Manage Control App” window, click **Add**.
4. In the “Add Control App” window, enter the following information. Available items vary depending on the platform.
   - **Platform**: Select a platform.
   - **Package Name**: Enter the application package name.
   - **Bundle ID**: The retrieved bundle ID for the application is displayed.
   - **Bundle Name**: The retrieved bundle name is displayed. If there is no value, “-“ is displayed.
   - **Publisher**: Enter the application publisher.
   - **Application Name**: Enter the application name.
   - **Preload App**: Select whether to set the application as a preloaded application.
5. Click **Save**.

To bulk add multiple control applications, complete the following steps:

1. Navigate to **Profile**.
2. Click **Manage Control App**.
3. In the “Manage Control App” pop-up window, click **Bulk Add**.
4. In the “Bulk Add Control Apps” pop-up window, select a platform and download the template.
5. You can check the results of adding applications in the “Bulk Add Result” pop-up window.

To modify applications, complete the following steps:

1. Navigate to **Profile**.
1. Click **Manage Control App**.
2. In the “Manage Control App” window, select an application name to modify, and then click **Modify**.
3. In the “Modify Control App” window, modify the information.
4. Click **Save**.

To delete applications, complete the following steps:

1. Navigate to **Profile**.
2. Click **Manage Control App**.
3. In the “Manage Control App” window, select an application name to delete, and then click **Delete**.
4. In the “Delete Application” window, click **Save**.

Setting up the profile priorities

Set up the profile priorities for when multiple profiles are being applied to the same group or organization.

To set up priorities, complete the following steps:

1. Navigate to **Profile.**
2. On the “Profile” page, click **Manage Priority**.
3. In the “Manage Priority” window, click a profile to change the priority order.
4. Click ↑ or ↓ to change the priority order of the selected profile.
5. Click **Save & Apply** to save the changes and apply the changed profile to the devices.
   - Click **Save** to save the changes and not apply the profile now.
   - Click **Preview** to view the groups or organizations affected by the changed profile.
6. In the “Save Priority” or “Save Priority & Apply” window, click **OK**.

NOTE

Only one container, either Knox Workspace or Dual DAR Workspace, can be created in a device. Note that changing the profile priority deletes the container already on the device and creates a new one.

For example, if you deploy a high-priority Dual DAR profile to a device with Knox Workspace, a new Dual DAR Workspace will be created after deleting the previously created Knox Workspace. At the same time, all applications and data in Knox Workspace will be deleted.

Modifying profiles in detail

Modify the policies in a profile currently being applied to devices. You can also modify other information, such as conditions that are set for certain profiles.

NOTE Sub-administrators who only have the profile managing permission can only modify profiles that they have created or ones already assigned to them. If you are a super administrator and wish to assign profiles to sub-administrators, then see Adding an organization for more information.

To modify the profile information, complete the following steps:

1. Navigate to **Profile**.
2. On the “Profile” page, click the name of a profile to modify.
3. On the “Profile Detail” page, click **Modify Profile Info**.
4. On the “Modify Profile” page, modify the existing information if necessary.
5. Click **Save & Set Policy** to save the information and to proceed with configuring the profile in detail.
   - Click **Save** to save the information and return to the profile list.
6. Configure the profile details. For more information, see Configuring policies by device platform.

To modify the profile policies, complete the following steps:

1. Navigate to **Profile.**
2. On the “Profile” page, click the name of a profile to modify.
3. On the “Profile Detail” page, click **Modify Policy**.
4. On the “Set Policy” page, configure the policies. For more information, see Configuring policies by device platform.
5. Click **Save & Assign** to save the information and to proceed with assigning the policies to devices.
   - Click **Save** to only save the information.

NOTE If the policy is from migrated of existing components, the **component** letter is displayed at the top of the policy. Modifications to the setting of policy will affect other profiles that contain this setting as well.

Setting the profile update scheduler

You can set the schedule to update the latest policy applied to user devices and update the EMM Agent on a regular basis.

To set the policy update schedule, complete the following steps:

1. Navigate to **Setting** > **EMM Application and Policy** > **Profile Update Schedule**.
2. Click next to **Profile Update Schedule** to enable the scheduler feature.
3. Select a target type.
   - **Global Setting**: All profiles will be updated according to the schedule.
   - **Set by Group / Organization**: You can configure multiple schedules and select groups or organizations for each schedule setting.
4. Select days and set start time, and time zone.
   - Select groups or organizations for each schedule setting if you selected the group/organization target type.
   - The policy update time may vary depending on the time and time zone of the user device.
5. Click **Save**.

Exceptional profiles

You can create an exceptional profile with a policy that applies only to a specific user for a specific time period. Alternatively, you can select a Knox Portal application user to create a Knox Portal policy as an exceptional profile. You must apply a profile to devices so that the profile policies can take effect. Profiles can be applied immediately or at a specific time. You can assign exceptional profiles to only specific users for specific time periods. Users can be assigned multiple exceptional profiles, and the time period can be duplicated.

Creating an exceptional profile

An exceptional profile is a profile for applying exceptional policies for special purposes to users.

To add an exceptional profile, complete the following steps:

1. Navigate to **Advanced** > **Exceptional Profile**.
2. Click **Add**.
3. On the “Add Exceptional Profile” page, enter the following information:
   - **Name**: Enter a name for the profile. The entered name cannot be changed after saving.
   - **Exception Type**: Select the type of exceptional profile, either **Policy** or **Knox Portal App**. Create an exceptional policy for the policy set in the device profile, or create an exceptional policy for the policy of the Knox Portal application.
   - **Notification**: Sends a notification to the user when an exceptional profile starts or stops applying.
   - **Platform**: If you selected the exception type as **Policy**, click the checkbox to select the device platform.
     - If you want to set the policy using the Samsung Knox API in Android Enterprise devices, Samsung Knox should also be selected.
     - If you have selected the Android Enterprise platform, you can activate a device as a Fully Managed with Work Profile type by clicking the **Create Work Profile on Fully Managed** checkbox. Exceptional profiles do not support Dual DAR.

       NOTE
       - If you select to create Work Profile on Fully Managed, the Work Profile will be automatically created on devices with Android 8 or higher. If you do not select the option or the device runs Android 8 or higher, it will be activated as a Fully Managed type.
       - Fully Managed with Work Profile is not supported from Android 11, so devices with Android 11 or higher are activated as a Work Profile on company-owned type only.
       - You can set the Android Manage Type when adding users or organizations.

     - If you selected the Android Legacy platform, you can set the policy to apply to Knox Workspace by clicking the **Knox Workspace** checkbox. Exceptional profiles do not support Dual DAR.
   - **Description**: Enter a description for the exceptional profile.
4. Save the policy, click **Save & Set Policy** to save the information, and then set the detailed information of the exceptional profile.
   - Click **Save** to save the information and return to the exceptional profile list.
5. Set the detailed information of the exceptional profile.
   - For more information, see Configuring policies by device platform, and to set Knox Portal application policies, see Setting Knox Portal policies.

Assigning exceptional profiles

Assign exceptional profiles to a user. You can assign up to 10 exceptional profiles to a user when the exception type is policy, while Knox Portal exception type is allowed have only one exceptional profile.

To assign an exceptional profile to a user, complete the following steps:

1. Navigate to **Advanced** > **Exceptional Profile**.
2. On the “Exceptional Profile” page, click the checkbox for an exceptional profile to be assigned.
3. Click **Assign**.
4. On the “Assign Exceptional Profile.” page, click **Set Assignment**.
5. In the “Set Assignment” window, set the period to apply the exceptional profile and select users.
   - **Service Period**: Select a period to apply the exceptional profile. Service period can be overlapped.
     - To set the time for the service period, navigate to **Setting** > **Server** > **Configuration** and set **Exception Policy Scheduler**. The default value is 00:10.
   - **User ID**: Select users to assign the exceptional profile to. You can only assign to users with activated Android or iOS devices.
6. click **OK**.
7. Click **Assign & Apply** to assign and apply the exceptional profile to the selected users at the same time.
   - Click **Assign** to assign the profile to the selected users and not apply the profile now.
8. In the “Assign Profile” window, click **OK**.
   - When there are overlapped exceptional profiles with the same service period, the priority is decided by the order of assignment. To change the priority, see Changing priority of Exceptional Profile.

Collecting device location information

You can collect location data from devices on a regular basis.

The time in the collected location data is based on the device time. It may vary depending on the time and time zone of the device.

To set the location collection policy for Android Enterprise and Android Legacy devices, complete the following steps:

1. Navigate to **Profile**.
2. On the “Profile” page, click the name of the profile to configure the policy for.
3. On the “Profile Detail” page, click the “Policy” tab.
4. Click **Modify Policy** at the bottom of the page.
5. On the “Set Policy” page, navigate to the Location group of each device platform.
6. Set **Report device location** to **Allow**, **User consent**, or **Disallow**.
   - Location data is collected from the device only when you allow it.
   - When **User consent** is selected, the user should agree to permit data collection in the window on the device. This window appears only once after the device is enrolled or the profile is applied for the first time.
   - This policy holds a higher priority than the GPS policy and the Collect current location command. That is, when this policy is set to **Disallow**, either the device command is sent or location data is not collected, even if the GPS policy is set to **Allow** or **Disable on**.
7. Set the data collection interval and accuracy mode.
   - **Report device location interval**: Set the interval at which location data should be collected from the user’s device. For example, if you set the interval to 30 minutes, location data is collected from the device every 30 minutes after a profile is applied to the device.

     NOTE The Report device location policy will not be supported in versions released after EMM v2.5.0. To set the location collection interval for the devices with EMM v2.5.0 or higher installed, navigate to **Setting > Location Report Interval**. For more information, see Setting the interval to collect the device location.

   - **High Accuracy Mode**: Enable this mode to improve the accuracy of collected location data. When you enabled this mode, locations are detected using GPS and Wi-Fi and mobile networks. When you disable it, the locating method that the user has specified on the device is used instead.
     - For devices with Android 10 (Q) or higher, the user must agree to the notification on the status bar that asks for permission to use location data.

- When collecting location data by sending a device command, the locating method differs depending on whether the High Accuracy Mode is in use.

8. Click **Save**.

Setting the interval to collect the device location

You can set the server interval to periodically collect the device location data. The time of the collected location data is based on the device time. Setting to collect the location data is available in the Report device location policy. For more information, see Collecting device location information.

To set the location collection interval for Android Enterprise or Android Legacy devices, complete the following steps:

1. Navigate to **Setting > Location Report Interval**.
2. Click next to **Location Report Interval** to enable the location collection interval feature.
3. Select a target type.
   - **Global Setting**: The device location information will be updated according to the server interval.
   - **Set by Group/ Organization**: You can configure multiple collection intervals and select groups or organizations for each interval setting.
     - Click to add more device location collection interval settings.
4. Set the location collection interval for user devices.
   - **Report Interval**: Set the location collection interval for user devices. For example, if you set the interval to 30 minutes, location data is collected from the devices every 30 minutes after the location collection policy in the profile is applied to the devices.
   - **Group/ Organization**: Click **Select** and select user groups or organizations to apply the location collection interval.

     NOTE Even if you set the location collection interval, the device location information will not be collected when the **Report device location** policy is not set ('-' selected) or set to **Disallow**.

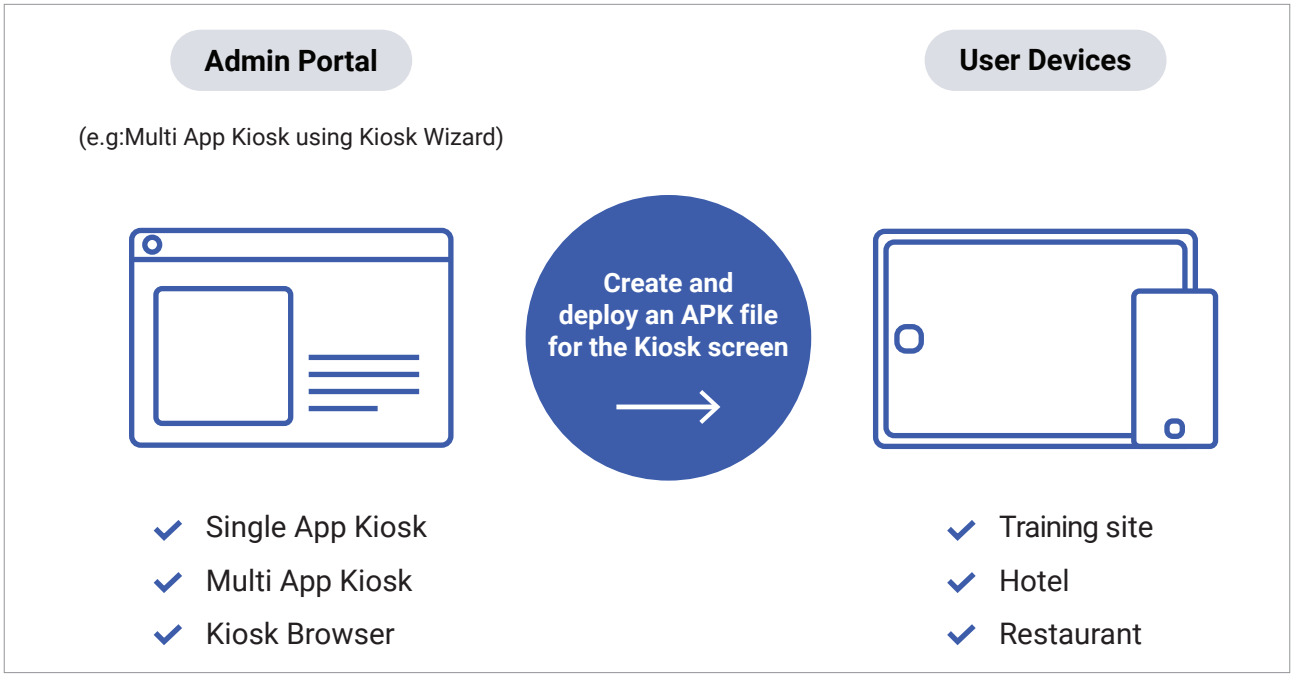
5. Click **Save**.

7

Kiosk

Kiosk

Kiosk is an application that is installed on a standalone device with a touch screen interface. With the EMM Kiosk feature, you can easily create Kiosks and configure the devices with applications, various widgets, and notifications. This allows you to utilize the Kiosk devices to fit your business and service needs for your company.



This chapter explains the following topics:

Introduction

The Kiosk runs only in Legacy (Android) or Android Enterprise devices. When Kiosk mode is applied, it is operated only in the configuration set by the IT admin on the home screen of the device. You can configure policies and applications to deploy on the device in Kiosk mode and they are applied automatically.

Kiosks can be configured as a Single App Kiosk or Multi App Kiosk. Single App Kiosk is useful when running a device with a single application. Multi App Kiosk is useful for creating an environment where the user interacts with multiple applications. EMM also provides a Kiosk Wizard that is an interface for app development and a Kiosk Browser that only connects to certain URLs for security, such as corporate websites.

NOTE When developing an application that runs in Kiosk mode, it is recommended that you design it to run in full screen.

Strengths of EMM Kiosk

The advantages of EMM Kiosk are as follows:

- Conveniently deploy different types of applications on the Kiosk at the same time.
- Utilize diverse features, such as wallpaper, orientation, and icon setting.
- Efficiently manage the device settings, such as Wi-Fi and Bluetooth.
- Disable Kiosk mode easily to manage the device quickly.

Kiosk types

Kiosk types available as follows:

- Single App Kiosk: Kiosk mode with a single app only
- Multi App Kiosk: Kiosk mode with multiple apps that can be easily configured by Kiosk Wizard
- Kiosk Browser: A web browser for running only specific URLs for a special purpose

Kiosk Wizard operating environment

To run the Kiosk Wizard successfully, you need a PC or a laptop that meets specifications stated below:

- CPU: i5, 2.X GHz or higher
- Memory: 4G or more
- HDD: 500G or more
- OS: Windows 7 or above

Supported device environment

The Kiosk types that can run on Android Legacy and Android Enterprise devices of Samsung or other manufacturers are as follows:

	Samsung Android Legacy	**Samsung Android Enterprise Fully Managed Device**	**Non-Samsung Android Legacy**	**Non-Samsung Android Enterprise Fully Managed Device**
Android 6.0 ~ 8.0	Single-app kiosk Multi-app kiosk Kiosk Browser	Single-app kiosk Multi-app kiosk Kiosk Browser	Not supported	Multi-app kiosk Kiosk Browser
Android 9.0 or Higher	Single-app kiosk Multi-app kiosk Kiosk Browser	Single-app kiosk Multi-app kiosk Kiosk Browser	Not supported	Single-app kiosk Multi-app kiosk Kiosk Browser

NOTE EMM provides Single-app Kiosk with Google managed apps for Android Enterprise devices with version 9.0(Pie) or higher.

Basic functions in a Kiosk menu

The following functions are provided in **Kiosk** in the Admin Portal.

- **Add**: You can create a new Kiosk by selecting between Multiple App Kiosk and Single App Kiosk.

  To create a single app Kiosk: See Creating a Single App Kiosk.

  To create a multi app Kiosk: See Creating a Multi App Kiosk.
- **Modify**: You can modify an existing Kiosk. For more information, see Modifying and deploying a Kiosk.
- **Copy Multiple Applications**: You can copy a multi app Kiosk and create a new Kiosk. A single app Kiosk does not support the copy function. For more information, see Creating a Kiosk application by copying a Multi App Kiosk.
- **Delete**: You can delete the selected Kiosk.
- **Device Command - Update Application**: Sends the **Update Application** device command, and updates the Kiosk on the device.
- **Apply**: Apply the selected Kiosk to the devices where the Kiosk policy is assigned.

Creating a Single App Kiosk

The methods for adding an application to Android devices to create a Single App Kiosk are as follows. To set Kiosk policies in a profile and install a Single App Kiosk to a device, see Creating a Single or Multi App Kiosk in a Profile and Installing a Kiosk on a device.

To convert an APK file into a single app Kiosk, follow the steps below:

1. Navigate to **Kiosk**.
2. Click **Add** and click **Add Single Application**.
   - **Installation File**: Click **Browse** to select an APK file of the application. When the file is registered, platform, version and package name are automatically entered.
   - **Application Name**: Enter name for the Kiosk application.
     - **Platform**, **Version**, **Package Name**: The platform information, application version and the package name of the registered file are displayed.
     - **Integrity validation**: Select whether you want to validate the integrity of data with a cyclic redundancy check (CRC). A CRC determines the check value used to ensure that there are no errors in data sent through a network, and sends it along with the data.
3. Click **Save**.

NOTE When you register an application as a single app kiosk, EMM AppWrapping might affect your app signing key. If your apk is dependent on an app signing key, please revise the `AndroidManifest.xml` file as below and rebuild your apk.

1. Check whether it has `category.HOME` and `category.DEFAULT`. If not, please add it.

```
android:name="android.intent.category.HOME"
android:name="android.intent.category.DEFAULT"
```

2. Add `android:lockTaskMode` configuration as below:

```
<activity
    android:name=".MainActivity"
    android:lockTaskMode="if_whitelisted">
    <!-- ... -->
</activity>
```

3. Rebuild the apk and try to register as a single kiosk app.

Creating a Multi App Kiosk

The methods for creating a Multiple App Kiosk configured with applications and widgets using Kiosk Wizard are as follows. To set Kiosk policies in a profile and install a Multi App Kiosk to a device, see Creating a Single or Multi App Kiosk in a Profile and Installing a Kiosk on a device.

You can configure the multi-app kiosk with various applications and utilities as follows.

- Applications: Internal, public and control applications of EMM.
- Utility: Folder, Banner, Text, Calendar, Cock, Bookmark, Dialer

Creating a Multi App Kiosk

To launch the Kiosk Wizard and create a multi app Kiosk, follow the steps below:

1. Navigate to **Kiosk**.
2. Click **Add** and select **Add Multiple Applications**.
3. Configure the Kiosk launcher using Kiosk Wizard in “Add Kiosk“ window.
    - For details about each Kiosk Wizard component, see Exploring Kiosk Wizard.
    - To learn how to use the Kiosk Wizard, see Using Kiosk Wizard.
4. Click **Save** to generate an APK file.

Creating a Kiosk application by copying a Multi App Kiosk

You can create a new by copying an existing. Kiosk copy is only available for multi app Kiosk.

To copy, follow the steps below:

1. Navigate to **Kiosk**.
2. Select a multi-app kiosk to copy from the list and click **Copy**.
3. Enter information in “Copy Kiosk“ window.
4. Click **Save**.

Creating a Single or Multi App Kiosk in a Profile

You can create a single or multi app Kiosk when you set a Kiosk policy in the Profile menu.

To create a single or multi app kiosk in the Profile menu, follow the steps below:

1. Navigate to **Profile**.
2. Click **Add** to create a new profile.
3. On the “Add Profile” page, enter the required information, including Name and Platform, and then click **Save & Set Policy**.
4. On the “Set Policy” page, click **Kiosk** under **Android Enterprise or Android Legacy**.
5. Select a Kiosk type between **Single app**, and **Multi app** to create in **Kiosk app settings**.
6. Click **Add** to create a new Kiosk. If you want to configure the existing kiosks, click **Select** and choose from the list of already registered Kiosks in the Kiosk menu.
7. Create a Single app or Multi app kiosk in the “Add Single/Multiple Application” window and click **Save**.
8. Click **Save or Save & Assign** to apply the policy to the devices.

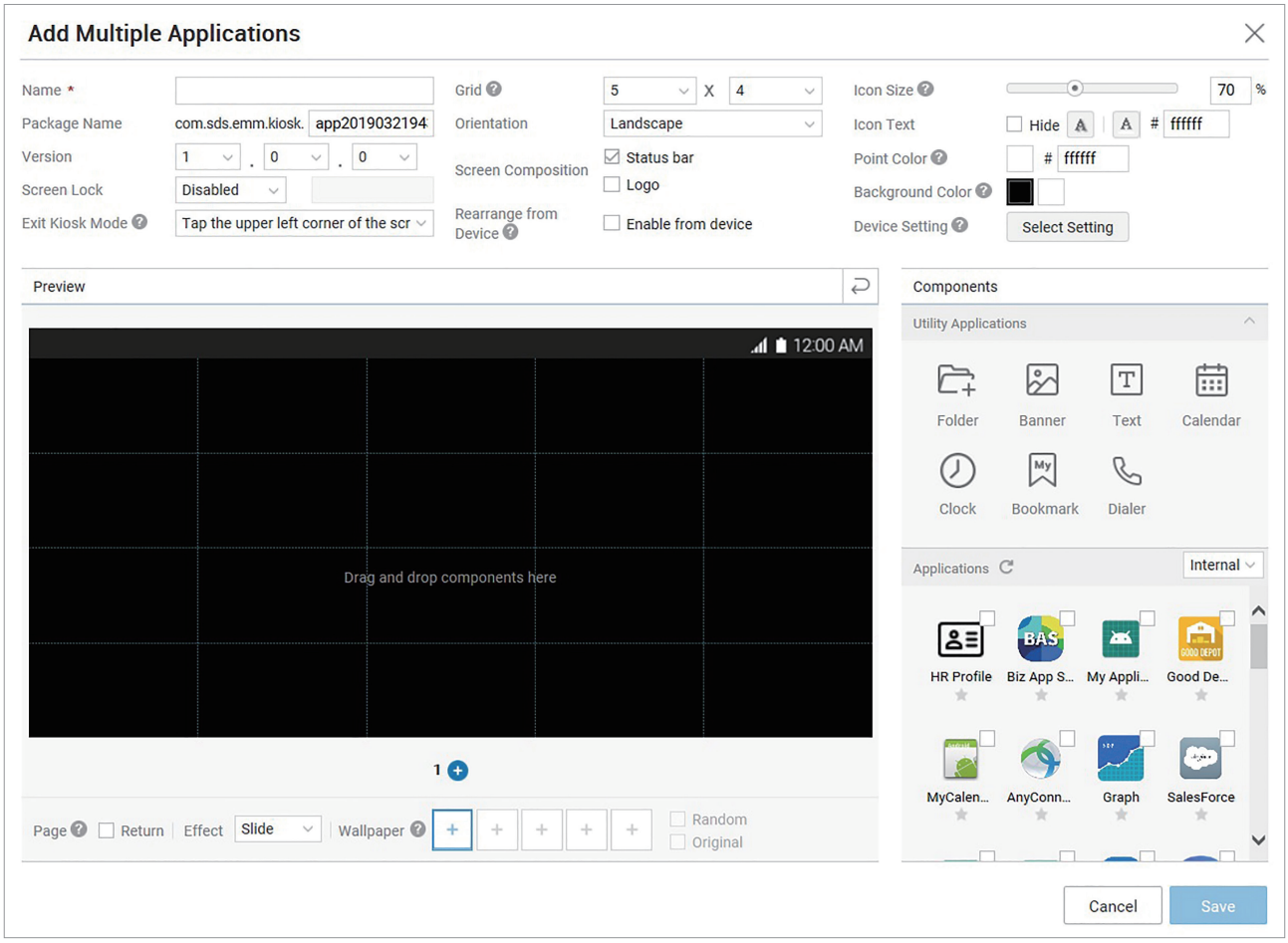
Exploring Kiosk Wizard

The Kiosk Wizard is an interface that enables to create a multi app Kiosk. EMM provides the Kiosk Wizard to help clients utilize Kiosk apps in a variety of work environments without needing to purchase an additional Kiosk launcher or develop one.

Using the Kiosk Wizard, you can deploy various types of applications as Internal, Public, and Control in Kiosk mode. Moreover, EMM provides diverse features, such as Bookmark and Clock, to be configured in devices using Kiosk mode.

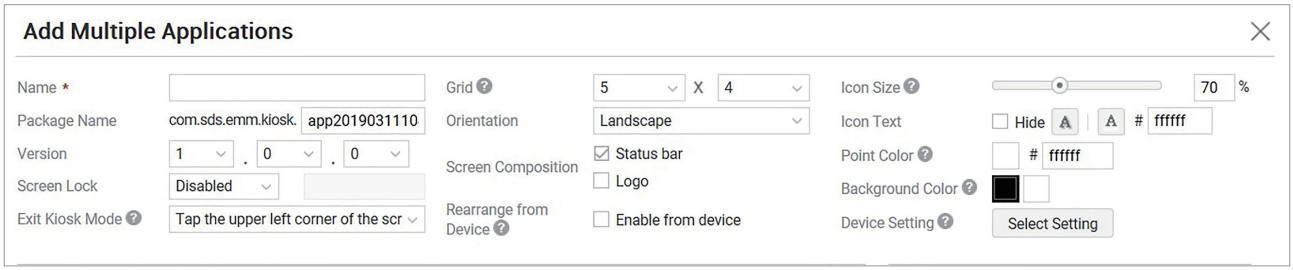
The Kiosk Wizard composition is as follows.

- **Kiosk Wizard menu**: Basic and advanced settings for customizing Kiosks
- **Preview**: Preview screen of the device in Kiosk mode
- **Components**: Utilities and applications that can be added



Kiosk Settings

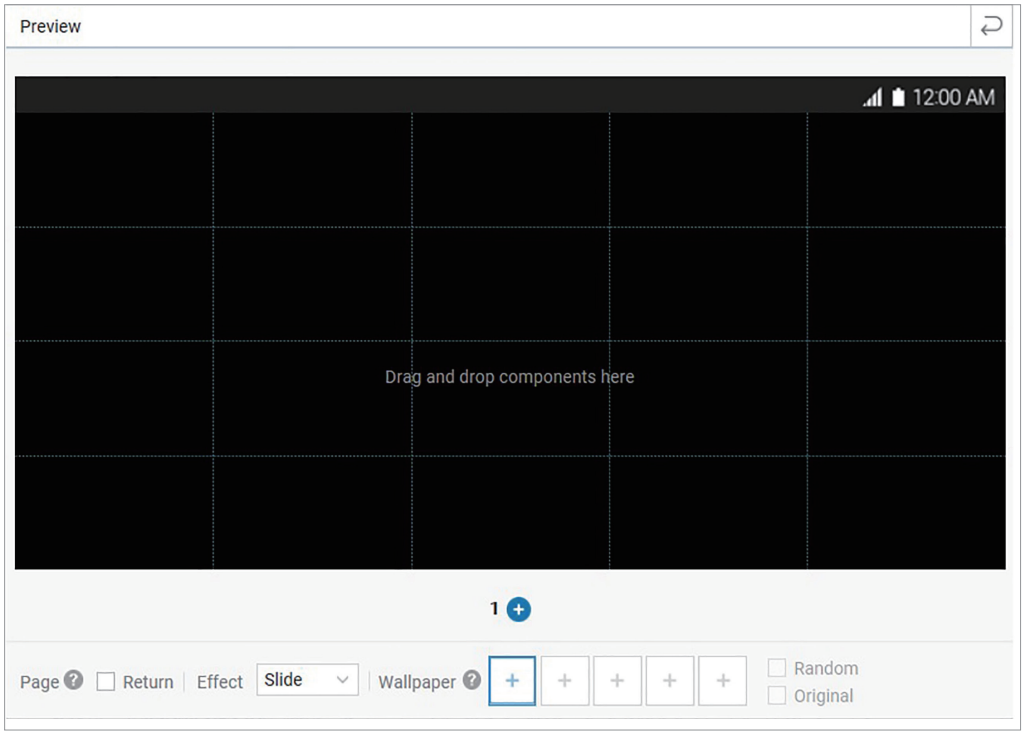
Configurable items are shown below:



- **Name**: Enter the name of the Kiosk
- **Package Name**: Enter a package name of the Kiosk
  - When you create a new package, a package name will be generated automatically.
- **Version**: Select a version of the Kiosk. Default version is 1.0.0.
  - When you modify the version, the version number automatically increases.
- **Screen Lock**: Select the screen lock options for a Kiosk device.
  - You can set the screen lock password for Kiosk mode, and you must deploy the policy if you want to change the password.
- **Exit Kiosk Mode**: You can configure the user-end actions to unenroll the Kiosk device. This touch action can be used when the device is offline. For more information, see Exiting Kiosk mode.
- **Grid**: Select Grid option according to the orientation setting.
- **Orientation**: Select orientation setting.
- **Screen Composition**: You can add a status bar and logo on a customized Kiosk device.
  - When adding a logo, click **Logo** on the Preview screen. You can add an image via the “Register log image” window.
- **Rearrange from Device**: Check to allow users to rearrange icons on the device.
- **Icon Size**: Icon size can be adjusted from 50% to 100%
- **Icon Text**: Choose whether to show or hide the icon text.
  - If you select Show, you can also configure the style, such as the font color and shadow options.
- **Point Color**: Set the color to be applied to the icons and page indicator in the Kiosk launcher.
- **Background Color**: If there is any space other than the Kiosk background image, it is filled with black or white.
- **Device Setting**: Click Select to configure the device settings to be used in Kiosk mode. For more information, see Allowing device settings.
  - You can select all items or select each item to be allowed in the “Select Device Setting” window.

Kiosk preview

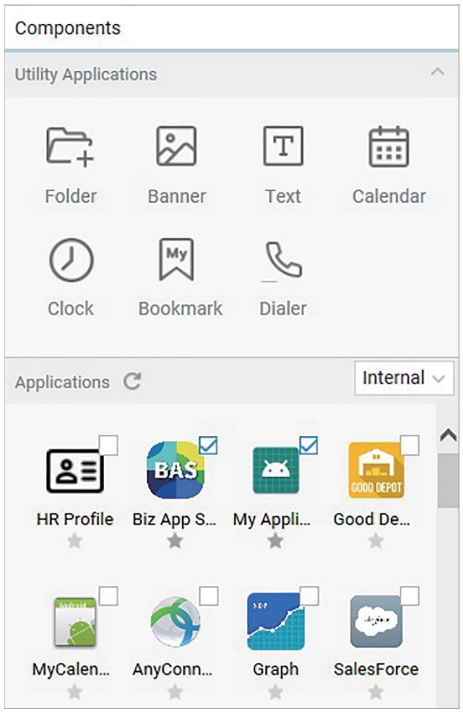
You can arrange Utility Applications and Applications on the Kiosk preview screen.



- : Click to reset the preview page.
- **- / +**: Click - or + to add or delete pages. You can add up to 9 pages.
- **Return**: Check to allow users to return to the first page from the last page of Kiosk mode.
- **Effect**: Select an effect for turning page.
- **Wallpaper**: Upload an image for the background. Click the box to add the wallpaper image. You can upload up to 5 images. Then, click the gray box area in the “Register background image” window.
  - **Random**: Check to show the registered wallpapers in random order.
  - **Original**: Check to use the original size of the image.

Wizard components

Kiosk components consist of Utility, Internal applications, Public applications, and Control applications. You can easily drag and drop components on the Preview screen for the customized Kiosk layout.



- **Folder**: To manage applications by folder, drag and drop the folders on the preview screen.
  - The name of folders can be modified. When there are applications in the folder, thumbnails of the applications are shown. Double click the folder to add, delete, or move the applications inside.
- Drag and drop items on the preview screen, and configure details from the pop-up window:
  - **Banner**: The Banner component can be customized in the “Add Banner” window, you can configure settings such as the ratio, image, and URL.
  - **Text**: The Text component can be customized in the “Add Text” window, you can configure settings such as the Text content, ratio, and text style. Text can change font size, colors and location.
  - **Calendar** and **Clock**: The Calendar component can be customized in the “Add Calendar” window, you can configure settings such as the ratio, widget style, and text color. Clock mode can be selected between 12-hour clock and 24-hour clock which is shown on device.
    Clock and Calendar are available in multiple languages (Korean, English, French, German, Italian, Portuguese, and Spanish) on user devices.
  - **Bookmark**: The Bookmark component can be configured to use a specific URL in the “Add Bookmark” window. You can configure the icon image of the bookmark, name, and URL.
  - **Dialer**: The Dialer component is used for the call feature on the kiosk device.

- **Applications**: Choose applications to allow users to use in the Kiosk app. You can search with application category such as Internal, Public and Control.

  Drag and drop the application to add to the preview screen. When you hover your mouse over applications, you can find app name, version, package name, supporting device and service period.

  - **Internal app**: These are the EMM internal apps registered in the Application menu.

    There are two types of internal apps; Automatic and Manual. To set the app as an Automatic app, click the star icon on the bottom of thumbnail of each app. And check the installed to device automatically upon Kiosk installation.

    To set the app as manual app, do not click the star icon and just check the check box or drag&drop the app to the screen. These applications will be installed on the device upon the Kiosk installation, but the app will be shown as empty icon and the user needs to click the icon to install the application.
  - **Public app**: These are the public apps registered in the Application menu.
  - **Control app**: These are the control apps registered in the Application menu.

NOTE Maximum length of URL in Bookmark, Text, and Banner is 300 characters including special characters.

Using Kiosk Wizard

Below is a Kiosk Wizard user guide that can help you develop a multi-app kiosk more easily.

You can build a multi-app kiosk using the Kiosk Wizard as follows:

- Configuring wallpaper
- Setting grid
- Creating logo
- Creating banner
- Configuring applications
- Configuring Widget
- Allowing device settings

Configuring wallpaper

According to the IT admin's plans, the Kiosk home screen contains the in-store application, and the second page has a clock, calendar, and widgets.

To register a Kiosk home screen's wallpaper, follow the steps below:

1. To register a wallpaper on the Kiosk home screen, click + next to **Wallpaper**, at the bottom of the preview image.
2. In the "Register background image" window, click and select the file you want to upload, then click **Save**.
   - You can upload image files in PNG and JPG formats, and you can use the mouse wheel to adjust the image size and position. (File type recommended PNG)
3. Select the application for the wallpaper to configure the store management screen. For more details, see Configuring applications.
4. To configure the second page, click **+** at the bottom of the preview image, and then click + to add a wallpaper. Drag the following widgets from the Utilities area to the preview screen: Clock, calendar and then in the window, choose the size, style, and text color for each item.
   - In the "Add Clock" window, the selected clock format clicking **Use 24-hour format** will be shown after it is deployed to user device.
5. Set **Effect** for page return to **Slide**.
   - When you click **Return**, you can swipe to the first page from the last one.

Setting grid

The IT admin wants to split the screen horizontally and vertically to configure the location of the widgets and applications.

To set the grid and orientation, follow the steps below:

1. In **Grid** and **Orientation** at the top menu, set **Grid** and click **Auto rotate** to apply both horizontal and vertical screens. Then, the grid area appears in the preview screen.
   - The Grid area changes depending on the screen switching such as Landscape, Portrait, or Auto Rotate.
   - Please note that if you change orientation or grid, the current configuration is reset or existing components are deleted.
2. To configure the screen, drag and drop widgets and applications into the grid area.
   - To reset screen configuration, click  .

Creating logo

The IT admin wants to add a company logo to the Kiosk.

To register the company logo, follow the steps below:

1. In **Screen Composition** at the top menu, click the **Status bar** and **Logo** checkbox, to get them displayed in the preview screen.
2. On the preview screen, click **LOGO**.
3. In the “Register logo image“ window, click and select the logo image file you want to upload, then click **Save**.

Creating banner

The IT admin wants to configure a promotional banner that leads you to the product promotion site when you click it.

To register the banner, follow the steps below:

1. In the Utility Applications pane under **Components**, click **Banner** and drag and drop into the preview screen.
2. In the “Add Banner“ window, select the banner size, register the image for clicking , enter the promotional site address in the URL area, and then click **Save**.
   - Size options may be limited, depending on the grid settings.

Configuring applications

Configure the internal and public applications that the multi app Kiosk should run. The applications registered in Application menu in the Admin Portal appear as thumbnails in the Applications pane of the Kiosk Wizard menu.

To add applications that should be included in the multi app Kiosk, follow the steps below:

1. In the Applications pane under **Components**, select **Internal**, and then choose the Secure Browser application and other work-related Internal applications.
2. In the Applications pane under **Components**, select **public**, and then select a control application.
   - To remove an application from the preview screen, click at the top.

Configuring Widget

To ensure user convenience, add the Clock, Calendar, Dialer widgets to the background.

To register the widgets, complete the following steps:

1. Drag the following widgets from the **Utility Applications** area to the preview screen: **Clock**, **Calendar**, and **Dialer**.
2. In the “Add...“ window, choose the size, style, and color for each item. Then, click **Save**.
3. To change the information about a widget, double-click the widget, and then make modifications.
   - To relocate the widgets, drag and drop it.
   - To remove a widget from the preview screen, click at the top.

Allowing device settings

You can allow users to change the kiosk device's settings. Users can tap i in the bottom left corner of the Home screen, tap **Settings** in the Kiosk Launcher details pop-up window, and then open the Settings screen.

You can allow the following device settings:

- Wi-Fi, Location, Bluetooth, Display, NFC, Lock Screen, Mobile Data, Sound, Device Maintenance, Mobile Networks

NOTE In case of tablet, following items of settings can be accessible even though the IT admin has not allowed the Settings to the device. For tablet devices with Android 9.0 or a higher version, all items of settings cannot be accessible if the IT admin has not allowed the Settings to the device.

- Bluetooth, NFC, Mobile Data, Location

To allow users to change the kiosk device's settings, follow the steps below:

1. Click **Select Settings** at the top menu.
2. Choose the settings that you wish to allow in the "Device Setting" window.
   - Click the **Select All** to select all settings. If you click individual setting, the **Select All** becomes disabled automatically.
   - Any settings that are not supported by the device can't be configured, even if you allow them.
3. Click **Save**.

Using a Kiosk Browser

EMM provides Kiosk Browser for connecting to specific websites, such as corporate websites that require security. Kiosk Brower is EMM's web exclusive browser and Secure Browser is the device exclusive browser which can run only URLs of designated websites for security purposes.

Specifying the URL for Kiosk Browser

To add the URL that Kiosk Browser should connect to, follow the steps below:

1. Navigate to **Profile**.
2. In the list, click the name of the profile to which you are trying to add a policy.
3. On the "Profile Detail" page, click **Modify Policy** in the footer.
4. On the "Set Policy" page, click **Kiosk** under **Android Enterprise** or **Android Legacy**.
5. Set **Kiosk app settings** to **Kiosk Browser**.
6. Set the items that appear at the bottom of the Kiosk app settings. You can set various policies related to Kiosk Browser. For more information about applicable policies, see Configuring Android Legacy Policies and Configuring Android Enterprise Policies.
   - **Set Kiosk Browser**: The default Kiosk Browser file provided by EMM is automatically input.
   - **Default URL**: Enter the URL of the default webpage that should be called when Kiosk Browser is launched. You can enter the URL up to 128 bytes including alphanumeric characters and some special characters (_,., -, *, /).
   - **Screen Saver**: Configure the Screensaver settings to protect the screen when it is inactive for the maximum inactive session time.
   - **Session timeout**: Set the session timeout time in seconds.
   - **Text copy**: Set whether to allow or disallow text copying in Kiosk Browser.
   - **File Upload**: Set whether to allow or disallow file uploads in Kiosk Browser.
     - When file upload is set to **Allow**, attachments can be registered when composing a mail in Kiosk Browser.
7. Click **Save**.
8. To deploy the policy, click **Apply** on the "Profile Detail" page.
   - The new profile is applied to every device belonging to the organization or group to which the profile has been assigned.

Installing a Kiosk on a device

You can install a Kiosk on an EMM-installed device as follows:

- Install a Kiosk using a device command in the **Device**, **User**, **Group**, and **Organization** menus.
- Set a Kiosk in a profile and deploy it. Then, the Kiosk will be installed automatically.

Installing a Kiosk using a device command

To install a Kiosk on an enrolled Android Legacy or Android Enterprise device using a device command, follow the steps below:
For more information about a device command, see Sending device commands to devices.

1. Navigate to **Device**.
2. On the “Device” page, click the checkbox of the device and click **Device Command**.
3. In the “Device Command” window, click **Application** > **Install or Update App**.
4. In the “Request Command” window, enter the Kiosk application name into the field and click  .
5. Click the Kiosk application to install and click **OK**.

Installing a Kiosk by deploying a profile

Set a Kiosk-related policy in a profile on an Android device, and deploy a profile. Then, the profile containing the set policy is installed automatically to the device.

To configure a Kiosk policy in a profile and apply it to the device, follow the steps below:

1. Navigate to **Profile**.
2. On the “Profile” page, click a profile name to assign a Kiosk to.
3. On the “Profile Detail” page, click **Modify Policy** in the footer.
4. On the “Set Policy” page, click **Kiosk** under **Android Enterprise** or **Android (Legacy)**.
5. Set **Kiosk app settings** to **Single app**, **Multi app**, or **Kiosk Browser**.
   Configure the profile details by Kiosk app type. For more information about applicable policies, see Configuring Android Legacy Policies and Configuring Android Enterprise Policies.
6. Click **Save & Assign** to save the information and to proceed with assigning the policies to devices.
   - Click **OK** to only save the information and Kiosk set in the policy will be automatically installed.
   - Either by not configuring the **Kiosk app settings** or allowing to the **Delete Kiosk app when policy is removed**, you can set the Kiosk application to be automatically deleted from the device when a profile is deployed.

Modifying and deploying a Kiosk

If you need to modify the components of a Kiosk, then change the Kiosk file, build it again, and deploy it to the device. When you modify the settings of the Kiosk and build it again, a Kiosk file is created as described below:

- Single app Kiosk: Creates a Kiosk of the same version but under a new name.
- Multi app Kiosk: Creates a Kiosk of a higher version using the same name and the same package name.

To modify the components of a Kiosk, and then deploy it to the device, follow the steps below:

1. Navigate to **Kiosk**.
2. In the list, click  next to the Kiosk that you want to modify.
3. In the “Modify Single Application“ or “Modify Multiple Applications“ window, modify the items in the fields and click **Save**.
4. When modifying a multi app Kiosk, describe the changes in the “Confirm update“ window, and then click **Yes**.
   - Once the input fields are validated, the build will be completed.
5. Click  next to the re-created Kiosk and deploy it.
6. In the “Device Command - Update Application“ window, click **OK**.
   - The Kiosk on every device that uses the relevant Kiosk is updated, based on the Inventory information on the device. If there are no devices to update, a notification message appears.

Checking the version history of a Kiosk

To check a version history of a Kiosk, follow the steps below:

1. Navigate to **Kiosk**.
2. In the list, click **Version** of the Kiosk that you want to modify.
3. In the “Version History“ window, check the update **Date**, **Version**, and **Changes**.

Enabling/Disabling a Kiosk

You can allow or not allow users from launching a Kiosk installed on a device. The Kiosk that is not allowed to be launched will appear as usual, but it cannot be launched, even if a user taps it.

To allow or not allow users from launching a Kiosk, follow the steps below:

1. Navigate to **Device**.
2. On the “Device” page, click the checkbox of the device and click **Device Command**.
3. In the “Device Command” window, click **Application** > **Run App** or **Stop App**.
   - For devices that have a Knox Workspace, click a target area between **General** and **Knox Workspace**.
   - For Fully Managed with Work Profile devices, click a target area between **Work Profile** and **Personal Profile**.
   - If multiple devices are selected, click devices or target areas under **Target Device & Area**.
4. In the “Request Command” window, click **OK**.
   - You can check the results of processing device commands in **Service Overview** > **History** > **Device Command History**.

Exiting Kiosk mode

If there is a problem with the device running a multi app kiosk or remote control is not possible due to communication error with the server, you can exit Kiosk mode by controlling the device or deactivating Kiosk mode.

For information about deleting a Kiosk from the device using a profile, see Installing a Kiosk by deploying a profile.

To exit Kiosk mode using a device command follow the steps below:

1. Navigate to **Device**.
2. On the “Device” page, click the checkbox of the device and click **Device Command**.
3. In the “Device Command” window, click **EMM** > **Exit Kiosk**.
4. In the “Request Command” window, click **OK**.
5. Kiosk mode stops, the device runs in normal mode, and EMM is activated.
    - To return to Kiosk mode, apply the profile again.

To exit Kiosk mode by deactivating it, follow the steps below:

1. Tap **i** in the bottom-left corner of the Home screen, or touch the left menu displayed on the device, and then tap **i About** that appears at the bottom of the screen.
2. Perform the touch actions as follow to disable Kiosk mode.
    - For Multi App Kiosks, perform the touch action that is entered in the **Exit Kiosk Mode** item in Kiosk Wizard.
    - For Kiosk Browsers, tap and hold ⓘ at the bottom-left corner of the home screen.
3. Kiosk mode stops, the device runs in normal mode, and EMM is deactivated.
    - To activate EMM and return to Kiosk mode, reinstall EMM.

8

Content

Content

Upload various types of content, such as documents, images, texts, and videos on the EMM Admin Portal and deploy them to devices by the Mobile Content Management. The uploaded content can be sent through the Content Delivery Network (CDN). CDN can prevent the server overload and send the data safely and quickly.

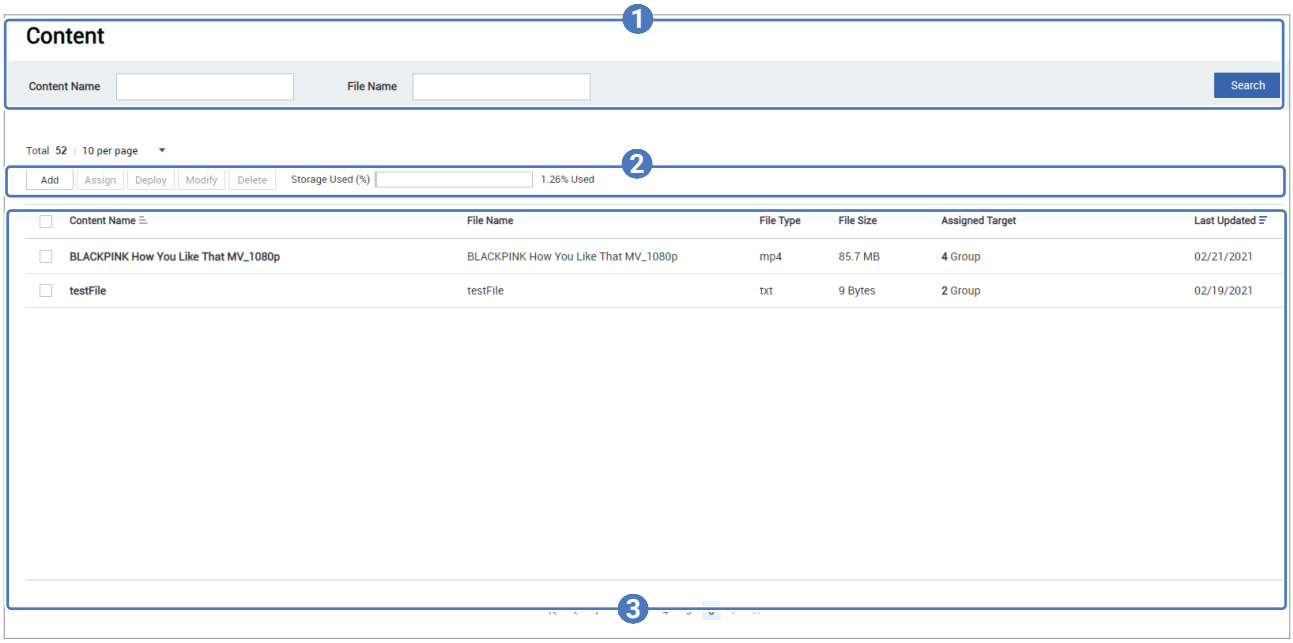
Check the following before using the Content service:

- Content is stored on the EMM server and no additional capacity limit applies.
- Targets that can be added as content are limited to documents and image files of corporate data without security issues. They can be deployed to groups, organizations, and all devices in the company.
- Deployed content is automatically synchronized between the server and the device and the download history is managed.
- The Content service is provided to Android Legacy, Android Enterprise, and iOS devices.

This chapter explains the following topics:

Viewing the content list

Navigate to Content to manage content added to the Admin Portal. You can also perform specific functions for the selected content on the list.



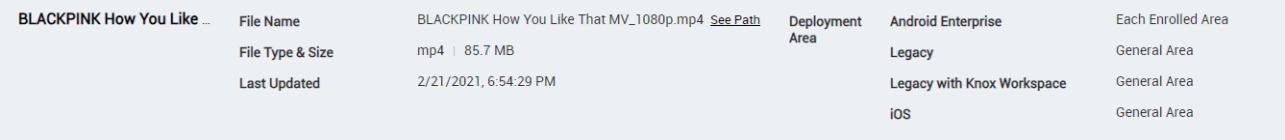
No.	Name		Description
1	Search field		Search for content.
2	Function buttons	Add	Add content. For more information, see Adding content.
		Assign	Assign content. For more information, see Assigning and deploying content.
		Deploy	Deploy content. For more information, see Assigning and deploying content.
		Modify	Modify content.
		Delete	Delete content.
		Storage Used (%)	EMM server usage appears. All other files such as APK in the server as well as the content are summed up in the usage.
3	Content list		View the information of the content on the list.

Viewing the content details

View the content details by clicking the Content Name on the content list.

Summary area

The summary area contains the information about the selected content, such as the file name, download path, file type and size, last update date, and deployment area.



Tab: Device

The Device tab shows the list of devices that the content was assigned to. The device list shows the status and name of the device to which the content is assigned, IMEI/MEID (additional IMEI will be displayed if using Dual SIM), serial number, user name, platform and management type, and download date. Click **Refresh**, to see the latest version of the device list.

Tab: Assigned Target

The Assigned Target tab shows the list of groups and organizations, or all devices that the content was assigned to. The Assigned Target list shows assigned targets (group/organization/all devices), target type, download method (automatic/manual), number of users assigned, number of devices assigned, and the last date assigned to the target. Click **Unassign** to remove the content assignment from the groups, organizations, and all devices on the list.

Adding content

Add images, text, videos, and other files to the Admin Portal to assign and deploy them to groups, organizations, or all devices. Deployed content is automatically synchronized between the server and the device and the download history is managed. Content can be redeployed after modification or deleted as needed.

NOTE

- The maximum file size that can be uploaded as content, and the maximum number of users and the maximum file size for downloading files at the same time are set in the Content category under **Setting > Server > Configuration**. For more information, see Configuring the environment.
- Content is automatically synchronized between the server and the device when EMM starts. It can also be synchronized by sending the update device command or clicking the update button on the device.
- Restrictions on Android 10: For devices running Android 10 OS, after files are deployed to devices, if the file is changed or the content name is modified, the files already deployed to the devices are not automatically updated. IT admins must deploy the files again for device users to see the modifications.

To add content, complete the following steps:

1. Navigate to **Content**.
2. On the “Content” page, click **Add**.
3. On the "Add Content" page, enter the following information.
   - **File (Maximum size MB)**: Click  and select the file to upload. The file types that can be added as content are as follows:
     - documents: doc(x), ppt(x), xls(x), gul, hwp, pdf, rtf, wks, wpd, txt
     - images: bmp, gif, jpeg, jpg, png, psd, tif, tiff, ico, 3gp
     - videos: avi, mkv, mp4, mov, mpg, mpeg, rm, swf, wmv, mp3, wav, vcf
     - etc.: rar, zip, json, db3, xml, kml, kmz, ovpn, html, htm, qmg, ogg, vtpk, geodatabase
   - **Content Name**: Enter the content name.
     - Enter a unique content name. Be aware that if a file with the same content name is assigned and deployed to target devices, the new content file overwrites the old file.
   - **Download Path**: Enter the download path. Content files are saved in the Download folder in Shared Storage, Internal storage/Download/EMM/Content for Android, and Sandbox for iOS.
   - **Deployment Area**: Select a deployment area. Content can be deployed only to the activated Android and iOS devices. If you select multiple areas, the content will be deployed to all the selected deployment areas.
     - For Android Enterprise, Android Legacy, and iOS devices, content will be automatically deployed to the designated area.
     - For Android Legacy devices with Knox Workspace, select a deployment area from among General Area, Knox Workspace, and General Area+Knox Workspace.
4. Click **Save & Assign** to save the information and proceed to assign the content. For more information, see Assigning and deploying content.
   - Click **Save** to save the information and return to the content list.

Assigning and deploying content

Assign and deploy the content added to the Admin Portal to groups, organizations, or all devices. Deployed content is directly transferred to the devices and the downloaded content list can be viewed on the device screen.

NOTE The content can be assigned to groups, devices, or organization. The content assigned to the parent organization is not inherited, so it must be additionally assigned to the sub-organizations.

To assign and deploy content, complete the following steps:

1. Navigate to **Content**.
2. On the "Content" page, select the content to assign and click **Assign**.
   For the content that has been assigned but not deployed, or the content that are to be redeployed, click **Deploy**.
3. On the "Deploy Content" page, select a download method and deployment targets.
   - **Download Type**: Select a download type. If you select Automatic, the content will be automatically downloaded to the device upon deployment. If you select Manual, the user must download it manually.

     NOTE In case that the download type is selected as Automatic, when a device is newly registered in a group or organization, content is automatically downloaded at the time of device activation. If the user randomly deletes content from the device, the content will be automatically downloaded when synchronized.

   - **Target Type**: Select the targets to deploy to. The deployment targets are groups, organizations, and all devices. Select groups and organizations that appear at the bottom according to the selected target type.
4. Click **Assign & Deploy** to deploy the content.
5. In the "Assign & Deploy Content" window, check the download method, deployment targets, content and deployment areas, and click **OK**. The deployed content is saved in the download path of the deployment area specified when adding the content.
   - To only assign content, click **Assign**. Content that has been assigned can be deployed by clicking **Deploy** on the "Content Detail" page.

NOTE
- Content can be downloaded only when EMM is running on the device.
- For iOS devices, background synchronization is not possible and downloaded files may be copied within the app and cannot be deleted depending on 3rd-party applications.
- The content is automatically redeployed, even if the target users enroll new devices after the deployment or delete the content from their devices.

Deleting content

To delete the content deployed to devices, complete the following steps:

1. Navigate to **Content**.
2. On the “Content” page, select the content to delete, and click **Delete**.
3. In the “Delete” window, click **OK**.

NOTE When user accounts or devices are assigned to a new organization or group, the content is automatically downloaded to devices. After the content is downloaded to devices, the content is automatically deleted from devices in the following cases:

- The user account is assigned to a different organization or group.
- The device is assigned to a different group.

Viewing the content download history

To view the download history of the content deployed to devices, complete the following steps:

1. Navigate to **Content**.
2. Click the content to view the download history.
3. On the "Content Detail" page, click the **Device** and **Assigned Target** tabs, and view the information of the device where the content was deployed and the assigned targets.
   - **Device**: Displays the list of devices where the content was deployed.
     You can view the device status and name, IMEI / MEID information, serial number, user name, platform information, and the date when the user downloaded the content.
   - **Assigned Target**: Displays the list of targets where the content was assigned.
     You can view the assigned targets (group/organization/all devices), target type, download method (automatic/manual), number of users assigned, number of devices assigned, and the last date assigned to the target.

9

Integration Services

Integration Services

EMM provides a variety of integration services that can be linked to the back-end system of the company. Also, connectors can be set up to provide services from servers that are registered to the integration system.

NOTE

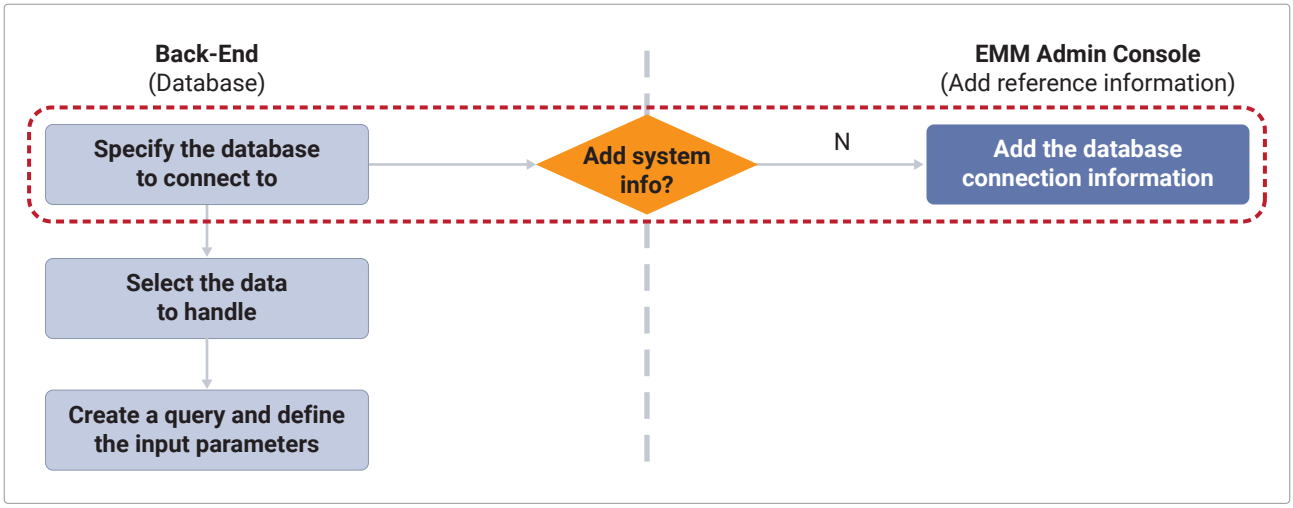
- The integration systems and connectors can show the Admin Portal menu, depending on license availability. Navigate to **Setting** > **License** for license availability.
- LDAP is not the subject of the CC evaluation.

Integrating with a database

A database is an integrated data system that collects and stores necessary data for operating all the resources and organizations within a company. Linked with a database, EMM controls and manages user devices registered in the database of a company.

To integrate with a database, you must enter the connection information required to access the database server and set up a database pool.

Access the database (DB) server and set up the database pool as described below.



Setting a database server

To connect to the database, complete the following steps:

1. Navigate to **System** > **Integration** > **Database**.
2. On the “Database” page, click + at the top of the page.
3. In the “Add Database” window, enter the following information:
   - **Pool Name**: Enter a pool name to manage the database. Up to 20 characters, including letters, numbers, and special characters (only dashes and underscores allowed), can be entered.
   - **Database Type**: Select between **ORACLE**, **MSSQL**, and **MYSQL** for the database type.
   - **User ID**: Enter the user ID of the database.
   - **Password**: Enter the user password of the database.
   - **Max Active Limit**: Select the maximum number of active connections from 10 to 50.
   - **Max Idle Limit**: Select the maximum number of idle connections from 0 to 30.
   - **Description**: Enter the description of the database connection.
   - **Database**: Enter the detailed information of the database connection.
     - **Automatic Input**: Enter the IP address. The JDBC URL will be automatically recorded.
     - **Manual Input**: Enter the JDBC URL directly.
     - **IP Address**: Enter the IP address of the database.
     - **Port**: Enter the port number of the database.
     - **Database Name (SID)**: Enter the SID or name of the database.
     - **JDBC URL**: Enter the URL for defining the database.
4. Click **Save**.

NOTE
- Pool names cannot be duplicated.
- Currently active databases cannot be deleted.

Checking the database connection status

To check the database connection status, complete the following steps:

1. Navigate to **System** > **Integration** > **Database**.
2. On the “Database” page, select an item to check, and then click **Check Database Status**.
   - The connection status will appear in the **Connection Status** field.

Integrating a directory server

EMM provides the Active Directory (AD) service that is built upon the industry-standard Lightweight Directory Access Protocol (LDAP) to access intra-enterprise data by integrating corporate's directory server.

Once the AD service is configured, you can perform the following:

- Keep user, organizational, and group information synchronized across multiple sites throughout the enterprise and update information on demand or automatically at specified intervals.
- Simplify the user registration process within the company through VPN, Microsoft Exchange, Certificate, or email account integration.

To configure and use the AD service, the following procedures must be performed:

Viewing the directory server status

Navigate to **System** > **Integration** > **Directory** to view all the directory server status information on the "Direct Integration" page. To view the detailed information of a specific directory server, click the pool name of a specific directory server on the list.

You can also perform the following actions on this page:

Icon and button	Description
Add	Add a directory server. For more information, see Adding a directory server.
Check Directory Status	Check the specific directory server status. For more information, see Updating the directory server status.
Search	Search for a specific directory server for the entered pool name or IP/host.
Modify	Modify the directory server information. For more information, see Modifying the directory server information.
Copy	Copy an existing directory server and add it to the list. For more information, see Copying a directory server.
Delete	Delete a directory server. For more information, see Deleting directory servers.

Adding a directory server

Add a directory server in the Admin Portal to synchronize corporate user information by integrating the corporate directory server.

To add a directory server, complete the following steps:

1. Navigate to **System** > **Integration** > **Directory**.
2. On the “Directory” page, click  at the top of the page.
3. On the Default Settings tab in the “Add Directory” window, enter the following information:
   - **Pool Name**: Enter a name for the pool that is up to 20 characters and that consists of letters, numbers, or special characters (only dashes and underscores are allowed) to distinguish it from other directory services.
   - **Encryption Type**: Select one of the following encryption types for the internet communication protocol used for communication with the directory server.
     - **None**: No encryption
     - **SSL**: Secured Socket Layer
     - **TLS**: Transport Layer Security
   - **Auth Type**: Select one of the following authentication types used for communication with the directory server.
     - **None**: no encryption
     - **Simple**: Select this if you are not certain about the authentication type.

- **DIGEST-MD5 (SASL)**, **CRAM-MD5 (SASL)**, or **GSSAPI (Kerberos)**: If you select one of these authentication types, configure the additional advanced settings on the Authentication Detailed Setting tab as follows:

Authentication type	Description
DIGESTMD5 (SASL) and CRAMMD5 (SASL)	Enter the following information for configuring the settings for Simple Authentication and security layer (SASL), which is a telnet-based protocol. • **SASL Realm**: Enter the realm value of the SASL server in the relevant domain's format, such as `sample.com`. • **Quality of Protection**: Select one of the following qualities of the data protection options. - **Authentication only**: Protects the data only for authentication. - **Authentication with integrity**: Ensures the integrity of all the data exchanged, including authentication data. - **Authentication with integrity and privacy**: Ensures integrity for all the data exchanges, including authentications through data encryption. • **Protection Strength**: Select one of the data protection levels. - **High**: Use 128-bit encryption. - **Medium**: Use 56-bit encryption. - **Low**: Use 40-bit encryption. - **Mutual authentication**: Click the checkbox to ensure data validity by inserting the key into the data exchanged between the client and server.
GSSAPI (Kerberos)	Enter the following information for GSSAPI (Kerberos) authentication. • **Kerberos Credential Configuration**: Select one of the following methods for obtaining a Kerberos ticket. - **Use native TGT**: Select this if you have already issued a ticket in the Admin Portal. - **Obtain TGT from KDC**: Issue a new ticket using the default user ID and password. • **Kerberos Configuration**: Select one of the following methods for configuring the Kerberos server. - **Use native system configuration**: Use the Kerberos server information defined in the Java Property. - **Use following configuration**: Enter the following Kerberos server information manually. - **Kerberos Realm**: Enter the realm of the Kerberos server. - **KDC Host**: Enter the Kerberos Key Distribution Center (KDC) host or the IP address. - **KDC Port**: Enter the KDC port number.

- **IP/HOST**: Enter the IP or host address of the directory server.
- **Port**: Enter the TCP port number that should be used for communication with the directory server. 389 is the default port number used for unencrypted communication with the directory server.
- **User ID**: Enter the user ID (administrator account) that can access the directory server. It can be entered in various forms, such as `domain\administrator ID`, `administrator ID@domain` or `CN=administrator ID`, `CN=Users`, `DC=domain`, `DC=com`.
- **Password**: Enter the user ID's password.
- **Max Active Limit**: Select the maximum number of active connections.
- **Max Idle Limit**: Select the maximum number of idle connections.
- **Description**: Enter a description of the directory server.
- **Cloud Connector**: Select whether to use the Cloud Connector.

4. Click **Connection Test** to test suitability with the entered information of the directory server, and then click **Save**.

Updating the directory server status

To update the directory server status, complete the following steps:

1. Navigate to **System** > **Integration** > **Directory**.
2. On the "Directory" page, click a specific directory server on the list, and then click **Check Directory Status**. You can view the updated information of the selected directory server on the list.

Copying a directory server

You can copy an existing directory server and add a new directory server to the list.

To copy a directory server, complete the following steps:

1. Navigate to **System** > **Integration** > **Directory**.
2. On the "Directory" page, click  in the row of the specific directory server that you want to copy information from.
3. In the "Copy Directory" window, modify the information, and click **Save** to add a new directory server to the list.

Modifying the directory server information

To modify directory server information, complete the following steps:

1. Navigate to **System** > **Integration** > **Directory**.
2. On the “Directory” page, click  in the row of the specific directory server that you want to modify the information of.
3. In the “Modify Directory” window, modify the information and click **Save**.

Deleting directory servers

To delete directory servers, complete the following steps:

1. Navigate to **System** > **Integration** > **Directory**.
2. On the “Directory” page, click  in the row of the specific directory server that you want to delete from the list.
3. In the “Delete Connection Information” window, click **OK**.

Linking services with LDAP and Cloud Connector

The IT admin at the client side can access the Admin Portal and configure the settings between LDAP and the Cloud Connector service. When the client’s LDAP is ready, the IT admin should enter the LDAP server information in the Admin Portal. The entered information is then sent to the SCC CS server with the tenant’s information, and the SCC CS server assigns an IP and Port for the LDAP service to the SCC server. From then on, EMM will not connect directly with the LDAP server, but will use the LDAP service using the IP and Port provided from the SCC server. For more information, see Integrating services in EMM.

Setting the connectors

EMM provides connectors to use various services within organization. Configure the operation hours of connector service by clicking **Connector Service** in **Setting** > **Server** > **Configuration**. For more information, see Setting the connector service operation hours.

Setting the database connector

The database connector supports checking and searching for data by connecting to the database server. This section describes how to set and manage database connectors.

Setting the database connector service

Configure the connector using the settings of the database server registered in **System** > **Integration** > **Database**.

To add a connector for database service, follow the steps below:

1. Navigate to **System** > **Connector** > **Database**.
2. On the “Database” page, click + at the top of the page.

3. In the “Add Service” window, enter the following information:
    - **Service ID**: Enter an ID for the service.
    - **Service Name**: Enter a name for the service.
    - **Status**: Select between Inactive, Activated, and Simulation for the service status.
    - **Pool Name**: Select the DB Pool name, which is used when the SQL type is queried.
      To view the registered pool, navigate to **System** > **Integration** > **Database**.
    - **SQL Type**: Select the **SQL ID**, **Query Type**, and **SQL Query** fields are enabled or disabled based on the SQL Type.
        - **MYBATIS** uses files registered as MYBATIS SQL Map on EMM.
        - **QUERY** uses query at SQL Query. If you choose a query, you can type a query in the SQL query test box.
    - **SQL ID**: Select the SQL Query ID registered on EMM. You can use this when SQL type is **MYBATIS**.
    - **Query Type**: Select the type of SQL query. You can use this when SQL type is **MYBATIS**.
    - **SQL Query**: Enter the SQL Query you want to execute. You can use this when SQL type is Query.
4. Click **Save**.

NOTE You cannot copy **Service ID** because it cannot be used as duplicate.

Testing the database connector service

You can check connection status of each database service through service tests to find out whether the service is working normally. To test each services, click  in **System** > **Connector** > **Database**. For more information, see Testing a directory service.

Setting the database service mapping information

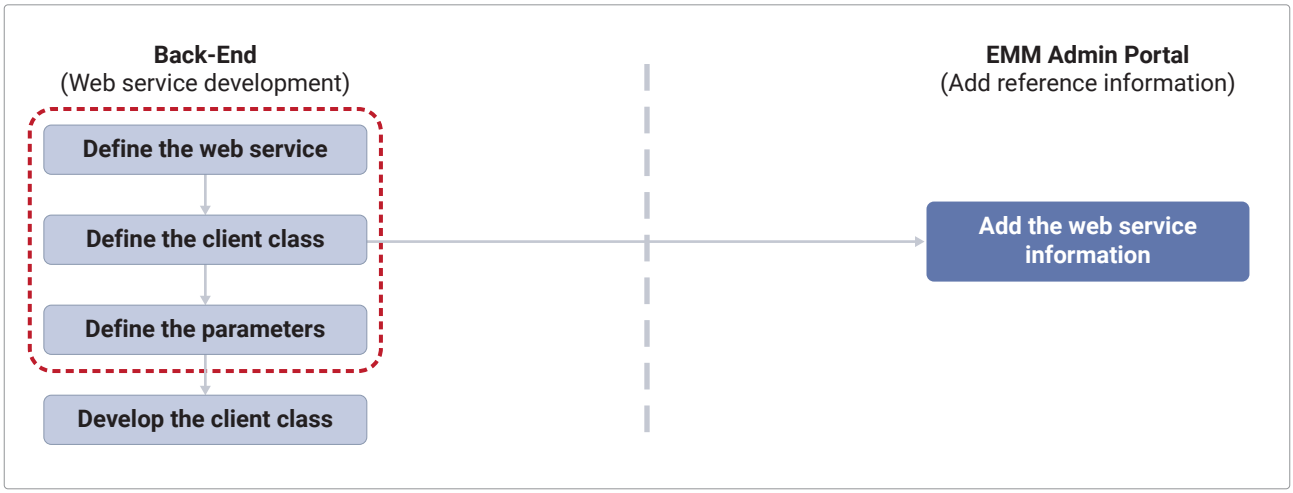
In the service mapping information, mapping information for the input and output parameters of the service can be automatically generated, added, modified, and deleted.

To set the input or output fields for mapping information for a service, follow the steps below:

1. Navigate to **System** > **Connector** > **Database**.
2. Click **Mapping Information**, if you set the **SQL Type** as **QUERY**.
3. Check the **Input Field** and **Output Field** in the “Mapping Information” window.
4. Click the **Input Field** tab:
   - Input Field is used as an input parameter for service calls.
   - You can change the **Alternate Name** and **Description**.
   - If you want to add an input field, click **Add Field** and if you want to delete an input field, click **Delete Field**.
5. Click the **Output Field** tab.
   - Output Field is used as an output field for responding to the service.
   - You can change the **Alternate Name** and **Description**.
6. Click the checkbox and click the field you want to use as the Output Field, and click **Save**:
   - Click **Delete All** to delete all registered output fields:
     - If you click **Delete All** to delete all output fields, the information transferred from integrated system is delivered to the devices without mapping.
   - Click **Load Output Field** to reconstruct the output field if the output field does not exist or if the SQL query has been changed.
     - Reconstruct the output field by analyzing the results, which are directly called after deleting the previous mapping information, in either XML or JSON format.

Setting the MBI connector

Mobile Business Integrator (MBI) supports customizing protocols and business logic. The section below describes the processing service of JAVA class-based business logic, such as Web Service and Custom Connector.



Setting the MBI service

To add connector for MBI service, follow the steps below:

1. Navigate to **System** > **Connector** > **MBI**.
2. On the "MBI" page, click + at the top of the page.
3. In the "Add Service" window, enter the following information:
   - **Service ID**: Enter an ID for the service.
   - **Service Name**: Enter a name for the service.
   - **Status**: Select between Inactive, Activated, Simulation for the service status.
   - **Client Class**: Select the class name, including the package of the Custom Class, that is be used for the service.
   - **Timeout (second)**: Select the service timeout limit.
4. Click **Save**.

NOTE You cannot copy **Service ID** because it cannot be used as duplicate.

Testing the MBI connector service

You can check the connection status of each MBI service through service tests to find out whether the service is working normally. To test each services, click in **System** > **Connector** > **MBI**. For more information, see Testing a directory service.

Setting MBI service mapping information

In the service mapping information, mapping information for the input parameters of the service can be automatically generated, added, modified, and deleted.

To set the input fields for mapping information for a service, follow the steps below:

1. Navigate to **System** > **Connector** > **MBI**.
2. Click **Mapping Information** after clicking the service item that you want to set the mapping information for.
3. Check the **Input Field** in the “Mapping Information” window.
4. Click the **Input Field** tab.
   - Input Field is the field used as an input parameter for service calls.
   - If necessary, you can change the **Alternate Name** and **Description**.
   - If you want to add an input field, click **Add Field** and if you want to delete an input field, click **Delete Field**.
5. Click **Save**.

Setting a directory connector

Using a directory connector, you can filter the user information of clients on the directory server integrated with EMM. You can extract the required user information through the directory type, set range, and detailed filter settings in the directory connector settings. Therefore, you can simplify the user registration process, which will improve work efficiency.

Viewing the directory connector status

Navigate to **System** > **Connector** > **Directory** to view all the directory connector status information on the ”Directory” page. To view the detailed information of a specific directory server, click the service ID of the specific directory connector on the list.

You can also perform the following actions on this page.

Icon and button	Description
Add	Add a directory connector. For more information, see Adding a directory connector.
Search	Search a directory connector.
Modify	Modify the directory connector information. For more information, see Modifying directory connector information.
Copy	Copy an existing directory connector and add it to the list. For more information, see Integration Services.
Delete	Delete a directory connector. For more information, see Deleting directory connectors.

Adding a directory connector

To add a directory connector, complete the following steps:

1. Navigate to **System** > **Connector** > **Directory**.
2. On the "Directory" page, click + at the top of the page.
3. In the "Add Service" window, enter the following information:
   - **Service ID**: Enter an ID for the service.
   - **Service Name**: Enter a name for the service.
   - **Status**: Select the status of the directory connector. The default value is **Activated**.
   - **Pool Name**: Select the directory pool name. To view the detailed information for each registered pool, navigate to **System** > **Integration** > **Directory**.
   - **Service Type**: Select one of the following service type to perform user authentication or user searches on the directory server integrated with EMM.

Classification	Service type	Description
Authentication	Authentication	Makes Authentication requests to a client's directory server. **NOTE** The filter and output fields are automatically entered in accordance with the directory server type.
	User-defined authentication	Makes Authentication requests to a client's directory server. **NOTE** The filter and output fields must be entered manually in accordance with your desired settings.

Classification	Service type	Description
Search	User Search	Searches for user information only. **NOTE** The filter and output fields are automatically entered in accordance with the directory server type.
	Organization Search	Searches for organization information only. **NOTE** The filter and output fields are automatically entered in accordance with the directory server type.
	User-defined search	Searches for desired user information using the filter values entered manually. This information can also be sent to devices.
	Profile Configuration (User information)	Searches for user information using the filter set for the directory connector. To use this type, check if the profile has been set as below: 1. Navigate to the Profile menu. 2. Click the profile name, and then click **Modify Policy** at the bottom. 3. On the “Set Policy” page, click Exchange, Email Account, and VPN by platform. 4. Check if Connector interworking is selected for the user information input method. 5. Check the connector in the User information Connector. For more information on configuring policies, see Configuring policies by device platform.
	Profile Configuration (Certificate information)	Authenticates for a user using the filter set for the directory connector. To use this type, check if the profile has been set as below: 1. Navigate to the Profile menu. 2. Click the profile name, and then click **Modify Policy** at the bottom. 3. On the “Set Policy” page, click Certificate by platform. 4. Check if Connector interworking is selected for the user certificate input method. 5. Check the connector in the User certificate Connector. For more information on configuring policies, see Configuring policies by device platform.

NOTE To authenticate users on devices by selecting Authenticator as globalLdapServiceAuthenticator in **Authentication Setting** under **Setting** > **Server** > **Configuration**, **Select Type** must be selected as **Authentication** or **User-defined authentication** when registering a connector. For more information, see Setting the user authentication method.

- **Base DN**: Click  to open the "Select the Base DN" window and select a starting location for searches in the directory server. Entering a Base DN value can reduce the time required to search for data by limiting searches to a specific location.
  - **Selected DN**: Shows the selected DN (Distinguish Name).
- **Filter**: Click to open the "Select Object Class" window and select an Object Class and attributes for the LDAP Syntax string that will be used to filter search results.
  - **Recommended Properties**: Displays the recommended properties of the selected object class.
  - **Return Value**: Displays the LDAP Syntax of the selected property information and object class.
  - **Default**: Select the object class name defined by default as a filter.
  - **Custom**: Select the object class name defined by connected directory server as a filter.
- **Range**: Select one of the following search range for the directory server based on the specified base DN.
  - **Object**: Within the level of the base DN.
  - **One Level**: Within the level including the sub-level of the base DN.
  - **Subtree**: Within all sub-levels of the base DN.
- **Output Field**: Select one of the following return information range to only extract the desired attributes.
  - **All**: Returns all attributes for the searched entries.
  - **Select**: Returns only the selected attributes for the searched entries. To select the desired properties to be used for the filter, click **Select Property** to open the "Select Property" window and select the desired properties on the loaded attribute list. To apply the selected properties click **Save**.
    -  : Move the selected attributes to the selected properties list.
    -  : Delete the selected attributes from the selected properties list.
    - **Default**: Select the object class name defined by default as a filter.
    - **Custom**: Select the object class name defined by the connected directory server as a filter.

NOTE
- To modify the name of the selected sources and return properties, double-click an item on the "Output Field Settings" field, and then modify it.
- The return property names may not be returned if the modified property names are same as existing property names on the loaded attribute list.

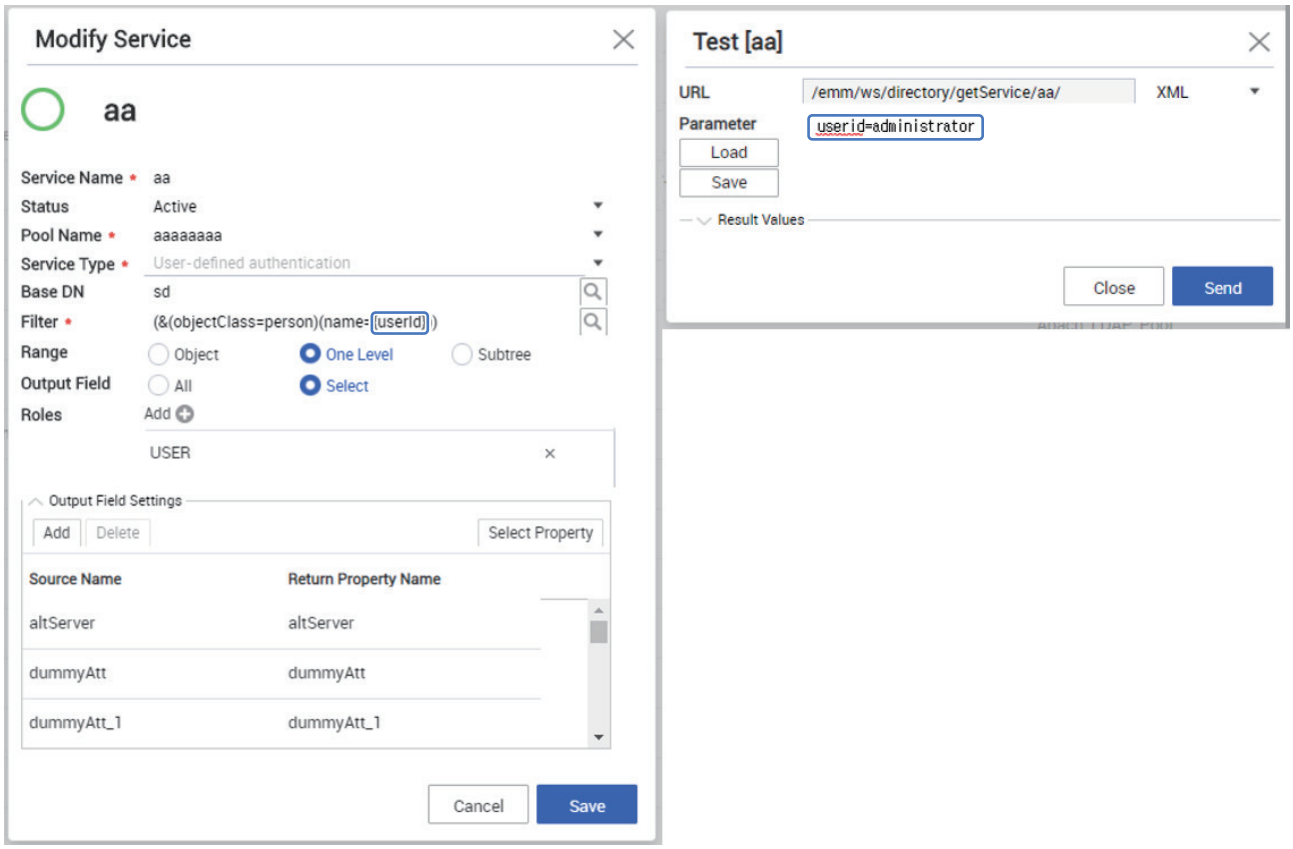
4. Click **Save** to add a directory connector.

Testing a directory service

Before using the directory connector, check if the directory connector operates properly on the directory server.

To test a directory connector, complete the following steps:

1. Navigate to **System** > **Connector** > **Directory**.
2. On the “Directory” page, click in the row of the directory connector that you want to test.
3. In the “Test” window, enter the following information:
   - **URL**: Select the output form from the drop-down list. The URL will be automatically entered for a test when the service is requested.
   - **Parameter**: Enter a parameter key and value (ex. userId=administrator) in the filter.
     - **Load**: Select the desired parameter previously saved in the “Save Input Parameters” window that you want to uses as an input parameter.
     - **Save**: Enter the following information to save an input parameter. If an input parameter is successfully saved, it will be listed in the “Input Value List” window.
       - **Input ID**: Enter an input ID of up to 50 characters containing letters, numbers, and special characters (only dashes and underscores are allowed) to distinguish it from other parameters.
       - **Description**: Enter a description of the input parameter.
       - **Parameters**: Enter a parameter key and value (ex. userId=administrator) in the filter. The test parameter must be identical to the value entered in the service’s filter.



4. Click **Send** to test the service connection, and then view the test results displayed in a tree structure with the results expanded to the last node in the Result Values area.

Copying a directory connector

You can copy an existing directory connector and add a new directory connector to the list.

To copy a directory connector, complete the following steps:

1. Navigate to **System** > **Connector** > **Directory**.
2. On the "Directory" page, click in the row of the specific directory connector that you want to copy information from.
3. In the "Copy Service" window, modify the existing information if necessary, and click **Save**.

Modifying directory connector information

To modify directory connector information, complete the following steps:

1. Navigate to **System** > **Connector** > **Directory**.
2. On the "Directory" page, click in the row of the specific directory connector that you want to modify the information of.
3. In the "Modify Service" window, modify the existing information, and click **Save**.

Deleting directory connectors

To delete directory connectors, complete the following steps:

1. Navigate to **System** > **Connector** > **Directory**.
2. On the "Directory Connector" page, click in the row of the specific directory connector that you want to delete from the list.
3. In the "Delete" window, click **OK**.

Viewing the connector log

EMM manages the usage history of connectors that occur during connector service operations as log information. IT admin can check information, such as user information, device information, connector service type, service request time and response time, using the connector service through connector log information.

To view connector logs for requesting, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Connector Log**.
2. Select the date range you want to search by clicking  on the top left side of the screen. Alternatively you can enter the **User ID** or **Service ID** in the search field and enter or click  .

Tracing activating transactions

To trace a transaction log of a connector service, you have to activate the Connector Service Transaction Log.

To activate the connector service transaction log, follow the settings below:

- Click **Connector Service** under **Setting** > **Server** > **Configuration**, click **Log Service** in the "Connector Service" window, select **Enable the connector service transaction log**, and save it.

Tracking transactions

This function tracks transactions for connector service responses and shows step-by- step processing information for the connector service.

To view the transactions for connector service response, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Connector Log**.
2. Select the date range you want to search by clicking  on the top left side of the screen. Alternatively you can enter the **User ID** or **Service ID** in the search field and enter or click  .
3. Click the item you want to trace from the transaction from the log list, and click  .
4. Click **Transaction Step Status** in the "Transaction Trace" window. Transaction status and transmission data are displayed. Check the sections to figure out the transaction status.

Setting Windows 10

On PC and tablet devices which have Windows 10 installed, EMM controls Wi-Fi, Bluetooth, NFC, and USB ports and sets security policies, such as passwords and factory resets, on profiles to prepare in advance for device loss.

You can prevent information leaks from the company through blocking of the camera and screen capture functions. You can also use company network settings, such as Wi-Fi and VPNs for user devices, exchanges and so on. For more information on policy settings for windows devices, see Configuring Windows Policies.

To set the Open Mobile Alliance Uniform Resource Identifier (OMA-URI), which enables you to control certain functions of a device where Windows 10 is installed, navigate to **System** > **Windows 10** > **CSP Setting Management**. OMA-URI is a standard setting used by equipment manufacturers to control the functions of a PC, tablet, or mobile device. For more information about CSP settings, see the Custom URI settings of Windows 10 system on the Microsoft website.

To register the provisioning package (.ppkg) files for Windows updates for logging into the EMM on a Windows 10 device, navigate to **System** > **Windows 10** > **PPKG File Management**. To create a provisioning package, install the Windows ADK for Windows 10 on the MS website and create a package using Windows ICD. For more information about provisioning packages, see Provisioning package, starting Windows ICD on the Microsoft website.

Configuring CSP settings

The CSP settings are provided by default when EMM is installed. The CSP Setting Management screen displays the default CSP, which is restricted from being modified or duplicated and prohibited from being deleted by user request. IT admin additionally registering, modifying, copying, or deleting CSP is only possible only if the target type is **Device Command**.

- To add, modify, copy or delete CSP settings, see Setting CSP.
- To control the application through a black or white list, see Setting CSP for application control.
- To send CSP to your device, see Deploying CSP to devices.

Setting CSP

To add CSP setting, follow the steps below:

1. Navigate to **System** > **Windows 10** > **CSP Setting Management**.
2. On the “CSP Setting Management” page, click + at the top of the page.
3. In the “Add Configuration Service Provider” window, enter the following information:
   - **Name**: Enter the name of the CSP for controlling the functions of the device.
   - **Target type**: Device Command is selected as the default. (You can only add a Device Command).
   - **Execution type**: Select a CSP Execution type from Read, Add, Replace, Delete, and Exec.
   - **Value type**: Select value types such as string, XML string, date and time, integer, floating point, and Boolean value.
   - **Target Device**: Select the target device to control its functions.
   - **OMA_URI**: Enter the OMA-URI. To initialize, click **Initialization**.
   - **Default Value**: Enter the value if there is a default value.
   - **Description**: Enter simple descriptions and useful related information.

NOTE

- The default CSP configuration items cannot be deleted, but the CSP configuration items can only be modified according to the changes in the OMA_URI settings that are used as standards. Also, beware that if you arbitrarily modify the OMA_URI, the existing functions may not work.
- You can only remove the CSP settings created by the IT admin.
- You can copy an already registered CSP setting and register it additionally, but copying is only possible for the Device Command types of the CSP settings items.

4. Click **Save**.

Setting CSP for application control

To control applications of the Windows AppStore with a black or white list from the AppLocker must have been registered in the CSP settings. The following is a description of the CSP setting for application control. For more information about how to control applications, see Application scenarios for the control with a black or white list.

1. Navigate to **System** > **Windows 10** > **CSP Setting Management**.
2. Enter **AppLocker** in the **OMA_URI** field in the search and click  .
3. Select **AppLocker** from the items, check OMA_URI in the “Modify Configuration Service Provider” window, and then click **Save**.
   - For more information about OMA_URI settings, see the Custom URI settings of Windows 10 system on the Microsoft website.
   - For more information about AppLocker settings, refer to the following Microsoft website below:
     - https://msdn.microsoft.com/en-us/library/windows/hardware/dn920019(v=vs.85).aspx

NOTE Examples of AppLocker CSP used in MS Intune: If the applications you want to control are in the formats of EXE, MSI, Script, StoreApps, or DLL, create a control settings value (XML) via Group Policy in Windows10 PC, and then deploy it to the device.

For more information, see the following:
https://www.petervanderwoude.nl/post/managing-applocker-on-windows-10-via-oma-dm/

Deploying CSP to devices

To deploy the CSP settings for device control on the Windows, follow the steps below:

1. Navigate to **Device**.
2. On the “Device” page, click a checkbox for a device you want to transfer the CSP settings from, and then click **Device Command**.
3. In the “Device Command” window, click the **Custom Control** menu, and then click **Select**.
4. In the “Device Command - Custom Control“ window, select CSP, and then click **Process** to send the CSP settings to the device.
   For more information on how to transfer the device commands, see Sending device commands to devices.

Application scenarios for the control with a black or white list

1. To control the applications of the Windows AppStore, navigate to **Profile**, click **Manage Control App** and register the application to the list. For more information, see Managing applications for specific purposes.
2. On the “Profile” page, click the name of the profile to apply.
3. On the “Profile Detail” page, click **Modify Policy**.
4. Click **Windows** from the device platforms.
5. Click **Application**, then add applications to **Add App Install Black/ Whitelist**, and click **Save**.
6. Navigate to **Devices**, click a checkbox for a device, and then apply the policy with the device command.
   - The application will be controlled according to the policy.
7. To check the applications that are controlled, navigate to **Device**, click a device name and then click the Application tab > Controlled Application tab.

Managing PPKG file

The PPKG file Management explains how to register PPKG files for using Windows ICD on the Microsoft website.

You can manage PPKG files as follows:

- To add, modify, or delete PPKG files, see Setting PPKG file.
- To transmit PPKG files to your device, see Deploying PPKG files to a device.

Setting PPKG file

To add PPKG file, follow the steps below:

1. Navigate to **System** > **Windows 10** > **PPKG File Management**.
2. On the "PPKG File Management" page, click + at the top of the page.
3. Enter the information in the "Add PPKG File" window and click **Save**:
   - **Name**: Enter the provisioning package name.
   - **PPKG File**: Click **Browse**, and select the `.ppkg`.
   - **Purpose**: Select your purpose from Enrollment and Data distribution.
     - In order to log into EMM on a device which has Windows 10 installed, you must register a PPKG file for Enrollment. After registering the Enrollment type, only the Data distribution type can be registered.
   - **Target Device**: Select the target device to which the provisioning package will be applied.

NOTE For 1607 devices on Windows10 platform, the provision package is saved on external SD card. To add the provision package and send it to a device, the external SD card must be installed on the device. For more information, visit https://learn.microsoft.com/en-us/windows/configuration/provisioning-packages/provisioning-packages.

Deploying PPKG files to a device

To deploy the provisioning package (`.ppkg`) files to a device on the Windows, follow the steps below:

1. Navigate to **Setting** > **EMM Application and Policy** > **EMM Client**.
2. On the "EMM Client" page, select **Select the PPKG file** from the **Windows 10 Desktop Data Deployment** or **Windows 10 Mobile Data Deployment** list.
3. Click **Save & Apply** to deploy the profile to the device.

10

Advanced

Advanced

Samsung SDS EMM provides you with more advanced features on the Admin Portal:

Enterprise-Firmware Over The Air (E-FOTA) service

E-FOTA service (for Cloud systems) allows you to manage and configure firmware updates on Samsung devices running Android 7.0 Nougat or higher.

Anti-Malware

EMM provides protection against malware. With Anti-Malware, devices can stay free from any virus or malware. Only the V3 application provided by AhnLab is available for Anti-Malware.

Certificates for applications

External certificates can be added for the different purposes and types on EMM to use network services such as Wi-Fi, VPN, Exchange, and APNs.

Directory server

Samsung SDS EMM provides the Active Directory (AD) service that is built upon the industry-standard Lightweight Directory Access Protocol (LDAP) to access intra-enterprise data by integrating corporate's directory server.

Open API

Open API supports the development of EMM functions, such as providing access to the EMM server, securing the authentication, and easily customizing the application programming and services.

Mobile Admin

EMM's Mobile Admin enables you to conveniently view the service history in a mobile environment and provides essential device management features, helping you to improve productivity at work.

Mail server

Mail servers, such as Microsoft Exchange Server or Office 365, can be integrated and used through EMM on the user's device.

Social distancing

Social distancing monitors the maintenance of social distancing between user devices. In the event of a COVID-19 confirmed case, it helps to track the infection route by determining whether there is contact between users, and helps prevent the spread of infection by sending an alarm message to the contact person.

This chapter explains the following topics:

Managing Enterprise-Firmware Over The Air (E-FOTA)

Samsung SDS EMM supports an Enterprise-Firmware Over The Air (E-FOTA) service that allows you to manage and configure firmware updates on Samsung devices running Android 7.0 Nougat or higher.

To use the E-FOTA service, you must configure E-FOTA settings. For more information see Configuring the E-FOTA settings.

Configuring the E-FOTA settings

To use the E-FOTA service, setting up an E-FOTA license is mandatory. If you do not have a valid E-FOTA license, the E-FOTA license settings menu will not appear in the Admin Portal. Only one E-FOTA license can be registered.

To configure the E-FOTA settings, complete the following steps:

1. Navigate to **Setting** > **License**.
2. On the “License” page, click **E-FOTA Settings**.
3. In the “Add License” page, enter the following information.

Item	License
Type	Select E-FOTA.
License Key	Enter an E-FOTA license.
Total Quantity	When the E-FOTA license key is verified, the number of devices eligible for firmware updates via E-FOTA will be displayed.
Start Date	Select the E-FOTA license execution date. The current date will be displayed by default and can be selected.
Expiration Date	When the E-FOTA License Key is verified, the E-FOTA License Expiration Date will be automatically displayed.
Server information	Enter the E-FOTA server address for calling the API from the E-FOTA server.
Token URL	You need a token to call the API in the E-FOTA server. Enter the URL for a token request.
MDM vendor ID	Enter the vendor ID issued by E-FOTA to use for the E-FOTA service.
Client ID	Enter the access ID for calling APIs from the E-FOTA server.

Item	License
Client Secret	Enter the password for calling APIs from the E-FOTA server.
Customer ID	Enter the Customer ID for the E-FOTA service.

4. To verify the E-FOTA license, click **License** at the bottom of the window.
5. Click **Save**.

Using the E-FOTA

To use the E-FOTA service, register an E-FOTA license in the Admin Portal. For more information on registering an E-FOTA license, see Configuring the E-FOTA settings.

Once you have registered the E-FOTA license in the Admin Portal, the E-FOTA groups organized by device model and carrier are created automatically. You can assign desired devices that need to be updated to an E-FOTA group and update them with the desired firmware version. If you update the firmware of Android Legacy devices to Android10 (SDK 29) or higher, the camera and Wi-Fi policies that have already been applied to the device cannot be canceled.

You must apply a profile with the policy disabled in advance and upgrade the firmware.

Viewing the E-FOTA group list

Navigate to **Advanced** > **E-FOTA** to view all the E-FOTA group information on the "E-FOTA" page. You can also perform the following actions on this page.

Icon	Description
E-FOTA Group Update	Update the E-FOTA group information.
Upload & Deploy File	You can upload the E-FOTA configuration file and deploy it to the devices of groups or organizations. For more information, see Update and deploy E-FOTA configuration file.
Search	Search for a specific group for the entered group model name or carrier code.
Assign Device	Assign devices to the E-FOTA group for firmware updates. For more information, see Assigning devices to an E-FOTA group for firmware updates.
Firmware update setting	Select the firmware update type and specify the firmware version. For more information, see Modifying the firmware update configurations.
Update status per device	View the firmware update status for each device in the E-FOTA group.

Icon	Description
E-FOTA change history	View the change histories of the E-FOTA group. For more information, see Viewing the change histories of E-FOTA groups.

Update and deploy E-FOTA configuration file

After registering or uploading the E-FOTA configuration file, you can deploy it to the devices of groups or organizations. You can register one E-FOTA configuration file for each tenant on the EMM Admin Portal. To run the Samsung E-FOTA application, the device must have the E-FOTA configuration file.

To upload the E-FOTA configuration file or change the groups and organizations to deploy the file, complete the following steps:

1. Navigate to **Advanced** > **E-FOTA**.
2. On the “E-FOTA” page, click **Upload & Deploy File**.
3. In the “Upload & Deploy File” window, enter the E-FOTA configuration file information.
   - Click next to E-FOTA File and select the E-FOTA configuration file to upload.
   - The E-FOTA configuration file has no extension restriction, and files under 500 KB can be registered.
4. To select the groups and organizations to deploy the E-FOTA configuration file to, in the “Upload & Deploy File” window, click **Select** next to the **deployment target**.
   - Select the group on the Group tab in the “Select Group / Organization” window, and select the organization on the Organization tab.
   - To assign the E-FOTA configuration file to the selected groups or organizations, click **OK**.
5. In the “Upload & Deploy File” window, click **Save & Deploy**.
6. In the “Save & Deploy” window, click **OK**.
   - The E-FOTA configuration file will be deployed to the selected groups and organizations on demand. The file is saved in the /Internal Storage/Download/ folder on each device.
   - The information of the groups and organizations that the E-FOTA configuration file is deployed to is not saved in the Admin Portal.

Assigning devices to an E-FOTA group for firmware updates

If there are devices using the same model name and carrier code as the E-FOTA group created on the E-FOTA group list on the “E-FOTA” page, assign the devices to the E-FOTA group for firmware updates.

To assign devices to an E-FOTA group for firmware updates, complete the following steps:

1. Navigate to **Advanced** > **E-FOTA**.
2. On the "E-FOTA" page, click in the row of the E-FOTA group that you want to assign devices to.
3. In the "Assign Device" window, click the checkboxes next to desired devices for firmware update on the device list, and then click to add the selected devices to the device with E-FOTA group list. The selected devices will be added to the device with the E-FOTA group list.
   - To remove the devices on the device with E-FOTA group list, click the checkboxes next to the devices to remove from the device with E-FOTA group list, and then click .
   - To add all the devices to the device with E-FOTA group list, click **Add all**.
   - To remove all the devices on the device with E-FOTA group list, click **Remove all**.
4. Click **Next**.
5. In the "Firmware update" window, select one of the following firmware update types from the drop-down list.
   - **Select**: Allows you to choose to update devices with the target firmware version or not. Users can postpone the firmware update.
   - **Force**: Updates the devices with the target firmware version forcibly at the set time. Users cannot postpone the firmware update.
6. On the firmware version list, select the desired firmware version to apply to the devices, and then click **OK**.
   - Click of the target firmware version to view the detailed information on the target firmware version.
   - If you select **Force** for firmware update type, specify the following information in the "Firmware Scheduling" window.
     - **Start Date**: Click to select a specific date to start the target firmware version update.
     - **Start Time**: Select a specific time to start the target firmware version update.
     - **End Date**: Click to select a specific date to end the target firmware version update.
     - **End Time**: Select a specific time to end the target firmware version update.

NOTE

- The updated date is set to GMT + 0.
- The start date and end date must be at least three days apart and can be up to a maximum of seven days apart. Also, the gap between the start time and the end time must not exceed 12 hours.

Modifying the firmware update configurations

You can modify the set firmware update configurations for each E-FOTA group.

To modify the firmware update configurations, complete the following steps:

1. Navigate to **Advanced** > **E-FOTA**.
2. On the “E-FOTA” page, click  in the row of the E-FOTA group whose firmware you want to modify to update its configuration.
3. In the “Firmware update” window, select one of the following firmware updates type from the drop-down list.
   - **Select**: Allows you to choose to update devices with the target firmware version or not. Users can postpone the firmware update.
   - **Force**: Update the devices with the target firmware version forcibly at the set time. Users cannot postpone the firmware update.
4. On the firmware version list, select the desired firmware version to apply to the devices, and then click **OK**.
   - Click of the target firmware version to view the detailed information on the target firmware version.
   - If you select **Force** for firmware update type, specify the following information on the “Firmware Scheduling” window.
     - **Start Date**: Click  to select a specific date to start the target firmware version update.
     - **Start Time**: Select a specific time to start the target firmware version update.
     - **End Date**: Click  to select a specific date to end the target firmware version update.
     - **End Time**: Select a specific time to end the target firmware version update.

NOTE

- The updated date is set to GMT + 0.
- The start date and end date must be at least three days apart and can be up to a maximum of seven days apart. Also, the gap between the start time and the end time must not exceed 12 hours.

Viewing the firmware update status of devices

You can view the status of firmware updates of the devices in an E-FOTA group.

To view the firmware update status of the devices, complete the following steps:

1. Navigate to **Advanced** > **E-FOTA**.
2. On the “E-FOTA” page, click in the row of the E-FOTA group that you want to view the status of device firmware updates.
3. In the “Update status per device” window, view the detailed update status information for each device, such as the user and device information, OS version, device status, and the detailed result of the firmware updates.
   - Click to send a device command to the filed or unapplied devices for updating the firmware to the target OS version.

Viewing the change histories of E-FOTA groups

You can view the history of changes made to an E-FOTA group.

To view the change histories of an E-FOTA group, complete the following steps:

1. Navigate to **Advanced** > **E-FOTA**.
2. On the “E-FOTA” page, click in the row of the E-FOTA group that you want to view the change histories of.
3. In the “E-FOTA change history” window, view the detailed update information specified for the relevant E-FOTA group and update results on the list. You can also view the log date, update type, target firmware versions, and OS version.

Managing Certificates

Enhance security by using certificates issued by applications. Add external certificates on EMM for the different purposes and types to use network services such as Wi-Fi, VPN, Exchange, and APNs. You can view the details of the issued certificates and delete the invalid ones.

To use the EMM certificate service, certificate authority (CA) must be constructed on a separated server within the company. After interlinking EMM with the CA server by CA adaptor, you can register the CA among Active directory certificate service (ADCS), Generic simple certificate enrolment protocol (SCEP), network device enrolment service (NDES), and CertAgent on EMM. The CA uses a certificate template when issuing a certificate.

Communication certificates

EMM devices communicate with server through a transport layer security (TLS) communication. To check certificates' validation when a device user logs in the EMM Client on device, the EMM Client checks CRL. CRL is checked using two methods. The first method is checking the CA server's CRL directly. The second method is using the online certificate protocol (OCSP) via specifying the URL. For more details about checking the CRL, see Deleting certificates. For communication certificates, both Android and iOS device users can request a certificate update. The server regularly checks a certificates' expiration date and notifies the EMM client when the expiration date is approaching. If the user receives a reissued certificate before the certificate expiration date, the user can use EMM, but if the certificate expires or is revoked, the user must enroll the device again. The Push server or App Tunnel servers regularly check the expiration dates of server certificates, and if the expiration date approaches, the server sends a notice to EMM through alert. IT admins request a certificate from the CA after checking the notice. This chapter describes the overall certificate management: registration, modification, and deletion of certificates.

NOTE For more information about the interlink method between the CA server and EMM, see the Samsung SDS EMM Installation guide.

Authenticating devices using TLS communication

To issue and use certificates for the device, you must integrate EMM with a CA using

an adaptor. For authentication, the device communicates with the EMM server through Transport Layer Security (TLS) communication. This chapter describes how to issue and manage certificates for TLS communication.

Issuing certificates

The EMM server certificates and device certificates must be issued on devices for TLS communication. Certificates for servers, such as Push Server, Push Proxy, AT Relay, and AT Server, are needed.

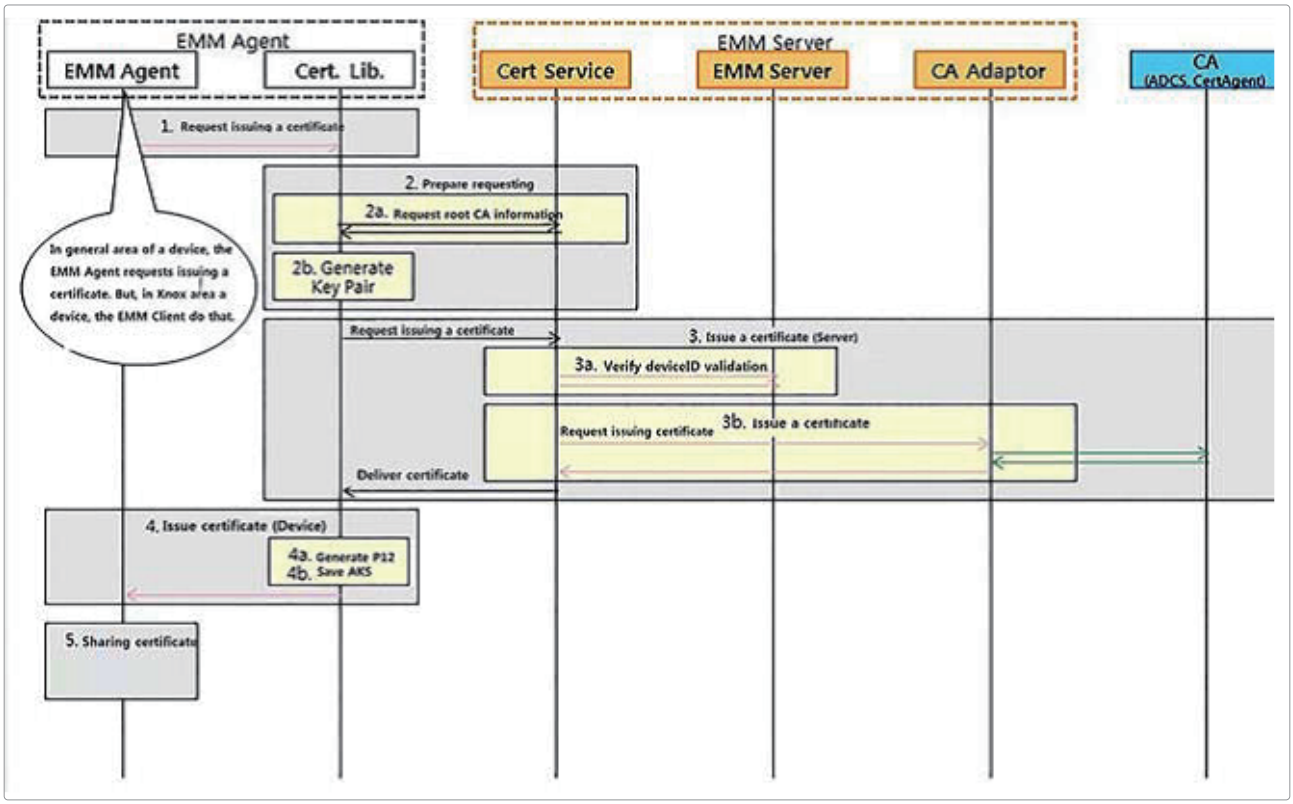
- IT admins need to receive certificates that are issued from the CA.
- IT admins need to save certificates in the JKS file format.

A Certificate for the EMM Device Agent can be issued by a device. To issue a device certificate, complete the following steps:

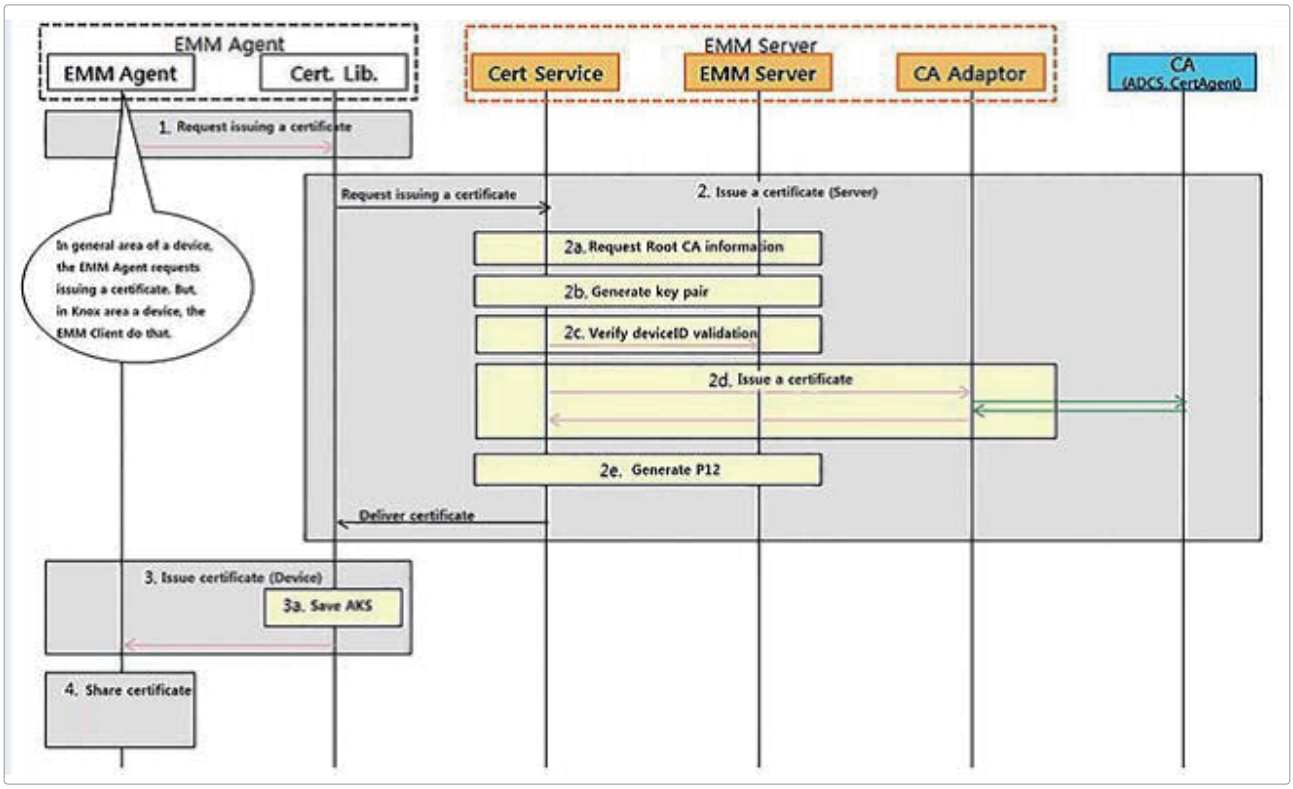
1. After EMM is registered on a device, Public Key and Private Key are generated on the device or server depending on the generation algorithm.

   See the figure below.

   - Key generation flow on a device:



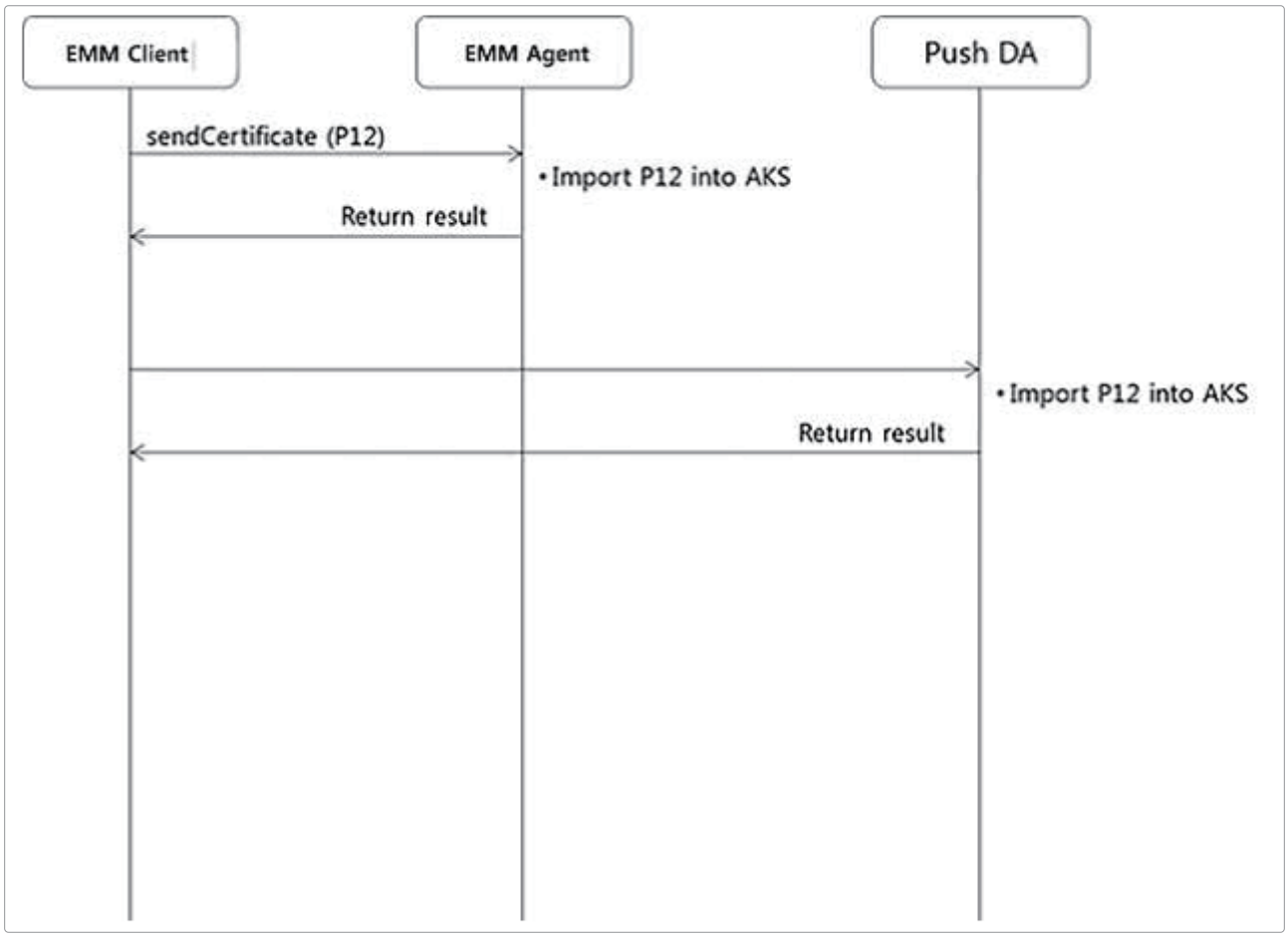
- Key generation flow on the server:



2. Request the certificate for signing and sending the Public Key and Device ID to the EMM server.
3. Check whether or not you can sign in the EMM server, then send a CSR message through the adaptor from the connected CA.
4. Send the Signing Certificate and Root CA Certificate to the devices:
    - The Private Key, Signing Certificate, and Root CA Certificate are stored in the Android KeyStore.

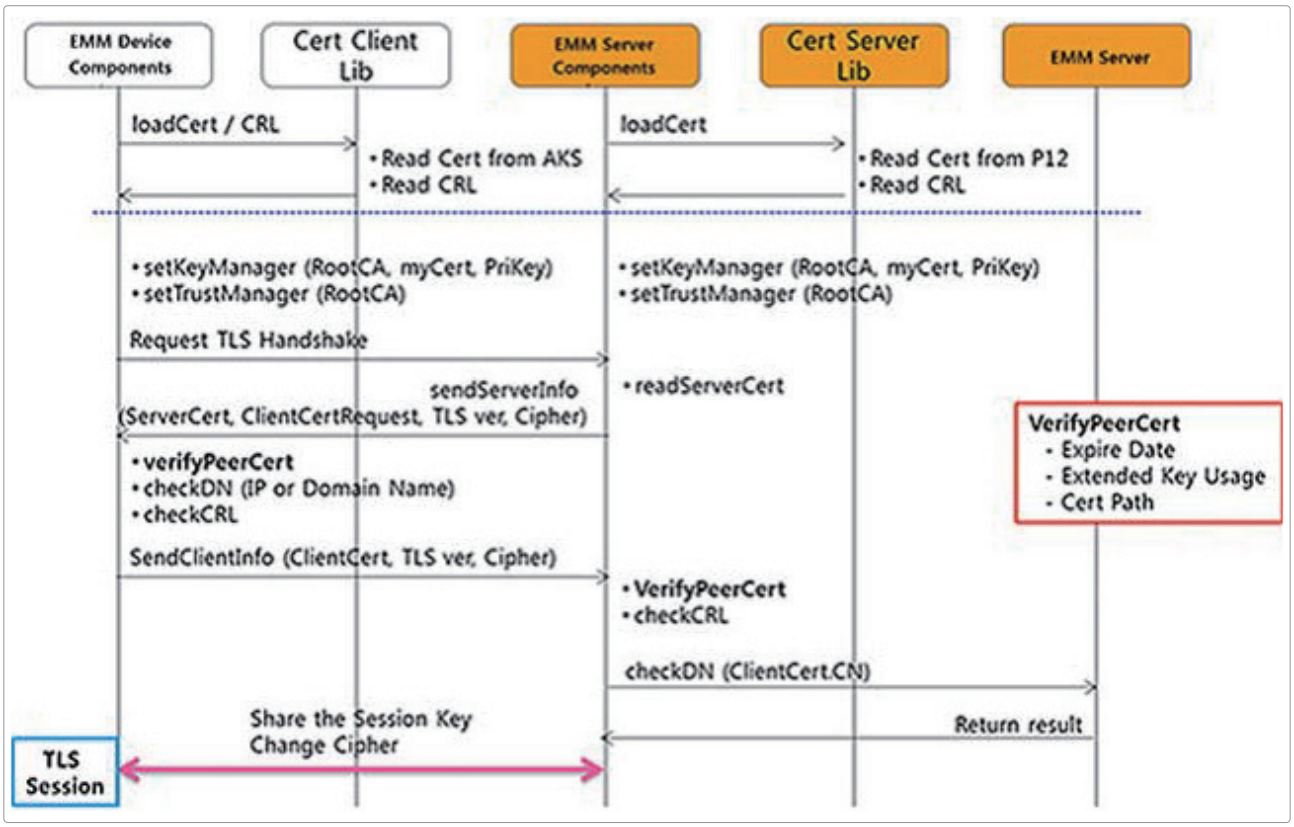
Sharing a certificate on a device

To share a certificate for the device, refer to this diagram.



Establishing TLS communications

To share a certificate on devices, refer to this diagram.



NOTE

- When working with TLS communication, only MS CA can be used.
- The EMM product supports multi level hierarchy CA.
- The EMM product supports multi level hierarchy CA.

Checking certificate validation

The EMM server and devices automatically check the validation of certificates.

1. Self-check: Expire date, basic Constraints, extension Usage.
2. Check Root CA Chain Validation
3. Check the DN (Distinguish Name), including the Device ID:
   - Verifies the information of the owner of peer's certificate for establishing TLS communication. Refer to the following for the flow:
     - Device: Check if the server information to connect (IP or Domain Name) is the same as the CN of the certificate.
     - Server: Check if the owner (CN = Common Name) of the certificate for connection requests is the same as the certificate issued during EMM enrollment.
4. Check CRL. For more information about CRL sync, see Deleting certificates.
   - Verifies if the certificate is revoked when establishing TLS communication.

NOTE The EMM agent receives a renewed certificate for a device before any device certificate expires.

Certificate authority (CA)

Register the Certificate Authority (hereinafter CA) to use the EMM certificate services. Before adding the CA, first download the CA root certificate from a SCEP-supported CA server. This also enables you to issue device certificates and external certificates.

Adding a certificate authority (CA)

To add a CA, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Authority (CA)**.
2. On the "Certificate Authority (CA)" page, click **Add**.
3. In the "Add Certificate Authority" window, enter the following CA information.
   - **CA Name**: Assign a unique name for each CA.
   - **Description**: Enter a description for the CA.

- **CA Type**: Select a CA type. The input information varies depending on the selected CA type.
  - When the CA type is **ADCS**:

Item	Description
Host Name	Enter the CA server host URL address. e.g. http://emm.smartemm.com/
Request Method	Select a method to send the certificate validity check request to the CA. • **CERTSRV**: Validity is checked with the CRL method when logging into the user device. • **URL**: Validity is checked with the OCSP method when logging into the user device.
CA Cert Chain URL	Enter the CA Cert Chain URL address. **NOTE** This field is automatically entered based on the host name if the **CERTSRV** is selected as the request method.
WSURL	Enter the registered Certificate Enrollment Web Service (CES) address to provide web service with the CA.
Key Algorithm	Select a key algorithm type between **EC** and **RSA**.
Key Length	Select a key length. **NOTE** The key length varies depending on the selected key algorithm type.

Auth Method	Select an authentication method from among **User account**, **Windows auth**, or **Certificate**.
	• If the authority method is selected as Windows auth, enter the following additional information:
	  - **Auth. Type**: Select the desired authority type.
	  - **Kerberos Credential Composition**: Select the desired Kerberos credential composition from among **Use Cache Ticket**, **Initial issue**, or **Use keytab**.
	• If the authority method is selected as **Certificate**, enter the following additional information:
	  - **Certificate Type**: Select the desired certificate type.
	  - **Certificate KeyStore**: Click **Browse** and then select the certificate KeyStore.
	  - **KeyStore Password**: Enter the KeyStore password.

User ID	Enter the EMM user ID.
Password	Enter the password for the user ID.
Workstation	Enter the workstation information.
Domain	Enter the domain name that is used on EMM.

Item	Description
Certificate Type	Select a certificate type. **NOTE** This field appears only when **Certificate** is selected as the authentication method.
Certificate KeyStore	Click **Browse** and select a certificate file in the CER, DER, PFX, or P12 format. **NOTE** This field appears only when **Certificate** is selected as the authentication method.
KeyStore Password	Enter the password for the uploaded certificate KeyStore file. **NOTE** This field appears only when **Certificate** is selected as the authentication method.

- When the CA type is **Generic SCEP** or **NDES**:

Item	Description
SCEP URL	Enter the SCEP IP or URL to send the certificate validity check request to the CA. e.g. http://emm.smartemm.com/certsrv/mscep/mscep.dll
Key Algorithm	Only **RSA** is supported when Generic SCEP and NDES CA types are selected.
Key Length	Select a key length from among **2048**, **3072**, or **4096**.
Challenge Type	Select a challenge type to authenticate the selected CA type. • **Dynamic**: Enter the information used on the EMM server for authentication configuration. • **Static**: Enter the challenge password. • **No Challenge**: If no challenge is selected the challenge password is not required. **NOTE** The **Dynamic** field is enabled only when the NDES type CA is selected.
User ID	Enter the EMM user ID. **NOTE** This field appears only when **Dynamic** is selected as the challenge type.
Password	Enter the password for the user ID. **NOTE** This field appears only when **Dynamic** is selected as the challenge type.

Item	Description
Domain	Enter the domain name that is used on EMM. **NOTE** This field appears only when **Dynamic** is selected as the challenge type.
Challenge URL	Enter the challenge URL address used on EMM.
Challenge Password	Enter the same password used for the authentication password. **NOTE** This field appears only when **Static** is selected as the challenge type.
Retry Count	Select a maximum number of retry to issue certificates. **NOTE** • The default value is set to 5. • The retry count value can be between 1 – 10 times.

- When the CA type is **CertAgent**:

Item	Description
RAMI URL	Enter the RAMI IP address or URL to send the certificate validity check request to the CA. e.g. http://emm.smartemm.com/certagentadmin/ca/rami
Key Algorithm	Select a key algorithm type between **EC** and **RSA**.
Key Length	Select a key length. **NOTE** The key length varies depending on the selected key algorithm type.
CA Account	Enter the CA account ID.
Certificate KeyStore	Click **Browse** and select a certificate file in the CER, DER, PFX or P12 format.
KeyStore Password	Enter the password for the uploaded certificate KeyStore file.

- When CA type is **EST**:

Item	Description
Host Name	Enter the CA server host URL address.
Port	Enter the CA server host port number.
Use proxy	Click the **Use proxy** checkbox to enable proxy use for the CA server.

Item	Description
CA Label	Enter the CA server label. **NOTE** Contact Samsung SDS EMM Technical Support for the CA label.
Key Algorithm	Select a key algorithm type between **EC** and **RSA**.
Key Length	Select a key length. **NOTE** The key length varies depending on the selected key algorithm type.
Challenge Password	Enter the password for the CA server authentication.
Auth Method	Select an authentication method between **User account** and **Certificate**.
User ID	Enter the EMM user ID.
Password	Enter the password for the user ID.
Certificate KeyStore	Click **Browse** and select a certificate file in the CER, DER, PFX or P12 format. **NOTE** This field appears only when **Certificate** is selected as the authentication method.
KeyStore Password	Enter the password for the uploaded certificate KeyStore file. **NOTE** This field appears only when **Certificate** is selected as the authentication method.

- **Test Connection**: Click to check if the entered CA information connects to the CA server successfully.

NOTE To add a CA, you must pass the connection test.

- **Managing CA**: Select a CA server name from the root CA list.

4. Click **Save**.

Viewing a certificate authority (CA)

Navigate to **Advanced** > **Certificate** > **Certificate Authority (CA)** to view all the CA information on the "Certificate Authority (CA)" page.

To view the detailed information of a specific CA, click the CA name of a specific CA on the list.

You can also perform the following actions on this page:

Action	Description
Add	Add the CA in the Admin Portal. For more information, see Adding a certificate authority (CA).
Modify	Modify the selected CA. For more information, see Modifying a certificate authority (CA).
Delete	Delete the selected CA. For more information, see Deleting a certificate authority (CA).

Modifying a certificate authority (CA)

To modify a CA, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Authority (CA)**.
2. On the "Certificate Authority (CA)" page, select one from the list you want to modify and click **Modify**.
3. In the "Modify Certificate Authority" window, modify the CA information. The information varies depending on the selected CA type.

NOTE You can register a new root certificate when modifying the CA.

4. Click **Save**.

Deleting a certificate authority (CA)

To delete a CA, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Authority (CA)**.
2. On the "Certificate Authority (CA)" page, select one from the list you want to delete and click **Delete**.
3. In the "Delete Certificate Authority" window, click **OK**.

NOTE You can delete the CA only when there is no template in use.

Certificate templates

The CA server manages certificates through certificate templates. You can add multiple templates and modify them to standardize and simplify the process of issuing certificates. In the high security version, a certificate template of the EMM type, which is an end user certificate template, must be registered.

Adding certificate templates

To add a certificate template, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Template**.
2. On the "Certificate Template" page, click **Add**.
3. In the "Add Certificate Template" window, enter the following information:
   - **Template Type**: Select one of the following template types.
     - **External**: Issues Wi-Fi, VPN and Exchange certificates.
     - **EMM**: Authenticates EMM device users. When all device platforms are selected, it is registered as one certificate template.
   - **Template Name**: Assign a unique name for each certificate template.

   NOTE
   - When creating an external template, enter a template name manually.
   - When creating an EMM templates, the template name is set to EMM_DEVICE_CERT and you cannot modify it.

   - **Platform**: Select a device platform for the certificate template.

   NOTE Depending on the device platform, the certificate usage type varies.

   - **Description**: Enter a description for the certificate template.
   - **CA**: Select a CA type. Input information varies depending on the selected CA type.
   - **CA Template Name**: Enter the CA template name. The CA template name is required when ADCS type CA is selected.
   - **Profile ID**: Enter the profile ID. The profile ID is required when CertAgent type CA is selected.

   NOTE A master profile will be used for an empty value.

   - **CA Label**: Enter the CA label. The CA label is required when EST type CA is selected.

   NOTE The label of the selected CA will be used for an empty value.

- **Subject Name**: Enter a subject name in a CN = {Subject name value} format. For an EMM type template, CN = {deviceID} is set automatically and the certificate usage is disabled.

> **NOTE** You can also click **Lookup** to open the reference item list and select an item from it. The reference value will be automatically entered.

- **Certificate Usage**: Select a certificate usage type.
  - **Wi-Fi**: Authorizes connecting with AP for Wi-Fi.

    > **NOTE** The device configuration for Wi-Fi needs to be checked if **Wi-Fi** is selected as the certificate usage.

  - **VPN**: Authorizes encrypted VPN communication when registering EMM on devices.

    > **NOTE** The device configuration for VPN needs to be checked if **VPN** is selected as the certificate usage.

  - **Exchange**: Authorizes user authentication and services in Exchange.
  - **Knox Generic VPN**: Authorizes encrypted VPN communication for Knox enabled Android devices.

    > **NOTE** The device configuration for VPN needs to be checked if **Knox Generic VPN** is selected as the certificate usage.

  - **Knox VPN**: Authorizes encrypted VPN communication specialized for Samsung devices.
- **SAN Type**: Select a SAN type, and then enter the SAN value. Then click **+** to add.

> **NOTE** You can also click **Lookup** to open the reference item list and select a SAN reference item from it. The reference value will be automatically entered.

4. Click **Save**.
5. In the “OK” window, click **OK**.

Viewing certificate templates

Navigate to **Advanced** > **Certificate** > **Certificate Template** to view all the template information on the "Certificate Template" page.

- To view the detailed information of the specific certificate template, click a template name from among the certificate templates on the list.
- To view the detailed information of the specific CA, click a CA from among the certificate templates on the list.

You can also perform the following actions on this page:

Action	Description
Add	Add the certificate template in the Admin Portal. For more information, see Adding certificate templates.
Search	Search for a specific certificate template for the entered template name.
Modify	Modify the selected certificate template. For more information, see Modifying certificate templates.
Delete	Delete the selected certificate template. For more information, see Deleting certificate templates.

Modifying certificate templates

To modify a certificate template, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Template**.
2. On the "Certificate Template" page, select one from the list and click **Modify**.
3. In the "Modify Certificate Template" window, modify the certificate template information.
   - **Template Type**: Only **External** is supported.
   - **Template Name**: Assign a unique name for the certificate template.
   - **Platform**: Select a device platform from among **Android** or **iOS**.
   - **Description**: Enter a description for the certificate template.
   - **CA**: Select a CA type. Input information will vary depending on the selected CA type.
   - **CA Template Name**: Enter the CA template name. The CA template name is required when ADCS type CA is selected.

- **Profile ID**: Enter the profile ID. The profile ID is required when CertAgent type CA is selected.

> **NOTE** A master profile will be used for an empty value.

- **CA Label**: Enter the CA label. The CA label is required when EST type CA is selected.

> **NOTE** The label of the selected CA will be used for an empty value.

- **Subject Name**: Enter a subject name in a CN ={Subject name value} format.

> **NOTE** You can also click **Lookup** to open the reference item list and select an item from it. The reference value will be automatically entered.

- **Certificate Usage**: Select a certificate usage type.
  - **Wi-Fi**: Authorizes connecting with AP for Wi-Fi.

    > **NOTE** The device configuration for Wi-Fi needs to be checked if **Wi-Fi** is selected as the certificate usage.

  - **VPN**: Authorizes encrypted VPN communication when registering EMM on devices.

    > **NOTE** The device configuration for VPN needs to be checked if **VPN** is selected as the certificate usage.

  - **Exchange**: Authorizes user authentication and services in Exchange.
  - **Knox Generic VPN**: Authorizes encrypted VPN communication for Knox enabled devices.

    > **NOTE**
    > - This field appears only when **Android** is selected as the device platform.
    > - The device configuration for VPN needs to be checked if **Knox Generic VPN** is selected as the certificate usage.

  - **Knox VPN**: Authorizes encrypted VPN communication specialized for Galaxy devices.

    > **NOTE** This field appears only when **Android** is selected as the device platform.

- **SAN Type**: Select a SAN type and then enter the SAN value. Then click **+** to add.

> **NOTE** You can also click **Lookup** to open the reference item list and select a SAN reference item from it. The reference value will be automatically entered.

4. Click **Save**.
5. In the “OK” window, click **OK**.

Deleting certificate templates

To delete certificate templates, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificate Template**.
2. On the “Certificate Template” page, select one from the list and click **Delete**.
3. In the “Delete Certificate Template” window, click **OK**.

NOTE You can delete the template in use only when the Android and iOS settings have been deleted from the device management profile.

External certificates

External certificates are used in the Profile settings for user authentication configuration. Register an external certificate and manage it in EMM without receiving a certificate issued from the CA.

Only CER, DER, PFX or P12 type external certificate files can be registered. Among these, only the FIPS 140-2 compliant certificate is supported, when registering a PKCS#12 type external certificate. If an error occurs while registering an external certificate file, check if the file complies with the FIPS Compliant and register after conversion, if necessary.

NOTE

- APNs certificate, which authorizes the Apple Push Notification services, can be viewed but not registered. For more information about registering APNs certificates, see Setting a APNs certificate (iOS only).
- Starting from EMM v2.4.1, the iOS external certificate is not necessary for using the iOS EMM Client.

Adding external certificates

To add an external certificate, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **External Certificate**.
2. On the “External Certificate” page, click **Add**.
3. In the “Add External Certificate” window, enter the following information:
   - **Name**: Assign a unique name for each external certificate.
   - **Purpose**: Select a purpose for the external certificate.
     - **Wi-Fi**: Authorizes connecting with AP for Wi-Fi.

NOTE The device configuration for Wi-Fi needs to be checked if **Wi-Fi** is selected as the external certificate purpose.

- **Knox VPN**: Authorizes encrypted VPN communication specialized for Galaxy devices.
- **VPN**: Authorizes encrypted VPN communication when registering EMM on devices.

> **NOTE** The device configuration for VPN needs to be checked if **VPN** is selected as the external certificate purpose.

- **Exchange**: Authorizes the user authentication and services in Exchange.

> **NOTE** If **Exchange** is selected as an external certificate purpose, the certificate type is automatically selected as **User**.

- **CA Cert**: Issued by the CA as requested by the user's public key.
- **Knox Generic VPN**: Authorizes encrypted VPN communication for Knox enabled devices.

> **NOTE** The device configuration for VPN needs to be checked if **Knox Generic VPN** is selected as the external certificate purpose.

- **Supervision Certificate**: Authorizes iOS device pairing to use the remote detection mode.

> **NOTE** If **Supervision Certificate** is selected as an external certificate purpose, the certificate type is automatically selected as **Server**.

- **Type**: Select a type for the external certificate.
  - **Root**: Highest level of certificate that identifies the Root CA (Certificate Authority).
  - **User**: Certificate issued for general purposes, such as devices or applications.
  - **Server**: Server certificate for general purposes.
- **File**: Click **Browse** and select a certificate file.

> **NOTE**
> - Only the CER, DER, PFX or P12 type external certificate file is supported.
> - Only the FIPS 140-2 compliant certificate is supported, when registering a PKCS#12 type external certificate.

- **Password**: Enter the password of the selected certificate.
- **Description**: Enter a description for the external certificate.
- **Revoked**: The certificate has expired and has been revoked by EMM.

4. Click **Save**.

Viewing external certificates

Navigate to **Advanced** > **Certificate** > **External Certificate** to view the external certificate information on the “External Certificate” page.

You can also perform the following actions on this page:

Action	Description
Add	Add an external certificate to the Admin Portal. For more information, see Adding external certificates.
Search	Search for a specific external certificate by entering its name.
Modify	Modify the selected external certificate. For more information, see Modifying external certificates.
Delete	Delete the selected external certificate. For more information, see Deleting external certificates.

Modifying external certificates

Modify external certificates by renewing the currently registered external certificate file with a new file.

NOTE

- The use and type of the external certificate cannot be modified.
- APNs certificates cannot be modified.

To modify an external certificate, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **External Certificate**.
2. On the “External Certificate” page, select one from the list and click **Modify**.
3. In the “Modify External Certificate” window, modify the following external certificate information if necessary:
   - **File**: Click **Browse** and select a certificate file.

NOTE

- Only the CER, DER, PFX or P12 type external certificate file is supported.
- Only the FIPS 140-2 compliant certificate is supported, when registering a PKCS#12 type external certificate.

   - **Password**: Enter the password for the selected certificate.
   - **Description**: Enter a description for the modified external certificate.
4. Click **Save**.

Deleting external certificates

To delete an external certificate, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **External Certificate**.
2. On the “External Certificate” page, select one from the list and click **Delete**.
3. In the “Delete” window, click **OK**.

NOTE APNs certificates and certificates in use cannot be deleted.

Viewing certificates issuing history

Navigate to **Advanced** > **Certificate** > **Certificates Issuing history** to view a history of all issued certificates. Issued certificates can be renewed upon expiration or user request. For Android devices, users can update certificates. For iOS devices, certificates are automatically updated by the CA server.

The certificate statuses of the issued certificates on EMM are as follows:

- **Generated**: The certificate has been successfully issued and is currently in use.
- **Deleted**: The certificate is deleted by the IT admin and cannot be used on EMM.
- **Revoked**: The certificate has expired and has been revoked from the CA server.

You can also perform the following actions on this page:

Action	Description
Delete	Delete the selected certificates used on iOS devices. For more information, see Deleting certificates.

Deleting certificates

You can delete certificates used on the iOS devices, which are saved and then distributed from the EMM server, unlike other device platforms. To delete a certificate, complete the following steps:

1. Navigate to **Advanced** > **Certificate** > **Certificates Issuing history**.
2. On the "Certificate Issuing history" page, click  to set an issued period.
3. Select one from the list you want to delete and click **Delete**.

NOTE Certificates used on devices other than iOS cannot be deleted.

4. In the "Delete" window, click **OK**.

Checking certificate validation

The EMM server and devices automatically check the validation of certificates.

1. Self-check: Expire date, basic Constraints, extension Usage.
2. Check Root CA Chain Validation
3. Check the DN (Distinguish Name), including the Device ID:
   - Verifies the information of the owner of peer's certificate for establishing TLS communication. Refer to the following for the flow:
     - Device: Check if the server information to connect (IP or Domain Name) is the same as the CN of the certificate.
     - Server: Check if the owner (CN = Common Name) of the certificate for connection requests is the same as the certificate issued during EMM enrollment.
4. Check CRL. For more information about CRL sync, see Deleting certificates.
   - Verifies if the certificate is revoked when establishing TLS communication.

NOTE The EMM agent receives a renewed certificate for a device before any device certificate expires.

Checking the certificate revocation status

The certificate revocation list (CRL) is a list of revoked or invalid certificates. When the EMM clients requests certificate validation, the EMM server checks whether the certificate has revoked and is valid by checking the CRL list of the CA server. For this, EMM checks the CRL distribution point (CDP) and provides an OCSP checking method to check the CDP. The OCSP method is an online certificate status protocol, which enables the CA server to check the CRL through a specified URL to check certificates on a real time basis. The OCSP method supports HTTP and HTTPS methods. You can specify several OCSP URLs at certificate. In this case, the server checks the URL in the URL order to check the certificate's validity. If the connection time for OCSP URL exceeds this, the connection process stops. In the following cases, certificates are revoked and included on the CRL list.

Revoked	Hold
Certificates are revoked if anyone of the following situations arise: • Private key of certificate is exposed or is expected to be exposed. • The private key of the CA is exposed or is expected to be exposed. • The certificate has been issued illegally. • The certificate owner is no longer found to be trustworthy. • Name of certificate owner changes. • The private key of certificate owner is exposed or is expected to be exposed.	Certificates become temporarily invalid in the following situations: • In case a device user has no confidence in forgetting the user's own private key, this certificate is kept. • If the private key is found later and someone doesn't have access to that private key, the certificate becomes valid and is excluded from the CRL.

Checking the CRL by the OCSP method

When a device communicates with TLS, the device attempts to connect the OCSP URLs in order which are specified on the certificate and then the connected URL verifies the CA server's CRL to check certificate validation. If the trial time for the connection exceeds 3 seconds, this connection expires. The OCSP supports the HTTP and HTTPS methods. For more detailed information about TLS communication, see Authenticating devices using TLS communication.

- In case the URL checks the CRL successfully: the Certificate is revoked. The requested TLS communication fails.
- If the URL cannot check the CRL: Try to connect to the next URL and check it.
- If the URL does not connect for 3 seconds: the Certificate is deemed valid.

Monitoring Social Distancing

Social distancing monitoring helps to curb the spread of COVID 19 and saves contact history between devices so that you can quickly check whether you have come into contact with an infected person. This can prevent further infections. If the user has been in contact with a confirmed patient for more than a certain period of time, the contact will be notified and instructions will be provided.

To monitor social distancing, Social Distancing Service must be set to Use in the Social Distancing category of **Setting** > **Server** > **Configuration** to display the Social Distancing menu on the EMM Admin Portal. Only Android Legacy devices or Android Enterprise Fully Managed type devices that are registered in the EMM Admin Portal can be monitored for their functions. If the user forcibly turns off Bluetooth on the device, social distancing between device users cannot be monitored. To monitor user distancing in the high-security version, at least one profile must be applied to the device. Only device information detected within the maximum measured distance between devices (Meters) between devices will be collected. For more information, see List of environment settings.

Viewing the social distancing list

To check the list of devices that are equipped with the social distancing function, complete the following steps.

1. Navigate to **Advanced** > **Social Distancing**.
2. On the “Social Distancing” page, enter the Device Name, User ID/Name, and Collected Date, and click **Search**.
   - **Collected Date**: Select the period for collecting social distancing information from the device. You can only select up to 15 days before the current date.
3. Check the following information in the social distancing list.
   - **Status**: Shows the device status.
   - **Number of Contacts**: Shows the total number of devices contacted by the device based on the collection date. You can only send notifications to active contacts when the Number of Contacts is available. If there is no data collection information, for reasons such as communication not being possible on the device, it will be displayed as “-”.
   - Click **See History** to check detailed information on the number of contacts. Device information and distance contacted by a specific device during the collection period set in the “Contacts History” window are displayed as a history. It is displayed based on the Maximum measured distance between devices (Meters) set by the IT admin in Configuration.

Sending social distancing notifications

In the event of a confirmed COVID-19 case, a notification message can be sent to users who have come into contact with infected people.

To send notifications to users who have come into contact with infected people, complete the following steps:

1. Navigate to **Advanced** > **Social Distancing**.
2. On the “Social Distancing” page, select a device and click **Send Notification**.

   Because each devices is counted separately, If a user has multiple devices, you must check them all. You can send notifications only when the contact’s device status is active.
3. In the “Send Notification” window, enter the Title and Message and click **OK**.

   A notification is sent to the contacted contact when you click See History in the device list.

Configuring Microsoft Exchange

Mail servers, such as the Microsoft Exchange Server and Office 365, can be integrated with Samsung SDS EMM on user's devices. To integrate a mail server with EMM, you should access and configure the Microsoft Exchange Server by authenticating user information in the Active Directory (AD) service based on a certificate issued by a Certificate Authority (CA). Before configuring Exchange, the following items must be configured and prepared:

- Active Directory (AD) service (For more information on configuring the AD service, see Integrating a directory server.)
- Certification Authority (CA) server (The client certificate must be issued for authentication.)
- Microsoft Exchange server (To use certificate based authentication in the Microsoft Exchange server, visit the Microsoft website at https://technet.microsoft.com/EN-US/library/mt791265(v=exchg.160).aspx and follow the instructions.)
- Registered user accounts and organizations (For more information on configuring the AD service, see Creating user accounts and Adding an organization.)

Configuring the Exchange server

To configure the Exchange server by authenticating the users on the devices with Exchange ActiveSync, additional settings are required for Certificate Authentication (CA), SSL, and client certificates.

Enabling Certificate Authentication (CA)

Active Directory Client Certificate Authentication must be enabled to configure Certificate Authentication.

To configure Certificate Authentication (CA), complete the following steps:

1. On your desktop, click **Start** > **Run**.
2. Type `inetmgr`, and then click **OK** to open the Internet Information Services (IIS) Manager.
   - Alternately, on your desktop, you can click **Start** > **Programs or All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager** to open the Internet Information Services (IIS) Manager.

3. In the **Connections** node, select the name of your web server, and then double-click **Authentication** in the “IIS” section.

4. Double-click **Active Directory Client Certificate Authentication**, and then click **Enable** in the “Actions” window.

Enabling SSL

After enabling Active Directory Client Certificate Authentication, the SSL must be enabled to use Active Directory Client Certificate Authentication.

To enable SSL, complete the following steps:

1. On your desktop, click **Start** > **Run**.

2. Type `inetmgr`, and then click **OK** to open the Internet Information Services (IIS) Manager.
   - Alternately, on your desktop, you can click **Start** > **Programs or All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager** to open the Internet Information Services (IIS) Manager.

3. In the **Connections** node, select **Microsoft-Server-ActiveSync** under **Default Web Site**, and then double-click **SSL Settings** in the “IIS” section.

4. Click the checkbox next to **Require SSL**, and then click **Require** under **Client certificates**.

5. Click **Apply** in the “Actions” window.

Configuring client certificate mapping

Configure client certificate mapping after enabling Certificate Authentication and applying SSL.

To configure client certificate mapping, complete the following steps:

1. On your desktop, click **Start** > **Run**.

2. Type `inetmgr`, and then click **OK** to open the Internet Information Services (IIS) Manager.
   - Alternately, on your desktop, you can click **Start** > **Programs or All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager** to open the Internet Information Services (IIS) Manager.

3. In the **Connections** node, select **Microsoft-Server-ActiveSync** under **Default Web Site**, and then double-click **Configuration Editor** in the “IIS” section.

4. From the Section drop-down menu, navigate to **system.webServer/security/authentication**.

5. Select **True** in the “enabled” section, and then click **Apply** in the “Actions” window.

Configuring ADCS and AD for Microsoft Exchange

To configure ADCS and AD for Exchange, some specific settings for the use of Exchange are required when creating a directory server, directory connector, Certificate Authentication (CA), and certificate template.

To configure ADCS and AD for Exchange, complete the following steps:

1. Add a directory server for accessing intra-enterprise data on the AD server. For more information about entering information in detail, see Adding a directory server.

2. Add a directory connector for specific filtered searches. For more information about entering detailed information, see Adding a directory connector.

NOTE If the service type is selected as **Profile Configuration**, the policy of the user information input method must be selected as **Connector interworking**. For more information on configuring policies, see Configuring policies by device platform.

3. Add a certificate authority (CA) for authenticating the users. For more information about entering information in detail, see Adding a certificate authority (CA).

NOTE Once a connection test is completed, the target CA that issues and manages the relevant certificates is displayed.

4. Add a certificate template. For more information about entering information in detail, see Adding certificate templates. Also, for Exchange settings, the following must be done.
   - The subject name must be selected as **CN = (Email)**.
   - The certificate usage must be selected as **Exchange**.
   - The San type must be selected as **Email Address** and click  to select **Email** from the SAN reference item list.

Configuring a profile for Microsoft Exchange

Configure a profile for Exchange using a certificate authority (CA) or a certificate connector. Some specific settings for using Microsoft Exchange are required when creating a profile.

To configure a profile using a CA or certificate connector, complete the following steps:

1. Create a new profile. For more information about entering information in detail, see Creating a new profile.

2. Configure policies by device platform. For more information about entering information in detail, see Configuring policies by device platform. Also, for the Exchange policy, the following must be done.

   - Click the checkbox next to **Office 365** to configure the Exchange settings by automatically filling out the Exchange server address and the setting the SSL option to **Use**.
   - Set the user information input method to **Connector interworking** to use a directory connector. For more information about creating a directory connector, see Adding a directory connector.
   - Select one of the user certificate input methods.
     - **Issuing external CA** (Using a CA): Select the certificate template. For more information about creating a certificate template see Adding certificate templates.
     - **Connecting interworking** (using a certificate connector): Select the certificate connector. For more information about creating a certificate connector, see Adding a directory connector.

NOTE To enable a certificate connector, the service type of the directory connector must be set as Profile Configuration (Certificate). For more information about selecting the service type, see Adding a directory connector.

   - Select **Use** for use of SSL to configure the SSL between the device and the Exchange server.

Accessing Microsoft Exchange on the device

After all the settings for Exchange are completed through the Internet Information Services (IIS) Manager and Admin Portal, access and use Exchange on the device.

To access Exchange on the device, complete the following steps:

1. On the EMM application, tap **Download Configuration** from the side menu, and then tap **Install** to download the Exchange configuration for the device. The user certificate for Exchange will be installed on the device.

NOTE To install the Exchange configuration, the EMM user ID must be same as the user ID of the AD server.

2. Tap the notification to set up the new email account.
3. Accept the privacy policy and activate the device user, and then check if the email account has been added to the Samsung Email application.

NOTE The user's email address that is registered in the Admin Portal is used as the email account for the Exchange server.

Using Anti-Malware

EMM provides protection against malware. With Anti-Malware, devices can stay free from any virus or malware. Only the V3 application provided by AhnLab is available for Anti-Malware. Before using Anti-Malware, you must purchase a V3 license and register it in the Configuration menu.

You can register the V3 engine server and the V3 license file for Anti-Malware and set up the engine update or scan interval.

Configuring the Anti-Malware settings

To configure the Anti-Malware settings, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. On the “Configuration” page, click **Anti-Malware** at the top of the page.
3. In the “Anti Malware” window, enter the following information:
   - **Anti-Malware Settings**: Allows configuration of the Anti-Malware settings.
   - **Local Download Server**: Set it to use a local server to download a V3 engine.
     - **Use**: Downloads the V3 engine from the engine update server specified in **Engine Update Server Address**. The server must also be configured after the EMM server is installed.
     - **Do not use**: Uses a Content Delivery Network (CDN)-based engine download server on the Internet.
   - **Engine Update Server Address**: Enter the address of the engine update server.
   - **Upload License**: Click  and select a V3 license file to upload. Only DAT files can be uploaded.
     - **Expiration Date**: Select the expiration date of the uploaded license to display the remaining period for the Anti-Malware software in the “License Status” area on the “Dashboard” page.
   - **Engine Update Interval**: Set the engine update interval. You can select the days and set the start time, and time zone.
   - **Malware Scan Interval**: Set the malware scan interval. You can select the days and set the start time and time zone.
   - **Automatic Malware Deletion**: Allows for the automatic deletion of scanned malware.
4. Click **Save**.

Configuring the Anti-Malware engine

Once the V3 setup has been completed in the Configuration menu, upload the downloaded V3 engine to **Advanced** > **Anti-Malware** > **Engine Update** and update V3 on the user device to the latest version.

Uploading an engine file

To upload an engine file to the Admin Portal, complete the following steps:

1. Navigate to **Advanced** > **Anti-Malware** > **Engine Update**.
2. On the "Engine Update" page, click **Upload Engine**.
3. In the "Upload Engine File" window, click  and select a V3 engine zip file (Max. 300MB) to upload.
   - Only ZIP files can be uploaded.
4. Click **Save**.
5. In the "Save Engine File" window, click **OK**.
   - The latest version information that appears next to the Upload Engine button will be updated when the upload completes.

Updating the Anti-Malware engine

To update the Anti-Malware engine, complete the following steps:

1. Navigate to **Advanced** > **Anti-Malware** > **Engine Update**.
2. On the "Engine Update" page, click the devices you want to update the engine of.
3. Click **Update**.
4. In the "Engine Update" window, click **OK**.
   - You can set the engine update interval to automatically perform regular engine updates based on a predefined schedule. For more information, see Configuring the Anti-Malware settings.

NOTE If the update status is "Failed" after updating the Anti-Malware engines, hover the mouse over ⓘ to view the reason.

Exporting the engine update list

To export the engine update list, complete the following steps:

1. Navigate to **Advanced** > **Anti-Malware** > **Engine Update**.
2. On the “Engine Update” page, click **Export to CSV**.
3. In the “Export to CSV” window, click **OK**.

Scanning devices for malware

You can scan mobile devices for malware and delete malware automatically.

To scan devices for malware, complete the following steps:

1. Navigate to **Advanced** > **Anti-Malware** > **Malware Scan**.
2. On the “Malware Scan” page, click the devices you want to scan.
3. Click **Scan** to scan for malware.
   - To delete scanned malware from devices, click **Delete Malware**.
   - To export the list of scanned malware, click **Export to CSV**.
4. In the “Malware Scan” window, click **OK**.
   - You can set the malware scan interval to automatically perform regular scans based on a predefined schedule. For more information, see Configuring the Anti-Malware settings.
5. Click on the row of a device to view the detailed scan results.
   - You can view the status, malware type, version, and size of the scanned malware.
   - You can select and delete the scanned malware by application or package name.

NOTE If the scan status is “Failed” after scanning devices, hover the mouse over ⓘ to view the reason.

Managing Open API

EMM uses the OAuth2 authentication method as a standardized open protocol to provide an Open API for developers. With the Open API, you can support the development of EMM functions, such as providing access to the EMM server, securing the authentication, and easily customizing the application programming and services.

To use the Open API, register the Client ID in the Admin Portal, issue a token valid for the period, and call the Open API. For more information, see the EMM API in the Samsung SDS EMM Developer's Guide and JAVADoc.

NOTE To activate the API client to use Open API, on the TMS Admin Portal, navigate to **Management** > **Tenant**. For more information about the license section, see the Samsung SDS TMS Administrator's Guide.

Adding API clients

To add a Client ID for using Open API, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the "API Client" page, click **Add**.
3. In the "Add API Client" window, enter the following information:
   - **Client ID**: Enter a unique client ID to use for a token request.
   - **Password**: Enter a new password between 8 and 30 characters. The password must be a combination of letters, numbers, and special characters.
   - **Token Validity(sec)**: Enter the access time for when the Open API is called.
4. Click **Save**.

Copying API clients

Copy an existing Client ID and create a new Client ID.

To copy a Client ID, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the "API Client" page, click **Copy** in the row of the specific API client you want to copy.
3. In the "Copy API Client" window, enter the following information.
4. Click **Save**.

Modifying API clients

To modify a Client ID, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the “API Client” page, click **Modify** in the row of the specific Client ID that you want to modify the information of.
3. In the “Modify API Client” window, modify the following information.
4. Click **Save**.

Deleting API clients

To delete a Client ID, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the “API Client” page, click **Delete** in the row of the specific Client ID you want to delete from the list.
3. In the “Delete“ window, click **OK**.

Activating or deactivating API clients

To activate or deactivate Client ID, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the “API Client” page, click **Change Status** in the row of the specific Client ID you want to change status from the list.
3. In the “Change Status” window, click **OK**.
    - The status of the API client changes to **Active** or **Inactive** depending on its previous status. Once activated, the Open API can be called using the API client. Once inactivated, the Open API cannot be called using the API client.

Invalidating tokens

Invalidate all the currently active tokens. An invalidated token cannot be used again and a new one must be requested through the OAuth2 authentication method.

To invalidate tokens, complete the following steps:

1. Navigate to **Advanced** > **EMM API** > **API Client**.
2. On the “API Client” page, click a specific Client ID in the list, and then click **Token Invalidate**.
3. In the “Token Invalidate” window, click **OK**.

Viewing the API log and API client log

Navigate to **Advanced** > **EMM API** > **API Log** and **API Client Log** to view all the API log and the API client log information. To view the API client log’s error details, click a specific API client log on the list. The error details are displayed at the bottom of the page.

The following is a sample of error codes details from the API client log list:

```
Parameters:deviceId=&
Result:{“resultValue”:null,”resultCode”:”-102”,”resultMessage”:”deviceId -
Null or Empty string”}
```

Using Mobile Admin

EMM provides Mobile Admin to allow you to manage and control EMM-installed user devices from other mobile devices. Using Mobile Admin's user-friendly interface, which is the same as the Admin Portal, you can monitor and manage users and devices.

EMM offers the following Mobile Admin features:

- **Dashboard**: Provides summarized information of the devices and users. You can also easily monitor the security status of the enrolled devices by viewing the compliance violation and device command history through the dashboard.
- **Device management**: Provides full management capabilities for devices of all OS types. You can view the information of all enrolled devices and control the devices by sending a device command.
- **User management**: Manages all user accounts. You can view the information of the user accounts and control the account status.

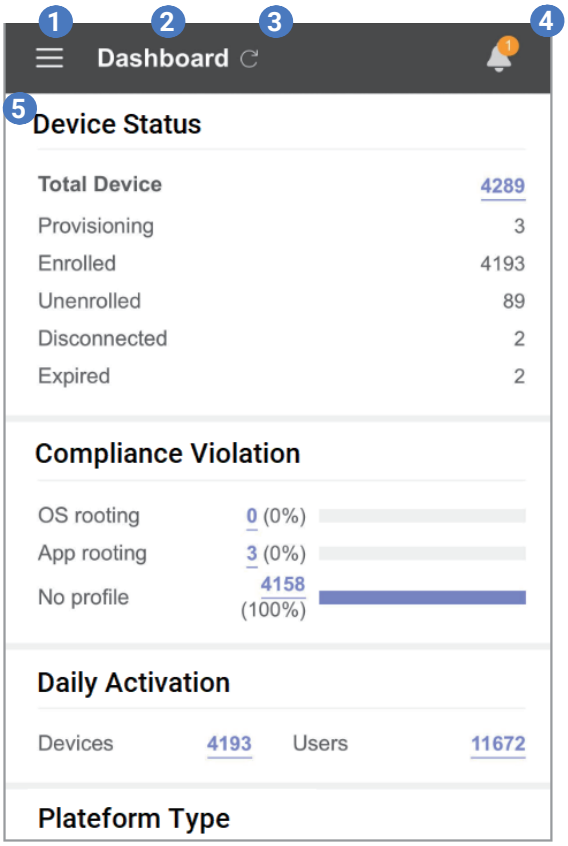
Meet the requirements listed below to ensure the efficient operation of Mobile Admin.

Item	Requirement
IT admin's PC	Browser: Chrome/Resolution: 5.8-inch display (1440 x 2960 pixels)
Mobile OS	All platforms are supported.
Supported language	English, Korean

NOTE If the selected language in Mobile Admin is not supported on the mobile device, Mobile Admin will be displayed in English.

Understanding the Mobile Admin screen

Get familiar with the Mobile Admin's interface features before starting Mobile Admin.



No.	Item	Description
1	Menu	Tap to open the side menus. The following menus are provided: • **Basic Information**: View the admin name, company name, admin ID, license version, license expiration date, and the number of registered devices by the total number of devices in the tenant's license. • **Dashboard**: View the management status of devices and users. For more information, see Viewing the Mobile Admin dashboard. • **Devices**: Manage the EMM installed devices. For more information, see Managing devices on Mobile Admin. • **Users**: Manage the EMM device users. For more information, see Managing users on Mobile Admin. • **Logout**: Logout from the Mobile Admin.
2	Content page name	Displays the content page name of the selected side menu.
3	Refresh	Tap to view the latest information on the content page.
4	Alert	Tap to view the alerts based on audit events that occurred on the device. For more information, see Viewing Mobile Admin alert list.

No.	Item	Description
5	Content page	Displays a list of information for the selected side menu or the details about the selected resources.

NOTE

- If you do not use the Mobile Admin screen for longer than the maximum session timeout value, the logout pop-up appears. Tap **Cancel** to stay logged in.
- The maximum session timeout value is set in **Setting** > **Configuration** on the Admin Portal.

Viewing the Mobile Admin dashboard

Tap ☰ > **Dashboard** to view the management status of devices and users and other information.

- **Device Status**: Displays the number of devices enrolled in EMM and the number of devices by device status.
  - Tap the total number of devices to move to the “Devices” screen.
- **Compliance Violation**: Displays the number of devices with a root OS, root app, no profile, or malware.
  - Tap the number of occurrences of the violation to move to the “Devices” screen.
- **Daily Activation(Activated)**: Displays the number of the activated devices and the number of activated users.
  - Tap the number of the activated devices or users to move to the “Devices” or “Users” screen.
- **Platform Type(Activated)**: Displays the number of the activated devices by OS type and the ratio of each OS to the total number of devices.
- **Users by Organization**: Displays the total number of organizations, total number of activated users, organization lists, and the users in each organization.
- **Device Command History**: Displays the number of device commands sent to devices by date.

Viewing Mobile Admin alert list

Tap  on the right corner of the Mobile Admin screen to view the major changes on devices. Based on the audit events that occurred on the user devices, you can view the alert list displaying the information on the audit event name, device ID, and audit event duration.

The filter types of the alert list on Mobile Admin are as follows:

- **Changes In Server Status**: Displays only the alerts for the audit events that occurred when the server's certificate status or the system file changed, or in the following situations:
  - A server certificate has expired or been revoked.
  - A system file has been created, modified, or deleted.
  - A system file integrity error occurred.
  - An uncertified package has been found.
- **Failed Policies**: Displays only the alerts for the audit events that occurred when the device commands sent to apply the policies via the device management profile failed.
- **Changes In Device Status**: Displays only the alerts for the audit events that occurred when the device status changed.
- **Security Violations**: Displays only the alerts for the audit events that occurred when the device violated policies or when a CheckPoint MTP finds a malicious application on the device.

  NOTE The alerts for security violations that occurred within a week are displayed.

- **Others**: Displays other audit events.

You can also perform the following actions on this screen.

Icon	Description
 Search	Tap to open the search window on the alert list. To close the search window, re-tap the icon.
 Sort	Rearrange the alert list by date of creation or by ascending/descending order.
 Filter	Apply a filter to display a relevant audit event on the alert list.

Starting up Mobile Admin

To begin using Mobile Admin, you will need to enter the Admin Portal URL in your device's browser. Then, tap **Go to Mobile Admin** at the bottom of the login page. Once you accessed and logged in to the Mobile Admin, you can view and control EMM's device management features on your device.

Logging in to Mobile Admin

Log in to Mobile Admin by using the same login credentials used for the Admin Portal. Super administrators can use all the features provided in Mobile Admin, while sub-administrators privileges have restricted use.

To login to Mobile Admin, complete the following steps:

1. Visit the Admin Portal using the web browser on the device to connect the Mobile Admin.
2. At the bottom of the screen, tap **Go to Mobile Admin**.
3. Enter the EMM admin ID and password on the Mobile Admin login page.
   If you select "Yes" for Mobile Admin in **Setting > Server > Configuration** and **Two-Factor Authentication**, OTP authentication will run as the second authentication. Log in after entering the OTP sent to the administrator's mobile phone number or email address.

   NOTE
   - If you enter incorrect user ID or password for 5 consecutive times, you will be locked out for 10 minutes.
   - If you log in to the Mobile Admin for the first time or use a temporary password, enter a new password and configure the password.

4. On the "Privacy Policy" pop-up, tap the checkbox next to **I agree**.
5. Tap **OK**.

Creating Service Desk administrator accounts

To create a Service Desk administrator account, you will need to add a sub-administrator with Service Desk administrator privileges on the Admin Portal.

To create a Service Desk administrator account, complete the following steps:

1. On the Admin Portal, navigate to **Setting** > **Admin Console** > **Administrator**.
2. On the "Administrator" page, click  .
3. In the "Add Administrator" window, enter the information. For more information, see Adding an administrator.

NOTE When entering the information in the “Add Administrator” window, you must select the administrator type as **Sub-Admin** and the administrator permission as **Service Desk**.

4. Click **Save**.

Using Mobile Admin at a Service Desk

Service Desk administrators can access Mobile Admin and manage the devices enrolled in EMM. For more information on the device command and device information, see Sending device commands on Mobile Admin.

NOTE Not all features on Mobile Admin are available to the Service Desk administrators.

Managing devices on Mobile Admin

View the device type, device status, and device information with Mobile Admin, and manage the devices by sending device commands or messages.

Using Mobile Admin device menu

Navigate to > **Devices** to view all the EMM enrolled devices. To view detailed information of a specific device, tap the device name of a specific device on the list.

You can also perform the following actions on this screen.

Icon	Description
Device Command	Send a device command to the activated devices.
Search	Search for a specific device for the entered device ID in the search window. To close the search window, re-tap the icon.
Sort	Rearrange the device list by the date of occurrence or in ascending/ descending order.
Filter	Filter the device list by the current device account status.

Viewing device activation types on Mobile Admin

Navigate to ☰ > **Devices** to view the device activation type at the right corner of the device list.

The device activation types on the device list are as follows:

- **Legacy**: Android Legacy devices
- **Knox Workspace**: Android Legacy devices using Knox Workspace
- **Fully Managed**: Corporate-owned device. Android Enterprise devices activated as a Fully Managed type
- **Fully Managed with Work Profile**: Corporate-owned device. Android Enterprise devices activated in combination with Fully Managed and Work Profile (supports up to Android 10 (Q)).
- **Work Profile on company-owned**: Corporate-owned device. Android Enterprise devices activated in combination with Fully Managed and Work Profile (supports Android 11 or higher).
- **Work Profile**: Bring Your own Device. Android enterprise devices activated as a Work Profile type.
- **DEP**: iOS devices activated through DEP

NOTE For Android Legacy or Android Enterprise (Fully Managed or Work Profile on company-owned) devices with Dual DAR settings, (Dual DAR) will be displayed for the device type on the device list.

Viewing device status on Mobile Admin

Navigate to ☰ > **Devices** to view the current status of a device on the device list. The statuses are displayed as an icon.

The device statuses on the device list are as follows:

Icon	Description
Provisioning	The device is enrolled and EMM is activated.
Activated	The device is activated and can be controlled.
Deactivated	The device is deactivated and cannot be controlled.
Blocked by System	The device has exceeded the set Keepalive interval, or it has been factory reset. It cannot communicate with the Admin Portal anymore so it is displayed as blocked by the system.
Activation blocked	The activation of the deactivated devices has been blocked by the administrator.
Blocked by Admin	The device has been stolen or modified, and blocked by the administrator.

Sending device commands on Mobile Admin

Control the device by sending device commands from the Mobile Admin. Device commands can only be sent to activated devices.

- For more information on the Android Enterprise device commands, see List of device commands: Android Enterprise.
- For more information on the Android Legacy device commands, see List of device commands: Android Legacy/Knox Workspace.
- For more information on the iOS device commands, see List of device commands: iOS.
- For more information on the Windows device commands, see List of device commands: Windows.

To send device commands on Mobile Admin, complete the following steps:

1. Navigate  > **Devices**.
2. On the “Devices” screen, tap the checkbox next to the device you want to control from the device list.
   - You can also tap  to open the search window and enter a mobile ID you want to control.
3. Tap  at the right corner of the device list.
   -  is enabled for activated devices only.
4. In the “Device Command” pop-up, tap the device command you want to send.
   - Select an area to send a device command depending on the device activation type.
5. Tap **OK**.

Sending messages on Mobile Admin

To send a message on Mobile Admin, complete the following steps:

1. Navigate to > **Devices**.
2. On the “Devices” screen, tap the checkbox next to the device you want to send a message to.
   - You can also tap to open the search window and enter a mobile ID you want to send a message to.
3. Tap at the right corner of the device list.
   - is enabled for activated devices only.
4. In the “Device Command” pop-up, tap **Push Notification**.
5. On the “Push Notification” screen, enter the following information:
   - **Title**: Enter the title of the message to be sent.
   - **Content**: Enter the message to be sent.
6. Tap **OK**.

Managing users on Mobile Admin

Manage the EMM device users on Mobile Admin.

Using Mobile Admin users menu

Navigate to > **Users** to view the information of the user accounts on EMM. To view detailed information of a specific user, tap the user name of a specific user on the list.

You can also perform the following actions on this screen.

Icon	Description
Search	Search for a specific user for the entered user ID or user name in the search window. To close the search window, re-tap the icon.
Sort	Rearrange the user list by the date of occurrence or in ascending/descending order.
Filter	Filter the user list by the current user account status.

Viewing user information on Mobile Admin

To view the user information, complete the following steps:

1. Navigate to ☰ > **Users**.
2. On the “Users” screen, tap the user on the user list you want to view the information of.
3. On the “User Information” screen, view the following:
   - **Registered Devices**: Displays the registered devices for the user account.
   - **Organization**: Displays the organization name the user belongs to.
   - **Employee No.**: Displays the user’s employee number.
   - **Email**: Displays the user’s email address.
   - **Phone Number**: Displays the user’s phone number.

Activating or deactivating user accounts

To activate or deactivate the user account, complete the following steps:

1. Navigate to ☰ > **Users**.
2. On the “Users” screen, tap the user on the user list whose account you want to activate or deactivate.
3. On the “User Information” screen, tap the following:
   - Tap ○ (**Deactivated**) to activate the user account.
     - Once the user account is activated, devices enrolled for the user account can be controlled.
   - Tap ● (**Activated**) to deactivate the user account.
     - Once the user account is deactivated, devices enrolled for to the account cannot be controlled, regardless of the device status.
4. Tap **OK**.

11

Setting

Setting

Customize various settings in the Admin Portal. Set the EMM applications, EMM Client 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 administrator's accounts.

This chapter explains the following topics:

→ Setting SecuCamera policies

Allow use of SecuCamera application and set the SecuCamera policies.

→ Setting Knox Portal policies

Allow use of the Knox Portal application and set the Knox Portal policies.

→ Configuring the Keepalive settings

Configure the Keepalive settings, such as the target type, expiration period, interval, and target groups/ organizations.

→ Managing message templates

View the provided templates of messages for device users and add and manage new templates.

→ Setting the logo

Customize the logo and header in the Admin Portal.

→ Managing administrator accounts

Add and manage administrator accounts in EMM.

To view the instructions for other settings in **Setting** > **Server** > **Configuration**, refer to the following topics:

→ Setting up the email server

→ Setting the user authentication method

→ Setting Terms and Policies

→ Setting public push servers

→ Configuring the SMS settings

→ Configuring the E-FOTA settings

→ Configuring the Anti-Malware settings

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** > **Server** > **Configuration**.
2. On the “Configuration” page, customize the environment settings. For more information about the environment settings, see List of environment settings.
3. Click  .

List of environment settings

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

Admin

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.
Default Country Code	Select the country code 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.
Mobile Admin	Set whether to use Mobile Admin. Select “Yes“ to use EMM Mobile Admin on mobile devices. • If you want to set OTP authentication, which provides two-factor authentication, when logging in to the Mobile Admin Portal, select “Yes“ for **Two-Factor Authentication** in **Setting > Server > Configuration**. You need to enter the mobile phone number or email address of the administrator for OTP authentication.
Mobile Admin allowed in Secure Browser only	Determine whether administrators can connect to Mobile Admin Portal via Secure Browser only. If you select “Yes,” then the Mobile Admin Portal cannot be accessed using other browsers. • To use Secure Browser, navigate to **EMM Application and Policy** > **Secure Browser**, select **Use** for **Use Secure Browser App**, and enter the mobile admin portal URL for the **Hompage URL**.

Option	Description
Secure Browser settings key value	Enter the settings key value for using Secure Browser. **SECUREBROWSER** is the default Secure Browser settings key value. • To change the Secure Browser settings key value, navigate to **Setting** > **EMM Application and Policy** > **Secure Browser** and select **Use Secure Browser App** as **Use**, and then change the **'User Agent' Settings Key Value**.
Multiple login	Allow concurrent logins to the Admin Portal.
Action When Admin Login Fails	Select the response of the EMM server when there are successive failed login attempts. • Delete account • 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. The default is 5.
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. The default is 30.
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. The default is 30.
Remote Support Relay URL (IP/Domain:port)	To provide remote support, enter the relay server's URL in **IP/domain: port** format. **NOTE** This option is not available for the high security version.
Copyright	You can set the copyright information.
User Password Strength Setting	Set whether to apply strength for user passwords. • If you set it as **TRUE**, you must enter the password directly when registering a single user or fill in the user information template file when registering bulk users. The passwords must contain letters, numbers and symbols between 8 and 30 characters. When registering bulk users, user registration will fail if you do not enter the passwords. • If you set it as **FALSE**, the passwords will be automatically entered the same as the user ID when registering bulk users, and user registration will be successfully completed.

Option	Description
Password Validity Period (Days)	Set the maximum period of the administrator password. When the set validity period expires, a password change pop-up window will appear on the screen when logging in. • You can enter a value from 0 to 365. The default value is 0. (When entering 0, there is no limit to the password usage period.)
Manage Password History (Times)	Set the number of times the administrator password can be reused. • You can enter a value from 1 to 5. The default value is 1. (If set to 1, the current password cannot be reused.)
Minimum Password Length	Set the minimum length of the administrator password. • You can enter a value from 6 to 16. The default is 8.

Application

Set the deletion range when deleting an application. EMM Application does not apply the option.

Option	Description
Use HTTPS for High-Security App Deployment	Set to use the HTTPS method instead of App Tunnel to transmit large binary applications to devices in High security version. The recommended application size in AppTunnel is 100 MB. To deploy a large application, you can use HTTPS instead of AppTunnel. • If you select **Yes**, large binary applications will be transmitted through the HTTPS method.
Manage Deletion	Set the deletion range when you delete an application from the Admin Portal's application list. • **Console**: The application will be deleted from the Admin Portal only. • **Console + Device**: The application will be deleted from both the Admin Portal and any device with the application installed.
Maximum Number of Devices Installing Apps at the Same Time	Supported only on Android devices. You can set the maximum number of devices that can simultaneously install an application. • You can enter a value from 0 to 10000. The default value is 0 (unlimited). **NOTE** The execution interval of the application installation scheduler based on the maximum number of devices setting is as follows. You can view the installation requests of the applications to be installed in **Service Overview > Device in Request > Application Installation**. • Scheduler execution interval: 5-30 minutes Device number: 1500 or less (5 mins), 3000 or less (10 mins), 4500 or less (15 mins), 6000 or less (20 mins), 7500 or less (25 mins), 10000 or less (30 mins)

Content

Set the maximum file size that can be uploaded as content, the maximum number of devices, and the maximum file size for downloads at the same time.

Option	Description
Maximum Uploadable File Size (MB)	Set the maximum file size that can be uploaded as content. And Set to 0 if you do not want to limit the number of users. • You can enter a value from 1 to 500. The default value is 100.
Maximum Number of Devices Downloading Files at the Same Time	Set the maximum number of devices which can download content at the same time. • You can enter a value from 0 to 1000. The default value is 0.
Maximum File Size Downloadable at the Same Time (MB)	Set the maximum file size for downloads at the same time. It can be set only when the maximum number of users downloading files at the same time is set. If the maximum number of users is set to 0, the item is disabled. • You can enter a value from 1 to the value set as the maximum file size. The default value is 100.

Certificate

Set whether to save an external certification in the EMM server.

Option	Description
Save iOS Certificate to the Server	You can set an external certificate needed for Wi-Fi, Exchange, and VPN authentication with an iOS device. Register an external certificate for iOS on the EMM Admin Portal and then you can set whether to save the certificate on the server. • **TRUE**: When an iOS certificate is issued, save a duplicate certificate on the EMM server. When you apply a profile, that certificate will be sent to devices. Also, if a user wants to delete Wi-Fi, VPN, and Exchange certificates from an iOS device, it must be set to TRUE. • **FALSE**: Whenever you apply a profile, a new certificate will be issued.

Device

Configure the device management settings.

Option	Description
Device Auto Registration	After registering the user on the Admin Portal, when the user logs into the EMM of the device, the device is automatically registered in the Admin Portal. **NOTE** If you want to register your device automatically in the EMM Admin Portal and log in to EMM without entering the Mobile ID on KME devices from EMM v2.5.5 version, set the following: (The Mobile ID will be created automatically without entering it.) • Select “True“ for Device Auto Registration. • Add “`ShowMobileId`” in JSON data on the KME profile for Android Enterprise. For more information about JSON data settings, see Creating MDM profiles for Android Enterprise devices.
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. It displays the gap between the current time and the last connected time of a device. If the gap does not exceed the standard, it is displayed in green. If the gap exceeds the standard, it is displayed in red.
Maximum Number of Active Devices per User	Select the number of devices that can be activated per user.
Limited Enrollment	Enable activation of mobile devices using their IMEI or serial numbers.
Google Maps API Key	Enter the API Key for using Google Maps. Once you set up a Google Maps API key, you can check the device's location via maps.
Device location	You can set a map to check the location information of the device. The default setting is Google Maps. Select Baidu Maps to display the device location in China. To locate the position of the device by using the map, go to **Device** and check the device details.
Server URL for device registration	You can set the EMM server address the user enters in EMM when logging in to the user device. Add “/” at the end of the server address. For example, https://emm.sds.com:35443/

EMM Client

The followings are the configurations for displaying the Privacy Policy Agreement (EULA) during the initial EMM login.

Option	Description
App permission to collect app info.	Allow EMM applications to collect application information data. When this option is allowed, application information is also collected on iOS devices.
Privacy Statement Title	You can set the title of the Privacy Policy Agreement (EULA).
Privacy Statement URL	You can set the URL address where users can find the Privacy Policy Agreement. At the bottom of the Admin Portal, click **Privacy Policy** to go to the detail page.
Event On Notification Icon Color	Select the color of the notification icon displayed on devices when the event is on. If the event is off, the notification icon color will be changed to the set security notification icon color.
Security Notification Icon Color	Select the color of the security notification icon displayed on devices.

Exception Policy Scheduler

Set the schedule to apply an exception profile.

Option	Description
Schedule(hr) to apply exceptional policies	You can set the time period to run an exception profile for users in their devices. The service period can be set under **Advanced** > **Exceptional Profile**. • You can enter a value from 0 to 23. The default is 0.
Schedule(min) to apply exceptional policies	You can set the time period to run an exception profile for users in their devices. The service period can be set under **Advanced** > **Exceptional Profile**. • You can enter a value from 0 to 59. The default is 10.

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. The inventory information for Android and Android Enterprise devices is collected according to the device scheduler. In other words, the collection interval depends on the device scheduler. However, on devices running Android 10 or higher, the inventory information is collected at random intervals due to restrictions on Google's OS background. • You can enter a value from 4 to 24 or 0(the device inventory is not collected). **NOTE** • Starting from EMM v2.5.0, the inventory information for Android devices are collected not by the device scheduler but the server scheduler. In addition, to set an interval for collecting the location data of Android devices, navigate to **Setting > Location Report Interval**. • In the version earlier than EMM v2.5.0, 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**.
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).

EMM App Store

Set whether to allow the application review function. The content of the review can be found in the evaluation section of the internal application.

Option	Description
App Store Review	Set whether to allow users to rate and review the application. • When set to 'Yes', users can write application reviews. • When set to 'No', writing and viewing application reviews are prohibited.

LOG

Set the data retention cycle of audit logs, log files, and databases in days. Data on the date after the set storage period will be deleted automatically.

Option	Description
Audit Log Retention Period (Days)	Set the audit log retention cycle. • You can enter a value from 1. The default is null. (If not entered, audit logs will not be deleted.)
Database Retention Period (Days)	Set the data retention cycle of the database. • You can enter a value from 1. The default is null. (If not entered, database data will not be deleted.)
Log File Retention Period (Days)	Set the log file retention cycle. • You can enter a value from 1. The default is null. (If not entered, logs files will not be deleted.)

NOTE The deletion targets and support scope that are automatically deleted from the EMM server are as follows.

- Support scope: Only Android Enterprise DO and legacy devices of Samsung Galaxy are supported.
- Log File: TSES_DEVICE_LOGFILE, the connected Device Log File
- Audit Log: TEMM_AUDIT_SERVER, TEMM_AUDIT_RESULT, TEMM_AUDIT_LOG_DATA
- Database Log:
  - Connector Log: TSES_USER_LOG, TSES_USER_LOG_RESP
  - Device Command History: TEMM_TRANSMISSION_HISTORY, TEMM_TRANSMISSION_HISTORY_GATE, TEMM_TRANSMISSION_HISTORY_MULTI
  - Email And SMS History: TEMM_MESSAGE_LOG
  - AD/LDAP History: TEMM_SYNC_SERVICE_LOG, TEMM_SYNC_ENTITY_LOG
  - API Log: TSES_OAUTH_LOG, TSES_OAUTH_CLIENT_LOG
  - Report Stat Log: TEMM_STATS_DEVICE, TEMM_STATS_USERS

MDM

Configure the mobile device control settings.

Option	Description
APNs Topic for iOS	APNs Topic is the ID of the holder of the APNs certificate for MDM. The APNs Topic is automatically entered when you upload a certificate under **Setting** > **Server** > **Configuration** > **Public Push** > **APNs**. If the APNs Topic value is different from the UID value of the Subject Name, 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=`".
Attestation Api Key	The key value for summoning Attestation API.
Attestation Server URL	The URL of the attestation server. When accessing the attestation server, you can set the use of the proxy server in **Setting** > **Server** > **Configuration** > **Network**.
Daily retries for device commands in request	Select how many notifications you will receive per day to send device commands which have been sent but not applied successfully. Unapplied device commands are listed in **Service Overview** > **Device Command in Request**. • **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.
Direct boot command polling interval for Android (min)	Set the polling cycle to control the devices in Direct Boot mode. EMM sends device commands to Android devices according to the polling cycle. Even if the polling interval is 0, polling is executed once after the EMM Agent is started. • You can enter a value from 0 to 1440 or 0(the polling will not be performed).
Knox app installation authority required package	Enter the required packages whose access must be granted upon installing the application within the Knox Workspace. You can enter multiple packages by separating them with a comma (,).
Interval of Multi device control distribution (second, Console)	Set the interval (in seconds) at which device commands should be sent to devices in each batch by an administrator from the Admin Portal or an Open API. • Android, iOS platform only
Device quantity of Multi device control distribution (Console)	Set the number of devices to which device commands should be sent in each batch by an administrator from the Admin Portal or an Open API. For instance, if you set the interval to 5 seconds and the number of devices to 500, then a device command will be sent to 500 devices in 5-second intervals. • Android, iOS platform only

Option	Description
Interval of Multi device control distribution (second, Schedule)	Set the interval (in seconds) at which device commands should be sent to devices in each batch by the EMM server, based on the schedule set for things such as the profile updates, inventory collection, or the location data collection schedule. • Android, iOS platform only
Device quantity of Multi device control distribution (Schedule)	Set the number of devices to which device commands should be sent in each batch by the EMM server, based on the schedule set for things such as the profile updates, inventory collection, or the location data collection schedule. For instance, if you set the interval to 5 seconds and the number of devices to 500, then a device command will be sent to 500 devices in 5-second intervals. • Android, iOS platform only
SCEP servlet URL	Enter the servlet URL that supports Simple Certificate Enrollment Protocol (SCEP). If you do not set this value, the JSCEP library that is built in to EMM will be used.
MDM service URL(http://host:port)	Enter the URL configured to use MDM service for iOS in the following format: http://host:port.
Communication digital signature certificate (iOS)	Configure the certificate to ensure secure safe data transfer from the EMM server to iOS devices. To register the certificate, set the certificate purpose as **iOS Sign Cert** and the certificate type as **Server** under **Advanced** > **Certificate** > **External Certificate**. The registered certificate will be downloaded and used on iOS devices.
Communication digital signature root certificate (iOS)	Configure the certificate to secure iOS app verification on iOS devices. To register the certificate, set the certificate purpose as **iOS Signing Root CA Cert** and the certificate type as **Root** under **Advanced** > **Certificate** > **External Certificate**.
SMS Permission Control	Set whether to allow SMS Permission Control to receive the gate access policy from the device through text when a device comes in. • Support range and restrictions: Applies only to Android Legacy devices, and if the user turns off mobile data on the device, switches to airplane mode, or blocks the phone number sending the text message, it is not possible to receive the text message.
Delete App upon Unenrollment	Set whether to delete the applications installed on a device before deactivating it. The deletion targets are internal applications for Android devices and all applications installed through EMM for iOS devices.

Option	Description
Keepalive Duration (days, set 0 to disable, Android Only)	Set the Keepalive duration. If there is no communication between the EMM server and devices for the set period, then it attempt to re-establish a connection directly with the device at the set Keepalive Interval instead. When the connection with server keeps disconnected, the device status will be changed to ”Blocked by System.” Once the status has changed to ”Blocked by System”, the administrator must change back the status to “Deactivated“ manually. To disable the Keepalive function, enter 0. If the device still fails to establish communication after the Keepalive duration, you can perform the action on the device as set in **Action after Keepalive Expiration**. • You can enter days from 3 to 365.
Keepalive Interval Period (hr, Android Only)	Set the Keepalive interval to check the connection between the EMM server and devices at the set interval. If you set the Keepalive interval period to 4 hours, Android devices try to establish communication with the EMM server every 4 hours. • You can enter hours from 4 to 24.
Reminder to Go Off Before Keepalive Expiration (hr, Android Only)	Set the reminder to go off before Keepalive expiration to notify Android devices that “Use of EMM is blocked due to Keepalive period exceeded.” • You can enter hours from 1 to 3.
Action after Keepalive Expiration (Android Only)	Select the action to perform after Keepalive expiration. • None • Lock Device • Lock Preloaded Email App • Factory reset(EMMAgent v2.0+) • Factory reset(incl. SD Card)

Network

Configure the log collection settings to monitor call and data usages. Logs are collected according to the inventory collection interval (**Server** > **Configuration** > **Inventory Scheduler**).

NOTE To instantly apply call and data usage changes, send a device command in **Device command** > **Apply Latest Profiles** and reboot the device.

Option	Description
Collect Call Usage Logs	Allow call usage log collection for devices.
Set Call Usage Warning	Allow sending a warning when call usage limit is almost reached.
Usage Threshold (Minutes)	Enter the call usage limit.

Option	Description
Collect Data Usage Logs	Allow data usage log collection for devices.
Set Data Usage Warning	Allow sending a warning when data usage limit is almost reached.
Usage Threshold (GB)	Enter the data usage limit.
Collection Start Date	Set the date to start collecting logs in a month. Log collection restarts on this date every month.
Number of Collections to Process when the Scheduler Runs	You can improve database performance by saving the network usage inventory information of the device in a temporary table in the database and setting the scheduler to inquire and process it on a regular basis. Set the number of temporary table collections that the scheduler processes at a time. • You can enter a value from 50 to 1000. The default is 500.
Collected Usage Processing Scheduler (Min)	Set the scheduler cycle to process the usage collected in the temporary table. • You can enter a value from 5 to 200 minutes. The default is 5 minutes.

Network Dashboard

Configure the starting points of the call and data usages that are displayed in **Advanced** > **Network** > **Dashboard**. The ranges are classified as Very Low, Low, Medium, High, and Very High.

Option	Description
Calls : Very Low Usage Starts At (minutes)	The starting point of the Very Low level of call usage. It is set to 0 and cannot be modified.
Calls : Low Usage Starts At (minutes)	Set the starting point of the Low level of call usage.
Calls : Medium Usage Starts At (minutes)	Set the starting point of the Medium level of call usage.
Calls : High Usage Starts At (minutes)	Set the starting point of the High level of call usage.
Calls : Very High Usage Starts At (minutes)	Set the starting point of the Very High level of call usage. The maximum value is 44639 (less than 60 (minutes) * 24 (hours) * 31 (days)).
Data : Very Low Usage Starts At (GB)	The starting point of the Very Low level of data usage. It is set to 0 and cannot be modified.
Data : Low Usage Starts At (GB)	Set the starting point of the Low level of data usage.
Data : Medium Usage Starts At (GB)	Set the starting point of the Medium level of data usage.

Option	Description
Data : High Usage Starts At (GB)	Set the starting point of the High level of data usage.
Data : Very High Usage Starts At (GB)	Set the starting point of the Very High level of data usage. The maximum value is 10000000 (10 * 1024 * 1024 (MB)).

Push

Set whether to use Public Push.

Option	Description
Public Push	Set whether to use Public Push. If there is more than one activated device, Public Push is not available.
Agent Ticket	The EMM Agent Ticket value, which is the value received by the delivery during push installation.
Agent Ticket Index	The EMM Agent Ticket Index value, which is the value received by the delivery during push installation.
Client Ticket	The EMM Client Ticket value, which is the value received by the delivery during push installation.
Client Ticket Index	The EMM Client Ticket Index value, which is the value received by the delivery during push installation.

SecuCamera

Set the SecuCamera license.

Option	Description
SecuCamera license	Configure the SecuCamera license. The default setting is unlimited. If it is set to unlimited, there are no restrictions for using SecuCamera, and a button for assigning SecuCamera does not appear on the top of the list in the User menu.

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.
Service Desk Website	Enter the service desk website address.

Service Broker

Set whether to check the integrity between the device and the EMM server when using a connector.

Option	Description
Developer Mode	Set the check integrity of the device and server. • **TRUE**: Do not check integrity. • **FALSE**: Check integrity.

Smart Key

Set the use of the smart key for vehicle control.

Option	Description
Smart key availability	Set whether to enable or disable the use of a smart key.

Social Distancing

Set whether to use Social Distancing to monitor the distance between devices as part of social distancing to prepare for COVID-19. Device-to-device distance monitoring can be checked on the EMM Admin Portal under **Advanced** > **Social Distancing**.

The Social Distancing item is disabled when you first log in. Contact the Samsung SDS EMM Support Team to display it in the Admin Portal for the Social Distancing settings.

Option	Description
Social Distancing Service	Set whether to use Social Distancing that monitors the distance between user devices.
Maximum measured distance between devices (Meter)	Enter the maximum measurement distance between devices to collect contact history. Only device information detected within the set value will be collected.
Storage period of contacts history in the device (Days)	Set the period to store the contact history in a device. Logs will be automatically deleted after the storage cycle.
Device scan interval (Minutes)	Sets the period of checking the device to check the contact history.
Upload interval of collected data to the server (Hours)	Set the period of uploading the collected data to the EMM server.

Tizen Wearable

Set information for using Tizen Wearable devices.

Option	Description
EMM/TMS Service URL	Register a shortened URL that is entered to log in to EMM/TMS from a Tizen Wearable device. EMM administrators can register a shortened URL of the EMM and TMS server, such as **https://bit.ly/**, that can be created on a URL shortening site, following the Note rules below. **NOTE** Please note the following when registering a shortened URL for the EMM or TMS server for Tizen using the recommended site, https://bit.ly/. For a Single Tenant: • E.g., https://[EMM host]:[EMM port]/**emm**/provision • E.g., EULA URL: http(s)://[host]:[port]/**emm**/provision/**eula** In case of Multi Tenants: • E.g., https://[TMS host]:[TMSport]/**tms**/provision/**[Tenant_ID]** • E.g., EULA URL: http(s)://[host]:[port]/**tms**/provision/[Tenant ID]/**eula**
Authentication Failure Count (Set as 0 not to limit.)	Set the number of times that the user authentication code used to log in to EMM from a Tizen Wearable can be entered. If the number is set to 0, it is limitless.
OTP Issuing URL	Enter the URL address of the issuing site to receive the OTP.
Authentication Code Valid Duration (hr) (Set as 0 not to limit.)	Set the validity period for the user authentication code that is entered for logging in to EMM from a Tizen Wearable. When the validity period expires, you must get a new authentication code. If the validity period is set to 0, it is limitless.

Windows 10

Set the information related to Windows 10.

Option	Description
Validation during On-Premise verification	Set whether to validate the settings of the Windows provisioning package (PPKG) for the activation of the MDM agent. • **TRUE**: Verify the match of the UPN and secret values written in the Windows PPKG to activate the MDM agent in Windows 10. If they do not match, the MDM agent will not be activated. • **FALSE**: Do not verify the match of the UPN and secret values written in the Windows PPKG.
Provide MDM Agent sync service	Set whether to synchronize or not with MDM agent. Updates and policy controls of Windows are performed through synchronization with the MDM agent.
MDM Provider Name	Enter the MDM provider identified in the setup menu of the device that Windows is installed on.

Setting the connector service operation hours

Set the connector service operating hours. When the connector service that is registered under **System** > **Connector** in the Admin Portal is enabled, you can configure the service operation hours, notify devices about service unavailability, and record service logs.

To set the operation time of a directory service, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Connector Service**.
3. In the “Connector Service” window, configure the connector service time, and click **Save**.
   - **Connector Service Time** tab: Select the service time type.

Item	Description
System Preferences	You can configure the connector service time, and the service is provided at the time and date of your choice. Multiple configurations are available. For example, Mon. 00:00-20:30, Tue. 00:00-24:00 and Fri. 13:00-13:30. • Select **Day** and **Time** and click ↓ to add an operation schedule. • Select **Day** and **Time** and click ↑ to delete an operation schedule.
View Timetable	You can check the time table of the day and time settings for the weekly operation schedule.

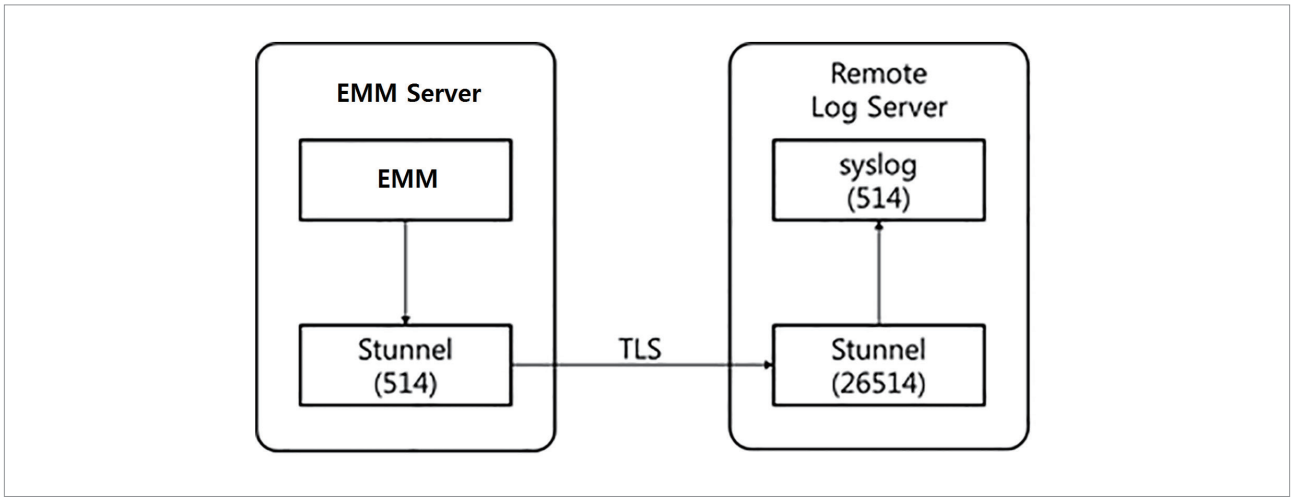
   - **Message During Non-Operation Hours** tab: Enter a message notifying users about non-operational hours. The message will be sent to user devices when the service is not in operation.
   - **Log Service** tab: Set whether to record the transaction log of connector service.

Item	Description
Enable the connector service transaction log	Choose whether to use the service transaction log or not.
Transaction Log Settings	• **Limit length of log data**: The amount of log data saved in bytes. • **Delete the previous logs**: You can set the retention period for previous logs from 30 to 600 days.

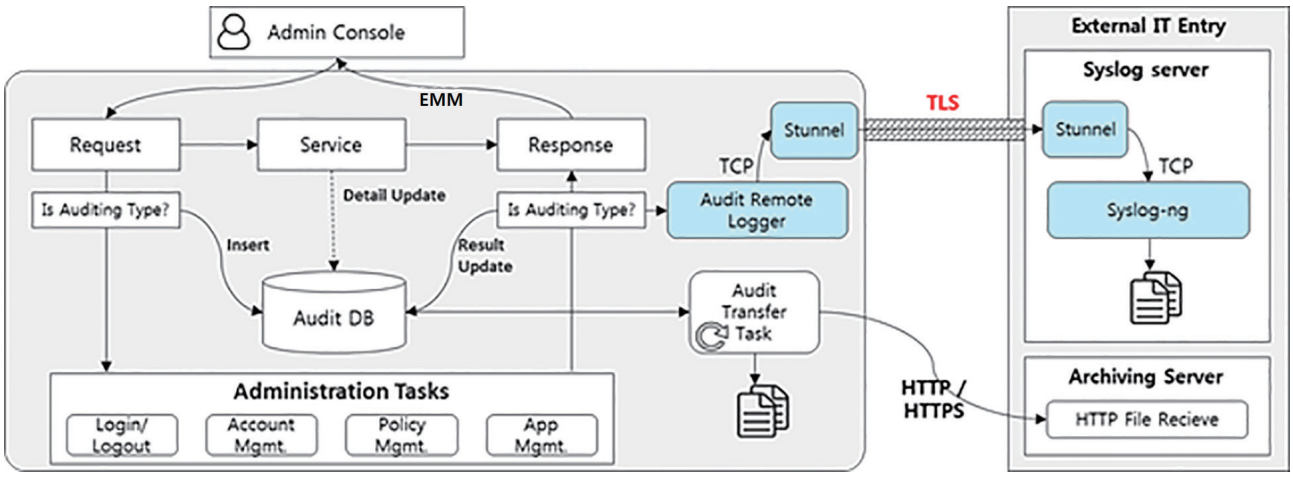
4. Click **Save**.

Configuring the audit log server

EMM records the information about the Admin Portal, user devices, and the EMM server to audit logs and manage them. Audit logs are stored in the database of the EMM server and the audit remote server. To manage audit logs in EMM, you can set the EMM server to transfer the files to the remote log server. Communication between the EMM server and the remote log server is protected by TLS secure communication or using Windows Server provided IPsec settings.
See the architecture diagram for the EMM server and remote log server by TLS secure communication below:



※ If IPsec is configured, it communicates directly with the EMM server without Stunnel.



The IPsec protection is the part of the CC evaluated configuration.
For more information about using Stunnel, see the information about remote logging in the Samsung SDS EMM Installation's Guide for installing and configuring the remote log server and configuring a secure communication channel between the EMM server and remote log server via Stunnel.

When the configuration is complete between the EMM server and remote log server, it will explain how to enter the information of the remote log server from the EMM Admin Portal.
To configure the remote log server, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Audit**.
3. In the “Audit” window, enter the following information:
   - **Remote Audit Log Server Settings**: If you transfer audit logs to the remote log server, click **Connect Remote Audit Log Server (SYSLOG**). When you enter the IP/Host address and port number and click **Save**, the audit logs are saved to the remote audit log server.
     - **IP/Host**: Enter the IP/Host address of the remote audit log server.
     - **Port**: Enter the port number of the remote audit log server.
   - **Audit Log Export Settings**: If you transfer audit log files to the remote log server, click **Export the Audit Log**, and then enter the items below:

Item	Description
Transfer Period	Select Daily, Weekly, Monthly, or Annually for the transferring period of the audit log.
URL	Enter the URL of the transferring server.
Certification Type	Select BASIC or NONE for the certification type. If you select BASIC, enter the login User ID and Password.
User ID	Enter the user id.
Password	Enter the user id's password.
Language	Select Korean, English, or Chinese for the language to write the audit log.
Execution Server	Select the server to run a transmission task.
Send File Name	This is the file name of the audit log to send outside.

   - **Audit Log Settings**
     - **Storage Limit of Audit Log**: Set the maximum number of audit logs to save. When the storage for the audit log surpasses 90% of its designated limit, a notice, **EMM inform Audit Saving Storage: 90%**, appears at the top of the EMM Admin Portal.
       - Input range: 1-10,000 records (1 million-10 billion). The default value is 1 million.
     - **Bring device audit to DB**: Set this as True or False.
       - True is default. Device audit logs, which are uploaded to the LTS log server, are saved to the DB.
       - If you set it as False, Device audit logs, which are uploaded to the LTS log server, are not saved to the DB. So, you can save CPU usage to process logs. To save CPU usage for the audit log process, construct LTS by separating it from the EMM server. For more information, see the Samsung SDS EMM Installation’s Guide.
4. To transfer audit logs to an external server, click **Transfer audit log** at the bottom of the “Audit” window, and click **OK** on the notification pop-up.
5. Click **Save** to save audit log configured.

Setting the proxy server

Set the proxy server, if necessary to connect the Android attestation server or search for Android Public AppStore.

To set the proxy server, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Proxy**.
3. In the “Proxy“ window, enter the following information.
    - To use a proxy server, click **use proxy**.
    - **Proxy Host**: Enter the proxy server address.
    - **Proxy Port**: Enter the proxy server port number.
    - **Proxy UserName**: Enter the user name needed for proxy server authentication.
    - **Proxy Password**: Enter the user password needed for proxy server authentication.
4. Click **Save**.

Managing service profile

Manage service profiles to operate EMM.The service profile is service information downloaded from the EMM server to the user device when the device is provisioned. The service profile manages information, such as the EMM Server, EMM Client, Push Server, AppTunnel Server, App store, Audit Server, Log Server, and MDM Server.

The followings are service profiles in Single-Tenant Mode and Multi-Tenant Mode for EMM. For more information about how to set the advanced items of service profiles, see the Samsung SDS EMM Installation’s Guide.

- Single-Tenant Mode: If the EMM server operates in Single-Tenant mode, the service profile will be activated on the upper-right side of the **Setting** > **Server** > **Configuration** menu. Click **Service Profile** to manage a service profile. The service profile sets the Item ID automatically, and administrators cannot modify it arbitrarily.
- Multi-Tenant Mode: If the EMM server operates in Multi-Tenant mode, you can manage service profiles at **Management** > **Service Profile** on the TMS Admin Portal.

To manage the service profile in Single-Tenant mode, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **Service Profile**.
3. In the "Service Profile" window, enter the following information.
   - **Preferences**: Enter the common setting items of the service profile. If the EMM Server, Push Server, and AppTunnel Server information is entered, it will automatically be mapped to the pertinent items in Advanced Settings.
     - If there is no valid server license, the pertinent server will not be shown on the setting item.
   - **Advanced Settings**:
     - **EMM Server**: Enter the setting information related to the EMM server.
     - **EMM Client**: Enter the download URL to install the Samsung SDS EMM Client.
     - **Push**: Enter the setting information of the Push and AppTunnel servers.
     - **AppStore**: Enter the AppStore connection URL.
     - **Audit Server**: Enter the setting information of the audit server. To manage audit logs through the remote server, set the remote log server. For more information, see Viewing audits.
     - **Log Server**: Enter the setting information for the log server.
     - **MDM**: Enter the EMM or Push Agent download URL, iOS MDM registration URL, and EMM Client download URL (if reset to factory settings).
4. Modify the value of the item ID based on its configuration and click **Save**.

Configuring SSO

Single Sign-on (SSO) is a service for signing in to multiple systems and applications using the same ID and password. Using SSO enables simple signing in using your existing account, without creating a new account only for EMM access. In order to use SSO in EMM, you must integrate EMM with the Active Directory Federation Services (ADFS) server. Configure the settings for the integration with ADFS.

To configure the SSO settings, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **SSO**.
3. In the "SSO" window, enter the following information.
   - **Admin SSO Settings**: Click **Use** to configure SSO.
   - **Service Provider Meta Data**: Click **Download** and download the service provider metadata.
     - Register the downloaded metadata on the ADFS server for provider trust registration. For more information, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736690(v=ws.10).
     - While registering the service provider metadata on the ADFS server, you must add the following claim rules. For more information, see https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configuring-claim-rules.
       - LDAP Attribute: SAM-Account-Name
       - Outgoing Claim: Name ID
   - **Identity Provider Meta Data**: In the "SSO" window, click  to upload the identity provider metadata downloaded from the ADFS server.
     - The default download URL is {ADFS Server URL}/FederationMetadata/2007-06/FederationMetadata.xml. Enter the URL in a web browser and download the metadata.
   - **Identity Provider URL**: The identity provider's URL that was retrieved by the uploaded identity provider metadata will be displayed in the **Identity Provider URL** field.
4. Click **Save**.

NOTE The ID registered in the ADFS server must be the same as the admin ID used for the EMM Admin Portal.

Setting the CAC Sign-In

Set CAC Sign-In to sign in to the Admin Portal via CAC smart card security authentication.
The necessary preparations for setting CAC Sign-In are as follows:

- Admin Registration: Register an administrator in the Admin Portal so that users registered in the AD DS system can sign in to the Admin Portal via CAC smart card security authentication. The administrator ID must be “user logon name“ among the attributes of the user registered in AD DS, and the domain name (@xxx.yyy) must be excluded.
- Tomcat Server Settings: Add <Connector>, which defines a separate port of two-way https for client authentication (CAC smart card user certificate) to the Tomcat configuration file. For the property values required when defining <Connector>, refer to CAC Sign-In of the Appendix.
- Directory Settings: Create a directory server by entering the AD server address in **System > Integration > Directory**, and add a directory service by setting the Base DN and filter to the directory server in **System > Connector > Directory**. For detailed input values, refer to CAC Sign-In of the Appendix.
- CAC Sign-In Settings: Set CAC Sign-In in **Setting > Server > Configuration**.

The following must be set in the Admin Portal for CAC Sign-In. For other necessary procedures, see CAC Sign-In of the Appendix.

To configure the CAC Sign-In settings, complete the following steps:

1. Navigate to **Setting > Server > Configuration**.
2. Click **CAC Sign-In** at the top of the “Configuration“ page.
3. In the “CAC Sign-In“ window, enter the following information.
   - **CAC Sign-In Settings**: Select whether to sign in via CAC smart card authentication. If you select Do not use, the items below will be disabled.
   - **Port**: Enter the port value of <Connector> that Tomcat has configured to support client authentication https.
   - **Directory Service Name**: Select the directory service set in **System> Connector> Directory** for CAC Sign-In.
4. Click **Save**.

Setting the QR code

Set the EMM installation QR code for Android Enterprise devices to be activated in Fully Managed or Work Profile on company-owned type devices. For the methods for activating a device by using a QR code, see Using a QR code.

To set the QR code, complete the following steps:

1. Navigate to **Setting** > **Server** > **Configuration**.
2. Click **QR Code**.
3. In the “QR Code” window, enter the following information:
   - **Pre-installation**: If EMM is operated on a closed network, you can install CA certification in advance on your device for EMM server access before EMM activation by selecting **Allow**.
     If you select **Allow** for pre-installation, a screen for certificate installation where you can select how to install the certificates appears after device reboot and before EMM enrollment. Users can install certificates by entering the **URL Address** on their devices or clicking **USB** and selecting files.
   - **Preload App**: Allows the use of the applications preloaded on devices.
   - **EMM APK Download URL**: Enter the URL for downloading the installation file of the EMM application.
4. Click **Save**.

Managing master data

Manage the standard information for EMM, which is classified into categories. The IT admin cannot add new categories to the master data but can configure and modify the key, value, selected value, and reference code in the Admin Portal.

Information managed in the master data is as follows.

- **Device**: Device model, status, ownership, platform, firmware, and carrier information
- **Language**: Supported languages by platform when searching for an external application and when registering an E-FOTA group
- **Application**: Application status, auto-update validation, compulsory application, and EMM package
- **Profile**: Network setting information, depending on the platform
- **User information**: Managing position, site, and security level

Adding master data

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

1. Navigate to **Setting** > **Server** > **Master Data**.
2. On the “Master Data” page, click .
3. In the “Add Master Data” window, enter the data information.
   - **Category**: Select the data category.
   - **Key**: Enter a key or code.
     - When creating a report from **Setting** > **Admin Console** > **Report**, the key value of the master data is used as the value of the query condition.
   - **Value**: Enter a value.
   - **Selected Value**: Select the value to be the default in the data category.

NOTE If you want to add additional reference codes, click **Reference Information** > and add it.

4. Click **Save**.

Modifying master data

To modify master data, complete the following steps:

1. Navigate to **Setting** > **Server** > **Master Data**.
2. On the “Master Data” page, expand the data categories and search for the value you want to modify.
3. Click  in the row of the value.
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 **Setting** > **Server** > **Master Data**.
2. On the “Master Data” page, expand the data categories and search for the value you want to delete.
3. Click  in the row of the value.
4. In the “OK” window, click **OK**.
    - The keys provided as master data by default cannot be deleted.

Viewing applied master data

Master data key value	Method for checking master data
Android OS Version Android Version iOS OS Version iOS Version Ownership Device Status Platform Windows OS Version Windows Device Type Android Firmware iOS Firmware Device Country Device Model Device Network	Navigate to **Device**. Check the device information on the "Device Detail" page.
Mandatory App	Navigate to **Device**. Click a device name to open the "Device Detail" page, and click the **Application** tab. View the application information.
AppClientLanguage AndroidMarketLang iOSMarketLang	Navigate to **Application**. Click **Add** > **Public** and check the language of the AppStore on the “Add Application” page. When the app is installed on the device, it will be installed using the default language set in AppClientLanguage.
Position Security Level Site	Navigate to **User**. Click **Add** and check the user information on the “Add User” page.
Managed App EMM PackageName	Navigate to **Setting** > **EMM Application and Policy** > **EMM Application**. Click **Add** > **Newly register** and check the validation of Package name for the installation file, and then check **Auto Update** in the “Add EMM Application” window.
Device Profile Configuration	Navigate to **Profile**. Click a profile name to open the “Profile Detail” page, and click **Modify Policy**. Click each platform and check policy details in the Android, iOS, and Windows tab on the “Set Policy” page.
Tizen Push URL	The Tizen URL address of the regional Request Manager (RQM) server to send Push Notification to the wearable devices.

Viewing the server information and server list

View the server information and server list where EMM is installed. EMM can be operated from multiple sites when servers are clustered. Check the server list for assigning tasks and monitoring servers.

Viewing the EMM server information

To check the information and clear the cache of EMM server, complete the following steps:

1. Navigate to **Setting** > **Server** > **Server Information**.
2. To clear cache or check the open source software and restricted rights, click **Clear Cache**, **Open Source License** and **Restricted Rights** at the top of the screen.
3. The following is the description items for the server information:

Item	Description
COMPUTERNAME	The computer name of the EMM server
CRYPTOJ_VERSION	The version of the RSA CRYPTO-J cryptographic module
EMM Host	The server host name of the EMM server
EMM IP	The server IP address of the EMM server
EMM Version	The version information and build number of the EMM server
FIPS Compliant	Federal Information Processing Standard (FIPS) compliant mode
JAVA_HOME	The home path of JAVA installed on the EMM server
JMX PORT	The JMX port installed on the EMM server
NUMBER_OF_PROCESSORS	The number of CPUs installed on the EMM server
OS	The type of OS in which the EMM is installed.
PROCESSOR_ARCHITECTURE	The processor's chip architecture on the EMM server
PROCESSOR_IDENTIFIER	The description of the processor on the EMM server
PROCESSOR_LEVEL	The model number of the computer's processor on the EMM server
PROCESSOR_REVISION	The revision number of the processor on the EMM server
RMI PORT	The port of the PMI on the EMM server

Viewing open source license and restricted rights

The Open Source Software provides software component versions, license information, and regulatory compliance for the use, development, and redistribution of the open source software. The Restriction Rights outlines the terms and policies for using the EMM product. You can check these information in **Setting** > **Server** > **Server Information**.

Managing the server list

To manage the server list, complete the following steps:

1. Navigate to **Setting** > **Server** > **Server List**.
2. Enter Server IP in the search field and click **Enter** or  .
3. The following is the description items for the server list:

Item	Description
Server IP	The IP address of the server
Host Name	The name of the server host
Monitoring Port	The service port that provides server monitoring
RMI Port	The service port for the RMI server
Connector Service	The status of the connector service, Activated or Deactivated
Server division	• **EMM**: Samsung SDS EMM server • **LTS**: The server used to store logs
Last Updated	The date of the most recent server update

Managing message templates

EMM 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	Administrator Authentication	Admin OTP Email
	Administrator Account Information	Admin ID
	Administrator Temporary Password	Admin Temporary Password E-mail
	User Temporary Password	User Temporary Password
	Android Enterprise QR Code	Android Enterprise QR Code (Android Enterprise Fully Managed or Work Profile on company-owned)
	Apple VPP	Apple VPP Invite: The email template for inviting VPP users
		Apple VPP Redeem: The email template for installing purchased VPP applications through redeemable codes
SMS	Administrator Authentication	Admin OTP SMS
	Administrator Temporary Password	Admin Temporary Password
Email/SMS	Tizen Wearable Installation	Tizen Wearable Email
		Tizen Wearable Code
		Tizen Wearable Information
		Tizen Wearable Installation: The SMS templates for sending Tizen Wearables things such as Tizen Wearable Information, Tizen Wearable Installation, and Tizen Wearable Code. However, ”Tizen Wearable Installation” and “Tizen Wearable Code” templates cannot be modified, as they are used for parsing the information from the Tizen device.

Adding message templates

To add a new template, complete the following steps:

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

NOTE

- The copyright, service desk email and phone number, EMM/TMS Service URL, OTP Issuing URL in the “Select Lookup Item” window are applied to the message template only when those values are set in **Setting** > **Server** > **Configuration**.
- If the contents of the SMS Tizen Wearable Information template exceed 80 characters, they are divided and then transmitted.
- 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

Modifying message templates

To modify message templates, complete the following steps:

1. Navigate to **Setting** > **Message Template**.
2. On the “Message Template” page, click **Modify** in the row of the template you want to modify.
3. In the “Modify Message Template” page, modify the existing information.
4. Click **Save**.

Deleting message templates

To delete message templates, complete the following steps:

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

Setting the logo

To change the EMM logo to your company logo, set the color of the header or header text, and write a notification message that should appear to the administrator when logging in to EMM, complete the following steps.

1. Navigate to **Setting** > **Admin Console** > **Logo Setting**.
2. On the "Logo Setting" page, choose a logo image and header color and write a notification message that will appear when you log in to EMM.
   - **Logo Image**: Click **Browse** 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 224 x 23 and must be 1 MB or lower.
   - **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.
   - **Login Notification**: Write text in a notification message that should appear to the administrator when logging in. The message will appear on the screen when you log in.
3. Click  to save it.

Setting EMM Client policies

The EMM Client is an EMM application that is installed on mobile devices to be controlled remotely. Add the EMM Client as an EMM application and configure the policies. For more information about adding EMM application, see Adding EMM applications.

To configure policies for the EMM Client, complete the following steps:

1. Navigate to **Setting** > **EMM Application and Policy** > **EMM Client**.
2. On the “EMM Client” page, click the “Default” tab.
   - The policies set in the “Default” tab will be applied to every group or organization that is not assigned other EMM Client policies in your tenant.
   - To apply different EMM Client policies to specific groups or organizations, click ⊞ and configure an EMM Client policy set.
3. Configure the policy details. For more information about the applicable policies, see Applicable policies for EMM Client.
4. Click **Save & Apply**.

NOTE When you apply an EMM application policy, all of EMM application policies will be applied at the same time.

5. In the “Save Changes” window, click **OK**.

Applicable policies for EMM Client

The following policies are available for EMM Client:

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 EMM Client**: Locks the EMM Client.	Android iOS Windows 10
Use Lock Screen	Allows the use of the lock screen for the EMM Client.	Android iOS Windows 10
Install Area	Select where the EMM Client 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 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

Policy	Description	Supported devices
>> 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 EMM Client**: Locks the EMM Client.	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
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 EMM Client.	Android iOS
Limitation of the Download Screen Display in the Public Application	Limits the display of the download screens of public applications in the EMM Client. 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

Policy	Description	Supported devices
> 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
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. Navigate to **System** > **Windows10** > **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. Navigate to **System** > **Windows10** > **PPKG File Management**, and select a provisioning package.	Windows 10

Setting Secure Browser policies

The Secure Browser, that is equipped with enhanced security features plus basic web features, is a web browser for corporations. It blacklists harmful websites and blocks users from accessing them. It also enables you to configure browser features, such as saving cookies or cashes, as policies. You must first add Secure Browser as an EMM application and configure the policies. For more information about adding EMM applications, see Adding EMM applications.

To configure policies for Secure Browser, complete the following steps:

1. Navigate to **Setting** > **EMM Application and Policy** > **Secure Browser**.
2. On the "Secure Browser" page, click + and add an agent policy set.
   - You can add more policy sets by clicking +.
3. Configure the policy details. For more information about the applicable policies, see Applicable policies for Secure Browser.
   - The policy set will only apply to selected groups or organizations.
4. Click **Save & Apply**.
5. In the "Save Changes" window, click **OK**.

Applicable policies for Secure Browser

The following policies are available for Secure Browser. Apart from the policy, Secure Browser supports pop-up window, location display, and cover keyboard functions.

Policy	Description	Supported devices
Use Secure Browser App	Allows use of the Secure Browser application.	Android, iOS
Remove available of Secure Browser	Allow user to remove Secure Browser app on the device.	Android
Hide URL	Allows the use of Hide URL where the address bar of the Secure Browser is deleted. Tap the Secure Browser icon to call the set home URL. To use this policy, the homepage URL must be set, and the file download policy is automatically disallowed.	Android

Policy	Description	Supported devices
Homepage URL	Set the homepage that appears when the device users start Secure Browser or click the home button on Secure Browser.	Android, iOS
> Force to apply Homepage URL	Locks the default homepage URL for the Secure Browser for all users. **NOTE** Users cannot change the homepage URL if this policy is set.	Android, iOS
URL Control Type	Set whether to allow or block certain URLs in Secure Browser. • **Allowlist**: Set URLs to allow in Secure Browser. • **Blocklist**: Set URLs to block in Secure Browser.	Android, iOS
URL Control List	Set the list URLs to allow or block. The URL address is classified as Schema (http, https), SubDomain (www), Domain (domain.com), and Path (after /). To allow or block all websites of certain URLs, use the following example. Ex) *.domain.com/* • To add a URL, enter the URL, and then click +. • To delete a URL, select a URL, and then click 🗑. **NOTE** If the **URL Control Type** is **Allowlist**, you need to allow the camera access and voice recording permissions on devices with Android 13 or higher to use the Web Cam feature on allowed websites.	Android, iOS
Link URL to the Other Apps	Allows downloading or running applications directly by tapping URLs on webpages. The URLs that have been added via Secure Browser include "intent://" or "market://". Then, when a user taps an application, they are connected to the application automatically. A "market://" URL opens the relevant page by launching Google Play, while an "intent://" URL allows the user to open a new browser page from the application.	Android, iOS
Cache	Allows there to be a store cache in the Secure Browser.	Android, iOS

Policy	Description	Supported devices
‘User Agent’ Settings Key Value	Set the User Agent settings key value which allows the Secure Browser to access the web server and the User Agent key values contained in the HTTP header. • The User Agent settings key value is a string used to distinguish which browser is making a request to connect to the webpage. **NOTE** User Agent key settings can be used to detect accessing non-Secure Browsers on the web server.	Android, iOS
Cookies	Allows accepting cookies in the Secure Browser and configuring the cookie settings.	Android, iOS
File Download	Allows downloading files in the Secure Browser. If you use the Tiny mode, the file download policy is automatically set to **Disallow**.	Android, iOS
Text copy	Allows copying text.	Android, iOS
Screen Capture	Allows using screen capture.	Android, iOS
JavaScript	Allows running Javascript in the Secure Browser and configuring the Javascript settings.	Android
Browser Template Auto Entry	Allows using Autofill in the Secure Browser and to configuring the Autofill settings.	Android
View Security Alert	Allows displaying security alerts in the Android Security Browser and viewing security alerts.	Android
HTTP proxy	Allows using Http Proxy in the Secure Browser. You can also set an IP for the Http Proxy.	Android
> IP/Domain : PORT	Sets the proxy server IP, domain address, and port.	Android

Setting SecuCamera policies

SecuCamera is a camera application with enhanced security. It prevents sensitive data leaks by sending the photo to a specified server or email address immediately after the EMM user takes a photo.

To use SecuCamera, a security camera license is required. Navigate to **Setting** > **Server** > **License**, click the license key with an EMM type, and then check **SecuCamera Count** on the "License Detail" page. If the SecuCamera license is set to unlimited in SecuCamera under **Setting > Server > Configuration**, SecuCamera can be enabled for all users. If the SecuCamera license is set to limited, navigate to **Setting > License**, click **EMM License**, and check **SecuCamera Count** on the "License Detail" page.

You must first add SecuCamera as an EMM application and configure its policies. For more information about adding EMM applications, see Adding EMM applications. If a user in a group or organization that is assigned with policies wants to use SecuCamera, the user must be assigned the SecuCamera feature. For more information about security camera installation and use, see the Samsung SDS EMM User's Guide.

1. Navigate to **Setting** > **EMM Application and Policy** > **SecuCamera**.
2. On the "SecuCamera" page, click + and add a SecuCamera policy set.
   - You can add more policy sets by clicking +.
3. Configure the following policies for SecuCamera.

Policy	Description
Use SecuCamera App	Allows use of the SecuCamera application.
Remove available of SecuCamera	Allow user to remove SecuCamera app on the device.
Configuration File	Select between **Use** or **Do not use** to apply the settings file to the application.
> INI file	Register as INI files by setting the SecuCamera server address, use of WaterMark, and whether to modify the email subject. For more information, see INI Setting.

   - The policy set will apply to only selected groups or organizations.
4. Click **Save & Apply**.
5. In the "Save Changes" window, click **OK**.

INI Setting

Set the SecuCamera server address, use of WaterMark, and whether to modify the email subject in an INI file.

Refer to the following example for setting the INI file.

```
[Info]
Address = https://127.0.0.1
[UseMark]
UseMark = false
[FinishTimer]
FinishTimerSec = 60
[Title]
UseCustom = true
```

- **Address**: Set the address of the SecuCamera server.
- **UseMark**: Whether or not to use watermarks on photographed images that are sent via email.
  - When a watermark is in use, the user's email address, email send date, or text entered by the IT admin is displayed in the center of images.
  - watermark.format= Enter one of the following numbers depending on the watermark display format.
    - 0: Do not use
    - 1: User's email address
    - 2: Email send date
    - 3: Specific text
  - watermark.custom= The IT admin enters text that should be used as the watermark (50 bytes).
- **FinishTimerSec**: If the SecuCamera application doesn't function for the specified period of time set in seconds, it closes automatically. If left unspecified, the default value of 60 seconds is used.
- **UserCustom**: Set whether to modify the email subject.
  - true: The user can modify the email subject when sending photos after shooting with SecuCamera.
  - No setting or false: The user cannot modify the email subject. For more information, see Configuring the SecuCamera server in the "Samsung SDS EMM Installation Guide".

Setting Knox Portal policies

Knox Portal is a business mail application that Samsung companies use at work. Navigate to **Setting** > **Server** > **License**, click the license key with an EMM type, and then check **Samsung Group** is in use on the "License Detail" page. You must first add Knox Portal as an EMM application and configure the policies. For more information about adding EMM applications, see Adding EMM applications. Knox Portal allows you to configure policies that can limit email viewing, attaching and downloading files, or syncing schedules or contacts with devices.

When users run Knox Portal applications in the EMM Client, their devices are controlled by the specified policies.

To configure policies for Knox Portal, complete the following steps:

1. Navigate to **Setting** > **EMM Application and Policy** > **Knox Portal**.
2. On the “Knox Portal” page, click + and add a Knox Portal policy set.
   - You can add more policy sets by clicking +.
3. Configure the policy details. For more information about the applicable policies, see Applicable policies for Knox Portal.
   - The policy set will only apply to selected groups or organizations.
4. Click **Save & Apply**.
5. In the "Save Changes" window, click **OK**.

Applicable policies for Knox Portal

The following policies are available for Knox Portal:

Policy	Description	Supported devices
Use Knox Portal App	Allows using Knox Portal applications.	Android
Remove available of Knox Portal	Allow user to remove Knox Portal app on the device.	Android
View Attachments of Incoming Mails	Allows viewing and accessing email attachments received from Knox Portal.	Samsung Knox 1.0 higher
View Attachments of Outgoing Mails	Allows viewing and accessing the attachments of outgoing mail sent by Knox Portal.	Samsung Knox 1.0 higher
View Outgoing Mails	Allows viewing and accessing outgoing mail sent by Knox Portal.	Samsung Knox 1.0 higher
View Mails Sent to Yourself	Allows viewing and accessing emails sent to you from Knox Portal.	Samsung Knox 1.0 higher
View Attachments of Out-tray / In-tray Mails	Allows viewing and accessing attachments of pending or approved documents in the electronic document approval system.	Samsung Knox 1.0 higher
View the Message of Out-tray / In-tray Mails	Allows viewing and accessing messages of pending or approved documents in the electronic document approval system.	Samsung Knox 1.0 higher
Specify Interval between synchronizations of Your Inbox	Set the synchronization period for emails received from Knox Portal. • 3 days	Samsung Knox 1.0 higher
Search Employee	Allows viewing and searching for employee information in Knox Portal.	Samsung Knox 1.0 higher
Activate Schedule Synchronization	Allow use of schedule and activating schedule synchronization in Knox Portal.	Samsung Knox 1.0 higher
Activate Contact Synchronization	Allows the use of contacts and activating contact synchronization in Knox Portal.	Samsung Knox 1.0 higher
Set Whether to Show Logout Button on The Lock Screen	Allow clicking of the logout button to log out when the screen is locked. If it is allowed, the logout button is activated.	Samsung Knox 1.0 higher
Lock Screen Timeout Period	Set the screen lock period of Knox Portal. The value can be between 0 – 1800 seconds.	Samsung Knox 1.0 higher

Configuring the Keepalive settings

Set up Keepalive to check the connection between the EMM server and the device. Keepalive sends and receives a message to check whether the data link is normal between devices and to prevent the data link from being broken. The EMM server periodically checks the connection between the server and the device through Keepalive.

To configure the Keepalive settings, complete the following steps:

1. Navigate to **Setting** > **Keepalive**.
2. Click next to **Keepalive** to enable the feature.
3. Select the target type.
   - **Global Setting**: Applies the Keepalive settings to all groups or organizations.
   - **Set by Group** / **Organization**: Applies the Keepalive settings to selected groups or organizations.
4. Configure the Keepalive settings.
   - **Keepalive Expiration (days)**: Set the period to check the connection status between the EMM server and the device. If no communication is established between the EMM server and the device during the set period, the connection is tried directly with the terminal during the Keepalive check period. For more information, see List of environment settings.
   - **Keepalive Interval (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**.

Managing administrator accounts

Add and manage other administrators' accounts. Management of administrator accounts includes changing passwords and selecting profiles and organizations to manage for administrators.

Administrators in EMM 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.

You can view the available EMM Admin Portal's menus and permissions by administrator type. For more information, see Viewing available menus by administrator type.

Adding an administrator

To add an administrator account, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Administrator**.
2. On the “Administrator” page, click  .
3. In the “Add Administrator” window, 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.
   - **Mobile Number**: Enter the mobile phone number of the administrator.
   - **Email**: Enter the email address of the administrator.
   - **Type**: Select the administrator type.
   - **Managing Permission**: Select the administration rights to give to the administrator.
     - You can view, add, modify, or delete permissions from the menus defined for each permission in **Setting** > **Admin Console** > **System**.
     - Only the administrators who have been granted the Service Desk Managing Permission can use the Mobile Admin Portal. To learn more about the Mobile Admin Portal, see Using Mobile Admin.
4. Click **Save**.

> **NOTE** To perform CAC Sign-In in the EMM Admin Portal, you must register the "User Logon Name" value among the user attributes that are registered in AD DS as an Admin ID. For more information, see CAC Sign-In.

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** > **Admin Console** > **Administrator**.
2. On the “Administrator” page, click  in the row of the administrator you want to change the password of.
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** > **Admin Console** > **Administrator**.
2. On the “Administrator” page, click in the row of the sub-administrator you want to give profiles to manage to.
3. In the “Select Profile” window, click the checkbox for profiles on the profile list, and then click .
   - To delete the selected profiles from the selected profile list, click the checkbox for the profiles and then click .
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** > **Admin Console** > **Administrator**.
2. On the “Administrator” page, click in the row of the sub-administrator you want to give organizations to manage to.
3. In the “Select Organization” window, select an organization from the organization list and click **Update**.
   - To select and add multiple organizations at once, click the organizations while holding down the Ctrl key and click **Update**.
   - To delete the selected organizations from the assigned organization list, click the checkbox for the organizations, and then click .
4. Click **Save**.

Activating administrator accounts

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

To activate administrator accounts, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Administrator**.
2. On the “Administrator” page, click **Inactive** in the row of the administrator you want to activate.
3. In the "Change Status" window, click **OK**.

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

Viewing available menus by administrator type

The EMM menu displayed on the EMM Admin Portal may vary depending on the manage permissions (administrator). All the menus managed on the EMM Admin Portal can be used by the super administrator. Sub-administrators can only use their assigned menus. Read-only administrators can only view all the menus. Check the required manage permissions (administrator) by menu.

To see the required manage permissions by EMM menu, complete the following steps:

To see administrator-specific system menus by type, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **System**.
2. Select **Top Level Menu**.
3. Enter the menu name and press Enter or click .

12

Monitoring

Monitoring

Monitor the data in the EMM server, such as the device status, user status, and so on. You can also check the status of EMM using audits, alerts, and history.

This chapter explains the following topics:

Setting the dashboard

After you sign in to the Admin Portal, the dashboard consisting of various reports appears. Three basic types of dashboard are provided and, in addition, you can create a new, customized dashboard by selecting the reports you wish to see.

Basic dashboards

Three basic types of dashboard are as follows:

Default dashboard

- **Device Status**: Displays the number of mobile and Tizen Wearable devices by status and net changes in the total number of devices. Click the number to view the devices in detail.
- **Compliance Violation**: Displays the number of mobile devices with compromised OSs, compromised applications, unapplied profiles and malware. Click the number to view the devices.

Item	Description
Compromised OS	A mobile OS is regarded as compromised in the following cases: • When a device is suspected of being a rooting device (e.g. SuperUser authority) by the EMM internal logic • When a device is suspected to have been compromised as a result of Attestation (Knox API inspection for OS compromise) Inspection for a compromised OS is performed whenever the EMM Agent is restarted or when any policies are applied on mobile devices.
Compromised App	An application is regarded as compromised in the following cases: • When the application's hash value (CRC) is different from the one registered on the Admin Portal • When you install the application on a device without registering it on the Admin Portal Inspection of compromised applications is performed whenever an application is installed or updated.
No profile	Devices without profiles are counted.
Malware	Devices where malware is detected are counted.

- **Platform Type**: Displays the number of activated devices by mobile and Tizen Wearable OS. Click the number to view the devices in detail.
- **Daily Activation**: Displays the current numbers of activated devices and users and net changes in the numbers.
- **Users by Organization**: Displays the number of activated users by organization in descending order. Click **See Detail** to view the organization list.
- **Device Command History**: Displays the number of device commands sent from the Admin Portal and its change on a daily or weekly basis. Click **See Detail** to view the device command history list.
- **License**: Displays the validity period of the EMM service, the total number of devices that can be activated, and the number of activated devices. Depending on the type of license used on the site, the validity period, the total number of devices that can be registered, and the number of activated KPE-Premium, KPE-Standard, KPE-Dual DAR, E-FOTA, or Tizen Wearable KPE-Premium devices will also be displayed. In addition, the Anti-Malware Service shows the validity period only. Click **See Detail** to see a list of license information.
- **Certificate**: Displays the total number of external certificates that are registered on the EMM Admin Portal and the number of external certificates that are scheduled to expire in a week.

EMM dashboard

- **New User Weekly**: Displays the users newly added within a week.
- **App Download Top3 (Current)**: Displays the three most downloaded applications up to the current date.
- **Device Count by Platform**: Displays the number and ratio of activated devices by mobile OS. You can exclude/include the item to display by clicking the chart legend.
- **Device Count by Status**: Displays the number and ratio of activated devices by status. You can exclude/include the item to display by clicking the chart legend.

Viewing another dashboard

To view another dashboard, complete the following steps:

1. Navigate to **Dashboard**.
2. On the right top of the screen, click the drop down field displaying the current dashboard name.
3. Click a dashboard you want to view.
    - If the selected dashboard is the one that you have created, the modification icon () next to the field is activated for modifying the dashboard. For more information about modifying the dashboard, see Modifying dashboards.

Adding a dashboard

To add a new dashboard, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Dashboard Management**.
2. On the “Dashboard Management” page, click +.
3. In the “Add Dashboard” window, enter the dashboard information:
   - **Dashboard ID**: Enter the ID for the new dashboard.
   - **Dashboard Name**: Enter the dashboard name.
   - **Description**: Enter a description for the dashboard.
   - **Column**: Select the number of columns you want to divide the dashboard area into.
   - **Layout**: Select whether to fix the height of each report portlet or adjust the height according to the screen ratio.
4. Select a report you want to add from the report list and click → to add them to the “Dashboard Setting” area.
   - To select and add multiple reports at once, click the reports while holding down the Ctrl key and click →.
   - Up to 10 reports can be added. For more information about each report, see Report list.
   - To rearrange the selected reports in the “Dashboard Setting” area, drag a report to a desired location within the area.
5. Click **Details** at the top of the window.
6. Click each selected report and configure their settings.
   - **Report Form**: Select whether to display data through a table or a chart.
   - **Refresh Interval**: Select the refresh interval for the report from 1 to 24 hours.
7. Click **Save**.
   - On the dashboard list, you can click to view the preview of the dashboard.

Adding a dashboard based on an existing dashboard

To copy an existing dashboard to create a new dashboard, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Dashboard Management**.
2. On the “Dashboard Management” page, click in the row of the dashboard you want to copy.
3. In the “Copy Dashboard” window, enter the dashboard information.
   - You must enter a new ID for this dashboard, but you can keep or change the dashboard name and other information.
4. Modify the existing reports in the “Dashboard Setting” area.
   - You can add another report and delete and rearrange the existing reports.
5. Click **Details** at the top of the window and modify the settings of the selected reports.
6. Click **Save**.
   - On the dashboard list, you can click to view the preview of the dashboard.

Managing dashboards

Change the main dashboard, which is displayed on the homepage, or modify existing dashboards.

Setting main dashboard

To set a dashboard as the main dashboard, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Dashboard Management**.
2. On the “Dashboard Management” page, click in the row of the dashboard you want to set as the main dashboard.
3. In the “Confirm” window, click **OK**.

Modifying dashboards

Modify the newly added dashboards. Basic dashboards cannot be modified.

To modify dashboards, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Dashboard Management**.
2. On the “Dashboard Management” page, click in the row of the dashboard you want to modify.
3. In the “Modify Dashboard” window, modify the existing information.
   - In the **Basic** tab, you can change basic information, such as the name, number of columns, layout, and reports.
   - In the **Details** tab, you can change the detailed information of each selected report.
4. Click **Save**.

Deleting dashboards

Delete the newly added dashboards. Basic dashboards cannot be deleted.

To delete dashboards, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Dashboard Management**.
2. On the “Dashboard Management” page, click in the row of the dashboard you want to delete.
3. In the “Delete” window, click **OK**.

Viewing reports

Reports provide information about devices, users, applications, and profiles and help take appropriate action when necessary. EMM offers various reports by default. In addition, you can add new reports using the report queries provided by EMM.

Viewing a report

View the information in a report. Displayed information can be filtered when you enter conditions.

To view a report, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Report**.
2. On the "Report" page, click  in the row of the report you want to view.
3. View the information in each tab.

Tab	Description
Table	The data is displayed in a table. • Click **Refresh** to view the updated information. • Click **Export** to export the information to an Excel file. • Click **Modify Input Value** to enter conditions and filter the information. For more information, see Entering input values.
Chart	The data is displayed in a chart. • Click **Save an image** to save the chart as an image file.

Entering input values

When you click **Modify Input Value** on the Table tab, the “Input Report Values” window appears to allow you to enter conditions. The input value you can enter varies depending on the data type of the report field.

1. In the “Input Report Values” window, hover the mouse over each report field in the table to find out the data type of the field.
   - A data type from among string, number, or date will appear.
2. Enter a condition depending on the data type in the input value field.

Data type	Description
String	Enter a character manually as an input value.
Number	Enter a number manually as an input value.
Date	In the Condition Type column, select either **Constant** or **Variable**. • If you selected **Constant**, enter the date (YYYY-MM-DD) manually. • If you selected **Variable**, enter values for the **Date Type**, **Before and After**, and **Detailed Setting**. – **Date Type**: Reference point for date setting. Select either **This Day** or **This Month**. – **Before and After**: Value to calculate the time from the reference point. Enter a negative or positive number. For example, if you enter “-1,” it means one day or one month ago. – **Detailed Setting**: Value for further specifying the calculated time. If **This Day** is selected, you can specify the time of the day. If **This Month** is selected, you can specify the day of the month.

3. Click **View Result**.
4. In the “Message” window, click **OK**.

Report list

The default reports are as follows. For the input values of reports, the input field values of the report queries or the key values of the master data are used. For more information, see Report queries list or Managing master data. You can find the key values, such as Platform, Ownership, or Device Status, in **Setting** > **Server** > **Master Data**.

Report name	Description	Report query
New Registered Users	Displays the newly added users.	User Basic Information
New Registered Users(C)	Displays the daily number of newly added users in a table and chart.	
New User Weekly	Displays the users newly added within the week.	
Device Inventory	Displays the inventory of the activated devices.	Device Basic Information
Apps Installed on Device	Displays the number of applications installed per device.	
Device Count by Version	Displays the number of activated devices by mobile OS and their version.	
Device Count by Status	Displays the number of activated devices by status.	
Device Count by Platform	Displays the number of activated devices by mobile OS.	
Device Count by Manufacturer	Displays the number of activated devices by mobile device manufacturer.	
User Count by Group	Displays the number of users by group.	User by Group
Device Count by Group	Displays the number of devices by group.	Device by Group
Device Security Status	Displays the security information, such as whether the device is compromised or the Keepalive status, by device.	Device Security Status
Device SIM/Roaming Status	Displays the detailed information about the SIM card and roaming status of devices.	Device Details Information
Activated Device Count per App Installed	Displays the number of devices on which an application is installed by application.	App Information Installed in Device
Device Command in Request	Displays the target device information of the device commands in queue.	Device Command in Request

Report name	Description	Report query
Device Command Queue Count	Displays the number of the device commands in queue per device in descending order.	Device Command Queue Count
New Registered Apps	Displays the applications newly added within the week.	App Basic Information
App Download Ranking (Current)	Displays the current ranking by application downloads.	App Download Ranking (Current)
App Download Top3 (Current)	Displays the three most downloaded applications up to the current date.	
App Download Ranking (Stats)	Displays the application download rankings of the previous day.	App Download Ranking (Stats)
App Download Top3 (Stats)	Displays the three most downloaded applications of the previous day.	
Profile Details by Device	Displays the profile list by device.	Profile Details by Device

Adding a report

Add a new report using report queries. Report queries are for filtering data or viewing statistics from the aggregate table in the EMM database.

To add a new report using report queries, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Report**.
2. On the "Report" page, click +.
3. In the "Add Report" window, enter the report information:
   - **Report ID**: Enter the ID for the new report.
   - **Report Name**: Enter the report name.
   - **Description**: Enter a description for the report.
   - **Report Queries**: Select the report query for the report. For more information, see Report queries list.
   - **Chart Type**: Select the chart type of the report. Click the checkbox next to **Legend** to display the chart legend and select its location.
4. Select a report field you want to add from the query fields list and click → to add them to the "Output Fields" area.
   - To select and add multiple report fields at once, click the fields while holding down the Ctrl key and click →. You can also click ⇒ to add all the report fields on the list.
   - To delete the selected report fields from the "Output Fields" area, click ←. You can also click ⇐ to delete all the selected report fields.
   - To rearrange the selected report fields in the "Output Fields" area, click one of the fields and click ↑ or ↓.
5. Configure the detailed settings of the selected fields depending on their data types.

Data type	Setting
String (A)	• **Output Name**: Change the field name if necessary. • **Chart Setting**: Select the field as the chart category if you want to display the chart.
Number (1)	• **Output Name**: Change the field name if necessary. • **Output Format**: Select the number display format. • **Chart Setting**: Select the field as the chart series or category if you want to display the chart. • **Summary Type**: Select the numeric value to display on the chart from among sum, average, maximum, and minimum.

Data type	Setting
Date ( )	• **Output Name**: Change the field name if necessary. • **Output Format**: Select the date display format. • **Chart Setting**: Select the field as the chart category if you want to display the chart.

6. Click **Save**.

Adding a report based on an existing report

To copy an existing report to create a new report, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Report**.
2. On the “Report” page, click in the row of the report you want to copy.
3. In the “Copy Report” window, enter the report information.
   - You must enter a new ID for this dashboard, but you can keep or change the dashboard name and other information.
4. Modify the existing report fields in the “Output Fields” area.
   - You can add another field and delete and rearrange the existing report fields.
   - You can modify the detailed settings of the selected fields.
5. Click **Save**.

Report queries list

The default report queries are as follows. Each report query has input fields and output fields. Output fields are used as elements included in reports. Input fields are the example for input values when entering conditions of reports.

Report query	Output field		Input field
App Basic Information	• Category • App Name • App Version Code • App Version • Package • App Type Code • App Type • App Status • Status • Platform	• Test App • Kiosk App • Supporting Devices • Supporting Devices • Grade • Valid from • Valid To • Registration Date • Download • Source	• LANG – Input value: ko, en, zh • APP_NAME • APP_PLATFORM – Input value: Master Data's Platform key • APP_TYPE – Input value: IA, PA (IA: Internal application, PA: Public application) • IS_ACTIVATED • IS_TEST – Input value: Y, N • IS_KIOSK – Input value: Y, N • DEVICE_TYPE – Input value: A, P, T (A: All devices, P: Phone-only, T: Tablet-only) • ENROLL_DAYS
Profile Details by Device	• Tenant ID • Device ID • Device name • User ID • User Name • Email • Platform Code • Platform • Device Status Code • Device Status • Serial Number • MAC Address	• IMEI • Manufacturer • Model • OS Version • Ownership code • Target Type • Assigned Group / Organization Group • Inherited Profile • Profile ID • Profile Name • Priority • Device Tag	• PLATFORM_TEXT • DEVICE_STATUS_TEXT • DEVICE_NAME • USER_ID • USER_NAME • DEVICE_TAG

Report query	Output field		Input field
App Download Ranking (Current)	• Ranking • Statistics Date • Category • App Name • App Version Code • App Version • Package • App Type Code • App Type • App Status • Status	• Platform • Test App • Kiosk App • Supporting Devices • Supporting Devices • Grade • Valid from • Valid To • Registration Date • Download	• LANG • RANK
App Download Ranking (Stats)	• Ranking • Statistics Date • Category • App Name • App Version Code • App Version • Package • App Type Code • App Type • App Status • Status	• Platform • Test App • Kiosk App • Supporting Devices • Supporting Devices • Grade • Valid from • Valid To • Registration Date • Download	• LANG • RANK

Report query	Output field		Input field
App Download Statistics	• Tenant ID • Statistics Date • App ID • App Name • Category ID • Category • App Version Code • App Version • Package • App Type Code • App Status • Platform • Supporting Devices • Auto Update	• Test App • Kiosk App • Grade • Valid from • Valid To • Registration Date • Download Total • Download Last Year • Download Last 6 Month • Download Last 3 Month • Download Last 1 Month • Creation Date	• FROM_DATE • TO_DATE
App Information installed in Device	• Package • App Name • App ID • EMM • App Version Code • App Version • Device ID • Mobile ID • User ID • Platform	• Device Tag • Platform • Device Status • Status • Device Count • Compromised Count • Installed Area • App Size • Mandatory • No. of execution	• DEVICE_STATUS - Input value: BS, A, BL, P, I (BS: Disconnected, A: Enrolled, BL: Expired, P: Provisioned, I: Unenrolled) • IS_NOT_LATEST - Input value: Y, N • DEVICE_TAG

Report query	Output field		Input field

Device Basic Information	• Device ID
	• Mobile ID
	• User ID
	• User Name
	• Organization Code
	• Organization Name
	• Ownership code
	• Ownership
	• Platform
	• Platform
	• Network Service Provider Code
	• Network Service Provider Name
	• Device Version
	• Device Version code
	• Device Version
	• Phone
	• Model
	• Device OS
	• Device Status
	• Status
	• Modem Firmware
	• Build Number
	• Build Type
	• Product Name
	• Device Kind
	• Manufacturer
	• Device Organization
	• Device Name
	• SD Card Encryption
	• Device Encryption
		• Creation Date
		• Present device management profile applied date
		• Last Connection Date
		• Whether to be compromised
		• App Count
		• Compromised App Count
		• Official App Count
		• Whether the app to be compromised
		• Battery Level (%)
		• Memory Size (GB)
		• Memory Usage (GB)
		• RAM Memory Size (GB)
		• RAM Memory Usage (GB)
		• AP Type
		• AP Speed (GHz)
		• Network transfer data (in) (MB)
		• Network transfer data (out) (MB)
		• Wi-Fi transfer data (in) (MB)
		• Wi-Fi transfer data (out) (MB)
		• Device Count
		• Device Tag
			• USER_ID
			• USER_NAME
			• ORG_CODE
			• ORG_NAME
			• OWNERSHIP
			  - Input value: Master Data's Ownership key
			• PLATFORM_CODE
			  - Input value: Master Data's Platform key
			• VERSION
			• STATUS
			  - Input value: BS, A, BL, P, I (BS: Disconnected, A: Enrolled, BL: Expired, P: Provisioned, I: Unenrolled)
			• MANUFACTURER
			• MODEL
			• IS_ROOTING
			  - Input value: Y, N
			• UNCONNECTED_DAYS
			• ACTIVATION_TYPE
			• DEVICE_TAG

Report query	Output field		Input field

Device by Group	• Group ID
	• Group Type code
	• Group Type
	• SD Card Encryption
	• Device Encryption
		• Target Type code
		• Target Type
		• Device ID
		• Mobile ID
		• Device Count
		• Device Tag
			• GROUP_ID
			• GROUP_TYPE
			  - Input value: User, Device, SYNC
			• TARGET_TYPE
			  - Input value: 0, 1 (0: User Member, 1: Device Member)
			• DEVICE_TAG

Device Command in Request	• Sent Date • Mobile ID • Platform Code • Platform • Device Status Code • Status • User ID	• User Name • IMEI • Phone • Transfer target • Device Command Type • Queue Count • Device Tag	• PLATFORM_CODE - Input value: Master Data's Platform key • MOBILE_ID • USER_ID • DEVICE_TAG
Device Command Queue Count	• Ranking • Mobile ID • Platform Code • Platform • Device Status Code • Status • User ID	• User Name • IMEI • Phone • Queue Count • Last Device Command • Last Sent Date • Device Tag	• PLATFORM_CODE - Input value: Master Data's Platform key • MOBILE_ID • USER_ID • LAST_DAYS • DEVICE_TAG

Report query	Output field		Input field
Device Details Information	• Mobile ID • User ID • User Name • Email • Organization Name • Ownership code • Device Status Code • Status • Platform Code • Platform • Device Version • Phone • MAC Address • Model • Firmware • IMEI • Serial Number • Device Tag • SD Card Encryption • Device Encryption	• ICCID • SIM Status • SIM Country • SIM Network • Roaming Status • Current Country • Current Network • Voice Roaming • Data Roaming • IMSI • Device OS • Device ID • Telephone Type • Network Type • Modem Firmware • Manufacturer • Device Type • Device Count	• USER_ID • USER_NAME • ORG_NAME • PLATFORM_CODE - Input value: Master Data's Platform key • DEVICE_STATUS_CODE - Input value: Master Data's Device Status key • ACTIVATION_TYPE • DEVICE_TAG
Device Security Status	• Device ID • Mobile ID • User ID • User Name • Platform Code • Platform • Device Status Code • Device Status • Compromised Device Status • SD Card Encryption • Device Encryption	• Lock Status • Locked Time • Unmanaged Status • Unmanaged Time • Device Count • Last Device Command • Last Device Command Status • Device Tag	• USER_ID • PLATFORM_CODE - Input value: Master Data's Platform key • DEVICE_STATUS_CODE - Input value: Master Data's Device Status key • ROOTING_STATUS - Input value: Modified, Official • LOCK_STATUS - Input value: Locked, Unlocked • UNMANAGED_STATUS - Input value: Managed, Unmanaged • DEVICE_TAG

Report query	Output field		Input field

User Basic Information	• User ID
	• User Name
	• Email
	• Contact
	• Organization Code
	• Organization Name
	• Company Code
	• Company Name
	• Position Code
	• Position Name
		• Site Code
		• Site Name
		• Security Level Code
		• Security Level
		• Enabled
		• Status
		• Registration Date
		• User Count
		• Number of Enrolled Devices
		• Number of Registered Devices
			• USER_ID
			• USER_NAME
			• ENABLED
			  - Input value: 0, 1 (0: Deactivated, 1: Activated)
			• REGISTERED_DAY
			  - Input value: Number (e.g. “7” means that list of users for last 7 days from current date)

User by Group	• Group ID
	• Group Type code
	• Group Type
	• Target
		• Type code
		• Target Type
		• User ID
		• User Name
		• User Count
			• GROUP_ID
			• GROUP_TYPE
			  - Input value: User, Device, SYNC
			• TARGET_TYPE
			  - Input value: 0, 1 (0: User Member, 1: Device Member)

Managing reports

Modify or delete the newly added reports. The default reports cannot be modified or deleted.

Modifying reports

To modify the newly added reports, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Report**.
2. On the “Report” page, click  in the row of the report you want to modify.
3. In the “Modify Report” window, modify the existing information.
4. Click **Save**.

Deleting reports

To delete the newly added reports, complete the following steps:

1. Navigate to **Setting** > **Admin Console** > **Report**.
2. On the “Report” page, click  in the row of the report you want to delete.
3. In the “Delete” window, click **OK**.

Adding a notice

Add a notice for device users. When you add multiple notices, the notice periods cannot overlap. English, Chinese, and Korean are the supported languages for notifications. On user devices, notices are displayed in the language that the user sets when signing in to EMM. Notices written in English will be displayed for unsupported languages.

To add a notice, complete the following steps:

1. Navigate to **Service Overview** > **Notice**.
2. On the “Notice” page, click  .
3. Set the notice period and enter the notice information.
    - 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**.

Viewing audits

EMM provides audit service to monitor all tasks and records which occur while operating EMM. The tasks performed by auditing targets are called audit events, and they are defined in the EMM system. The events which occur on the Admin Portal, the server, or activated mobile devices are recorded in the log. Audit logs can be saved in the EMM server or remote log server. To send them to a remote server, you must configure the remote log server. For more information, see Configuring the audit log server.

Understanding audit events

Audit events can be categorized by their point of occurrence and severity.

Occurrence point

- Console: Includes the events that occurred in the Admin Portal, such as the administrator's login, the management of policies and applications, and the connection of integrated systems.
- Device: Includes the events that occurred on mobile devices, such as device login, certificate issuance, and the reception of device commands. If the audit log file on a device exceeds the size limit, the file is sent to the server automatically and the audit logs are recorded in a new file.
- Server: Includes the request and respond events that occurred on the EMM server when the server and mobile devices communicate. The scheduled tasks on the server are also included.
- System: The events including EMM server booting or shut-down, encryption, and so on from EMM server logs.

Severity level

Level	Name	Description
High	Critical	Indicates that the event is a serious error. Your immediate action is required.
	Error	Indicates that the event is a general error. Your action is required but not urgent.
	Warning	Indicates that the event may potentially cause a problem.
	Notice	Indicates that you should be aware of the event.
	Info	Indicates that the event is for general information.
Low	Debug	Indicates that the event is defined in detail for developers.

NOTE To receive an alert about an audit event, set the alert level lower than the severity level of the audit event. For more information, see Configuring alerts.

Setting audit events

To set audit events to be recorded in the audit logs, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Audit Event**.
2. On the "Audit Event" page, click the checkbox for the audit events you want to set as auditing targets.
   - The severity of the selected audit events are recorded in the logs based on the value in the Level column if the events are successful, and based on the value in the Fail Level column if the events fail.
   - For more information about audit event types and event categories, see Audit event classification.
   - You can cancel the selected auditing targets by removing the checkmark.
3. Click  .
4. In the "Set Audit target" window, click **OK**.

Viewing audit logs

Audit logs are recorded in a log file for each server. See Audit logs of Push and AppTunnel for more information about audit logs recorded on the Push and AppTunnel server.

NOTE If the Audit Log Retention Period (Days) and Log File Retention Period (Days) of the LOG classification in **Setting** > **Server** > **Configuration** are set, the audit logs that have passed the retention period will not be searched. For more information, see List of environment settings.

To view the log of audit events, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Audit Log**.
2. Search for the audit logs you want to view.
   - You can search for audit logs by selecting the audit event type and the log period.
     - Audit Type: Select the audit event type. **Console/Server** includes the history of device commands sent from the Admin Portal and the changes made due to batch tasks on the server. **Device** includes the history of policies applied to mobile devices, device activation, and the event occurred on devices, such as revoking the activation of the EMM Agent. **System** includes occurrences of any VPP synchronizations, audit logs, or events added using the Inventory schedule or MDM scheduler monitor in the EMM Admin Portal.
     - Log Date: Select the start and end date of the log period. The end date can be up to 30 days from the start date.

- You can also search for audit logs by using the search field. Search within search results is available.

3. View the audit logs.
   - The **User ID** field displays the source of the audit event. If the audit event type is **Console/ Server**, refer to the following information:
     - When the audit event occurs while sending a device command or operating EMM, the administrator's ID is displayed.
     - When a device command is sent, the administrator's ID is displayed.
     - When a scheduled task is performed on the server, "SYSTEM" or the batchuser ID is displayed.
   - The **Device Name** field displays the name of the device on which the audit event occurred. If there is no device or the audit event is a scheduled task, blank is displayed.
   - The **View** field displays the request ID. The request ID helps to track how the audit event is applied to a device. The first three letters of the request ID complies with the following rule:
     - The first letter: Mobile OS of the device (A: Android, I: iOS, W: Windows, T: Tizen Wearable)
     - The second letter: Application type (A: Android/iOS EMM Agent, C: iOS EMM Client)
     - The third letter: Start point of the process (S: Server, D: Device)

     E.g. AAS: The audit event started from the server and applied to the EMM Agent installed on the Android device.

4. To view the detailed flow of an audit event, click the request ID in the View field.

5. In the "Audit Event" window, view each audit log.
   - If you click **Detail** in the row of a log, you can view the following information.

Item	Description
Process	The detailed information displayed in the "Process" tab: • Request History: Request details of the Audit events. For example, the Device ID, Data Information, User Info, or Notification ID. • Result Code: Event process result code. • Result History: The detailed result of the audit event. - When you change a policy in the Admin Portal, a new event is recorded in the profile category. e.g.) When an Android policy is changed, all policy events to be saved in Request History of "Save General Policy" are shown. - For the "Package deletion failure" event, a package name and the reason for the failure appear in Result History.

Item	Description
Log Data	The detailed information about the event is displayed in “Log Data” under the condition below: • For **Console** type: When sending more than 4000 bytes of data from the device to EMM server. • For **Server** type: When Event Category and Event are as below. - Event Category: Device command - Event: Agent Request to lock screen (Device ⟶ Server) or Agent Request to unlock device (Device ⟶ Server) or Agent Request for work report (Device ⟶ Server) or Handle multiple devices by sending device control - When profile settings, such as Wi-Fi and VPN, are applied to devices, the “Agent Request for work report (Device ⟶ Server)” event will be shown. Click Log Data to view the details. • For **Device** type: When Event Category and Event are as below - Event Category: Device command - Event: Device Lock/Unlock History
Reason for Saving	It shows the reason why the audit log was downloaded as a CSV file.

Below are the detailed descriptions of audit events.

- TLS audit events in the EMM Admin Portal are when the device requests TLS communication from the EMM server. The initiator is the ATC (AppTunnel Client) because the device and the EMM server communicate through AppTunnel service for TLS communication. The “TLS HANDSHAKE ERROR” event occurs in the statuses below.
  - Certificate Ordering Fail
  - ExtendedKeyUsages Check Fail
  - Certificate SAN or DN Fail
  - Certificate CRL Check Fail
  - Certificate OCSP, CDP Check Fail
  - SSL Exception
  - The “Self test for cryptographic module” event is for checking the encryption integrity of the server encryption module (Crypto-J), and its provide results are shown on the **Process** tab. When an algorithm’s known answer test fails, which encryption has failed is recorded in **Result History**, such as “Crypto-J Self test AES has failed.” The targets for the encryption integrity check are as follows:
  - JarVerify, SHA512, AES, TripleDES, KDFTLS10, HMACDRBG, ECDRBG, FIPS186Random, DSA, ECDSA, CTRDRBG
- The “Integrity Error” event occurs when the EMM server starts or it’s executable codes are modified. This event checks whether the signed and distributed EMM codes are right. If an integrity error occurs, that file path and a list of corrupted files are shown on **Result History**.

NOTE

- You can set a limit on the number of audit records stored by the EMM Server. Navigate to **Setting** > **Server** > **Configuration**, click the **Audit** button across the top of the window, and specify the maximum number of audit records retained by the EMM Server in the **Audit Log Settings** area of the screen. When the number of audit records stored reaches 90% of the limit, the EMM Admin Portal shows a notification message. The audit records are stored although the limit has been reached. The EMM server stores its audit records in the storage provided by the environment, and deletion of audit records must be performed using operations in the environment.
- To display a service profile and download the log of a user agreement when in single-tenant mode, navigate to **Service Overview** > **Log and Event** > **Audit Log**, and when you are in multi-tenant mode, use the TMS Admin Portal. For more detailed information, see the Samsung SDS TMS Administration guide.
- To enable device audit logs to be viewable, navigate to **Setting** > **Server** > **Configuration** and click **Audit** and set **Bring device audit to DB** to TRUE. For more details, see Configuring the audit log server.

Exporting audit logs to an Excel file

Export audit logs and save them in an Excel file. Exported logs are not deleted from the EMM server.

To export audit logs to an Excel file, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Audit Log**.
2. On the “Audit Log” page, enter the Audit Type, Audit Collection Date, User ID, Device Name, or Event to search for audit logs.
3. Click **Export to CSV** to download the searched list.
4. In the “Export to CSV” window, enter the reason for downloading the audit log in Reason for Saving.
5. Click **OK**.

Audit event classification

The classification of audit events based on the type and event category is as follows. For more information about audit events, see Lists of audit events.

Event Category	Occurrence point			
	Console	Server	Device	System
AD/LDAP Sync	O	O		
Admin Login	O			
Administrators	O			
Alerts	O			
Android Enterprise	O	O		
Applications	O	O		
AppTunnel			O	
Certificate Status			O	
Certificates	O			
Compliance		O	O	
Connectors	O			
Cryptographic Support		O		O
Dashboard	O			
Devices		O	O	
Device Command	O	O	O	
Device Enrollment Program	O	O		O
Devices	O	O		
E-FOTA	O	O		
Email	O	O		
EMM Agent			O	
EMM Client			O	
EMM System				O
Enrollment		O	O	
Groups	O			
Integrations	O			
InventoryScheduler		O		

Event Category	Occurrence point			
	Console	Server	Device	System
Kiosk Launcher			O	
License Management		O		
Logs	O	O	O	O
Network Usage				O
Notices	O			
Organization	O			
PreInstall			O	
Profile			O	
Profiles	O	O	O	
Provision		O		
Push				O
Service Profiles	O	O		
Settings	O			
SmartKey		O		
SMS	O	O		
System Configuration	O			
Time Trigger		O		
TxHistory		O		
User			O	
User Login		O		
User Management	O			
VPP Management	O	O		
Windows	O			

Managing alerts

Set alerts for important audit events. When the audit events set as alerts occur, the number of occurrences is displayed next to the **Service Overview** and **Alert** menus to help facilitate your next action.

Viewing entire alerts

To view the alerts of audit events, complete the following steps:

1. Navigate to **Service Overview** > **Alert**.
2. Select the period for which you want to view alerts.
   - You can also search for the target device by using the search field.
3. Click the alert you want to view.
   - There are five categories of alerts:
     - **Changes In Server Status**: This alert appears when a server error event occurs. For example, while creating new files, deleting, modifying or renaming existing files, executing unauthorized packages, or during integrity errors, server certificate expiration, and server certificate revocation.
     - **Failed Policies**: Informs you that sent device commands or policies are not applied to devices.
     - **Changes in Device Status**: Informs you of the device's status change to Disconnected. In this case, you cannot control the device because the Keepalive settings are expired and the device does not communicate with the EMM server.
     - **Security Violation**: Informs you of devices on which security violations have been detected during periodical device inspection.
     - **Others**: Informs you of the occurrence of other types of audit events.
4. On the "Details" area, view the detailed information about the audit event.
   - The necessary actions you must take according to the alert category are as follows:

Alert category	Description
Failed Policies	• If you cannot click the mobile ID on the alert list, it means the device's status is Unenrolled, Provisioning, or Disconnected and the policies are not applied. Check the device's status in **Device**. • If you see a log message about APNs or FCM in the "Log Detail" area, it means the Public Push value is not registered. Register an APNs certificate in **Setting** > **Server** > **Configuration** > **Public Push**. To configure the FCM settings, contact a TMS administrator.

Alert category	Description
Changes in Device Status	Click the mobile ID of the disconnected device and check the Keepalive status. Also, tell the device user to check the device's network connection status. The violation of Keepalive is detected when the connection of the device and the server is lost longer than the time set in the Keepalive settings.
Security Violation	• View the name of the package or application reported as the cause of the problem in the "Log Detail" area and uninstall the package or application. • When the device's status is Disconnected, the audit event "Agent Request to report policy violation" occurs. In **Service Overview** > **Log and Event** > **Audit Log**, search for and view the audit log to find out the cause of the disconnection.

Configuring alerts

Customize the alerts of audit events. You can also modify the default settings for alerts, such as the level, and result.

To configure alerts, complete the following steps:

1. Navigate to **Service Overview** > **Alert**.
2. On the "Alert List" area, click  .
3. In the "Monitoring Alert Setting" window, select audit events you want to add from the audit event list and click **Update**.
   - To delete the selected audit events from the alert list, click the checkbox for the events, and then click  .
4. Modify the level and result of the alerts if necessary.
   - Level: In default, the alert level is set the same as the audit event level. Click the alert level and modify it. To receive an alert, the alert level must be set the same or lower than the audit event level. For more information about audit event levels, see Severity level.
   - Result: Select the audit event result to receive an alert for when the result is a success, fail, or for both.
5. Click **Save**.
6. In the "Save" window, click **OK**.

Viewing the device log

View device logs for monitoring device operation. Device logs include the inventory and log messages of applied policies and device commands. The device with policy applied collects the log based on the policy. For more information about the log policy, see Logging (Android Legacy).

The default settings for device logs are as follows:

- Maximum collection capacity: 10 MB
- Maximum storage period: 7 days
- Log level: Records about debugging and other logs for developers

The method for changing the device log setting value is different depending on whether it is single for single-tenant mode or multi-tenant mode.

- Single-Tenant mode: Click a service profile at **Setting** > **Server** > **Configuration** to specify audit log setting.
- Multi-Tenant mode: Navigate to **Management** > **Service Profile** in the TMS Admin Portal to specify the audit log setting.

To view device logs, complete the following steps:

1. Navigate to **Service Overview** > **Log and Event** > **Device Log**.
2. On the “Device Log” page, search for a device by device name or user name. You can also search by setting the collection date.
3. Click the row of the device.
4. In the “Log Files” area, view the log files.
   - You can filter the collection period.
   - Name of the log file generated according to the policy. The types of device log files include the following:
     - `EMMClient_yyyymmdd.log`: EMM Client log
     - `EMMAgent_yyyymmdd.log`: EMM Agent log
       : For Tizen Wearable, only EMMAgent logs are available
     - `PUSH_DA_yyyy_mm_dd.txt`: Push DA log
     - `PUSH_DA_DB_yyyy_mm_dd.txt`: DB status log of Push DA
   - To export a device log to a text file, click  in the row of the log you want to export.
   - To delete a device log, click  in the row of the log you want to delete.

Viewing the service history

View the history of device commands or emails/messages sent from the Admin Portal.

NOTE If the Database Retention Period (Days) and Log File Retention Period (Days) of the LOG classification in **Setting** > **Server** > **Configuration** are set, the device history, Email and SMS history that have passed the storage period will not be searched. For more information, see List of environment settings.

Viewing device command history

To view the device command logs by each user or device, complete the following steps:

1. Navigate to **Service Overview** > **History** > **Device Command History**.
2. Enter a request date and a user or device name, and then click **Search**.
3. Click a device command.
4. View the device command history.
   - If you click **Detail** in the row of a log, you can view the following information.

Item	Description
Process	The detailed information displayed in the “Process” tab: • Request History: Request details of the Audit events. For example, the Device ID, Data Information, User Info, or Notification ID. • Result Code: Event process result code. • Result History: The detailed result of the audit event. – When you change a policy in the Admin Portal, a new event is recorded in the profile category. e.g.) When an Android policy is changed, all policy events to be saved in Request History of “Save General Policy” are shown. – For the “Package deletion failure” event, a package name and the reason for the failure appear in Result History.

Item	Description

Log Data	The detailed information about the event is displayed in “Log Data” under the condition below:
	• For **Console** type: When sending more than 4000 bytes of data from the device to EMM server.
	• For **Server** type: When Event Category and Event are as below.
	  - Event Category: Device command
	  - Event: Agent Request to lock screen (Device ⟶ Server) or Agent Request to unlock device (Device ⟶ Server) or Agent Request for work report (Device ⟶ Server) or Handle multiple devices by sending device control
	  - When profile settings, such as Wi-Fi and VPN, are applied to devices, the “Agent Request for work report (Device ⟶ Server)” event will be shown. Click Log Data to view the details.
	• For **Device** type: When Event Category and Event are as below
	  - Event Category: Device command
	  - Event: Device Lock/Unlock History

To view the device command logs by each group or organization, complete the following steps:

1. Navigate to **Service Overview** > **History** > **Group Command History**.
2. Enter a request date and a group ID or organization name, and then click **Search**.
3. Click a group or organization name.
4. View the device command history.

Viewing Email & SMS history

View the history of sent emails and text messages.

- Emails are sent through the SMTP email delivery service. EMM only tracks whether an email has been sent successfully to the SMTP server. The recipient’s receipt of the email is unknown.
- For text messages, EMM only tracks whether a message has been sent. Whether the message was received is unknown.

To view the emails or SMS messages you have sent to users, complete the following steps:

1. Navigate to **Service Overview** > **History** > **Email & SMS History**.
2. Enter a User ID and a Send Date, email address, or mobile number, and then click  .
3. View the email and/or message history.
   - To view the content of an email or message, click the email or message subject.

- When “Success” appears in Status column, it only indicates that the email has been sent successfully to the SMTP server, and the message has been sent from the Admin Portal. When “Failed” appears in this column, you can check the failure cause in the “Log Details” window.
- In the Sender ID column, the email sender account ID or the phone number of the outgoing text message is displayed.

Viewing the network usage

Monitor the call and data usage accrued from activated mobile devices. The network usage displayed on the Admin Portal may differ from the actual network usage tracked by the network service provider. To collect call and data usage logs, you should enable data usage log collection for devices. For more information, see Configuring the environment. You can change the usage level ranges in the charts in the **Network Dashboard** category in **Setting** > **Server** > **Configuration**. For more information, see Network Dashboard.

Viewing the usage chart

The call and data usage charts display the accumulated call and data usage from the pre-set start date for the current month to the current day. You can change the collection start date in the **Network** category in **Setting** > **Server** > **Configuration**. Each chart shows the number of devices and its ratio by usage level.

To view the usage charts, complete the following steps:

1. Navigate to **Advanced** > **Network** > **Dashboard**.
   - To view total usage information of devices, select **All** from the network name drop-down menu.
   - To view usage information by carrier, select a desired carrier name from the network name drop-down menu.
2. View the call and data usage charts.
   - Click a bar in the charts to view the list of corresponding devices.

Viewing the usage by device

View the call and data usage accrued from an activated device in detail.

1. Navigate to **Advanced** > **Network** > **Usage**.
2. Search for Device Name, User Name, or select Network Name, Calls, Data Usage Level, or Usage Date and click **Search**.
   - Select **Usage Date** that can aggregate usage. The default value is the current day and you can view the usage for up to the last 3 months.
   - To view the total usage information for all the devices, select **All** from the network name drop-down menu. To view the total usage information for the devices with a particular carrier (MCC and MNC), select a desired carrier name.
   - The Usage list includes the following information:
     - **Network Name**: Displays the carrier (MCC and MNC) of the device.
     - **Calls**: Displays the total usage amount of both sent and received calls.
     - **Data**: Displays the total usage amount of both sent and received data from the device system and installed applications. Wi-Fi data is excluded.
     - **App Usage**: Displays the usage amount of both sent and received data from installed applications. Wi-Fi data is excluded.
     - **Recent Data**: Displays the latest date when the device's call and data usage are aggregated.
3. Click a device from the list to view its usage in detail.
4. On the "Usage Detail" page, view the usage information of the selected device.
   - **Calls & Data History tab**: View the phone call and data usage during the usage aggregation period in graphs and compare it with the average value of all devices. You can also view the usage by day.
     - In the graphs, device usage shows the call and data usage of the device during the usage aggregation period, and the average usage shows the average usage amount of devices belonging to the tenant during the same period.
   - **App Usage** tab: View the list of applications installed on the device and the data usage by application during the usage aggregation period. Applications using the same package name will be displayed in their respective group.

NOTE You can export the usage list of all devices in an Excel file. On the "Usage" page, click **Export to CSV**.

13

Appendix

Appendix

In Appendix, you can view audit events in the Admin Portal, the error codes of the EMM server and user devices, and learn how to install and use EMM AppWrapper. You can check how to configurator CAC Sign-In on the Admin Portal.
You can also refer to the glossary to understand the technical terms and abbreviations used in this guide.

This chapter explains the following topics:

Lists of audit events

View the detailed information of audit events. You can view the lists of the audit events for the user devices, servers, Admin Portal, and system. Also, the audit log fields in an exported audit log file are described.

Device audit events

The list of device audit events for user devices while using EMM is as follows:

Event Category	Event Name
AppTunnel	• AppTunnel Start • AppTunnel Stop • TLS HANDSHAKE START • TLS HANDSHAKE COMPLETED • TLS TERMINATED • TLS HANDSHAKE ERROR • CORRUPTION CHECK SUCCESS • CORRUPTION CHECK FAIL • KEY GENERATION FAIL • ENCRYPTION FAIL • DECRYPTION FAIL • MAKE SIGNATURE FAIL • VERIFY SIGNATURE FAIL • CRL REQUEST FAIL • VERIFY DIGEST FAIL • NOT ALLOWED DATA RECEIVED • Handshake between Apptunnel server and Apptunnel client started • Handshake between Apptunnel server and Apptunnel client succeeded • Handshake between Apptunnel server and Apptunnel client terminated • Handshake error occurred between Apptunnel server and Apptunnel client

Event Category	Event Name
Certificate Status	• Cert Issue Fail (Key Generation Error) • Cert Verification Fail (Unknown) • BasicConstraints Check Error • Path Check Error • Valid Date Check Error • CRL Check Error • Cert Verification Fail (Unknown) • Cert Issue Request • Cert Issue Success • Cert Issue Fail (Parameter Error) • Cert Issue Fail (Not-initialized Object Error) • Cert Issue Fail (Internal Error) • Failure to establish connection to determine revocation status
Compliance	• Violated version control policy (Device) • Violated recording prevention policy (Device) • Check System Forgery

Event Category	Event Name
Device	• Failed to lock EMM screen (Device) • Log on status is changed to logout (Device) • Managed Google Play token issuance (Device) • Managed Google Play account registration (Device) • Managed Google Play account report (Device) • Managed Google Play account removal (Device) • SIM Card changed • Network usages resetted. • Cellular data limit reached. • Call limit reached. • Agent has been started. • Agent has been shutdowned. • Failure of the randomization process. • Failure of policy validation. • Result of importing the certificates to be used for authentication of Agent communications. • Request to device unenrollment by user • Request to device unenrollment by user policy is changedApp feedback has been received.
Device Command	• Keepalive Time Limited • Keepalive Notice • Device Command Received • Verify Device Command • Device Command Added • Device Command Process Started • Device Command Process Finished • Failure Installation Package • Failure Installation Package in KNOX • Failure Uninstallation Package • Failure Uninstallation Package in KNOX • Device Diagnosis Information • Device Lock/Unlock History • Failure Installation Package in Work Profile • Failure Uninstallation Package in Work Profile • Policy violation detected • Exit due to policy violation • Change Trigger State • Change Profile

Event Category	Event Name
EMM Agent	• Device Boot Completed • Change Network Connectivity • Change Agent Context • Initialize Agent • Change Airplane Mode
EMM Client	• EMM Login Failed • EMM Client Screen UnLock Failed • EMM Login Failed Count Exceeded • EMM Client Screen UnLock Failed Count Exceeded • Change Screen Lock Password EMM Client
Enrollment	• Push Registration Succeeded • Push Unregistration Succeeded • Enroll EMM Agent Started • Enroll EMM Agent • Unenroll EMM Agent Started • Unenroll EMM Agent • Enable Device Admin • Disable Device Admin • Activate ELM License • Activate KLMS License • Enrollment Request by UMC Agent
Kiosk Launcher	• Application installation request (Kiosk) • Application list request (Kiosk)
Logs	• Start Audit Logging • Send Audit Log To Server • Send EMM Agent Log • audit event white list change • audit event white list receive
PreInstall	• Install CA Certificate • Uninstall CA Certificate
Profile	• SIM card PIN code change
Profiles	• Device Password Attempts Failed Count Exceeded • Scheduler Raised • KioskMode Result
User	• Agreed to disable fingerprint lock (Device)

Server audit events

The list of server audit events for the EMM server and the external requests or inventory scheduler from devices is as follows:

Event Category	Event Name
AD/LDAP Sync	• Start external sync work • Stop external sync work • Add User By Sync • Modify User By Sync • Delete User By Sync • Ignore AD/LDAP Synced User • Error Occurred While Synching User • Add Organization By Sync • Modify Organization By Sync • Delete Organization By Sync • Ignore AD/LDAP Synced Organization • Error Occurred While Synching Organization • Initialize Sync Process • Finish Sync • Start external sync operation • Stop external sync operation • Automatically send profile to target users after synchronization ends • Request managed apps mapping action to target users after synchronization ends • Add groups through synchronization • Delete group via sync • Group modification via synchronization • Override group sync by setting • Invalid group sync attempt
Android Enterprise	• Failed to request the authentication token for Android Enterprise device enrollment • Failed to update Google Device ID (Google ⟶ Device)
Applications	• Modify App Status Due To App Service Expiration Date • Failed to import the app information from the multiple apps • Request the Uninstall App device command in a group or organization
Cryptographic Support	• Failure Of Select Nonce • Failure Of Update Nonce • Nonce Mismatched Between Server And Device

Event Category	Event Name
Compliance	• Report policy violation • Start Keepalive Check • Close Keepalive Check • Handle Keepalive violations • Check Point MTP Malware detection information • Update Device Status (System Block) • Run Keepalive task • No Keepalive task or not configured
Content	• Get Content URL
Contents	• Request Content List • Report Content Status
Devices	• Insert Device License • Update Device License
Device Command	• Distribute the latest device management profile/app information (Device control transmit) • Distribute the latest device management profile (Device control transmit) • Distribute the latest information on internal application (Device control transmit) • Implement User-defined event - Activate (Device control transmit) • Implement User-defined event - Deactivate (Device control transmit) • Implement Gate event - Activate (Device control transmit) • Implement Gate event - Deactivate (Device control transmit) • Disable Exchange block - Activate (Device control transmit) • Disable Exchange block - Deactivate (Device control transmit) • Install app (Device control transmit) • Implement app (Device control transmit) • Close app (Device control transmit) • Delete app data (Device control transmit) • Delete app (Device control transmit) • Allow/Disallow running an app - Allow (Device control transmit) • Allow/Disallow running an app - Disallow (Device control transmit) • Lock/Unlock the device - Lock (Device control transmit) • Lock/Unlock the device - Unlock (Device control transmit) • Reset screen password (Device control transmit) • Factory reset (Device control transmit) • Power off the device (Device control transmit) • Reboot the device (Device control transmit) • Initialize external SD card (Device control transmit)

Event Category	Event Name
Device Command	• Activate/Deactivate CC mode - Activate (Device control transmit) • Activate/Deactivate CC mode - Deactivate (Device control transmit) • Lock screen (Device control transmit) • Attestation (Device control transmit) • Initialize information on blocking (Device control transmit) • Deactivate service (Device control transmit) • Collect Audit log -Agent (Device control transmit) • Collect log -Agent (Device control transmit) • Collect diagnosis information (Device control transmit) • Update License (Device control transmit) • Update System app (Device control transmit) • H/W status (Device control transmit) • List of apps installed (Device control transmit) • Location (Device control transmit) • SIM verification (Device control transmit) • Report the status (Device control transmit) • Lock/Unlock container - Lock (Device control transmit) • Lock/Unlock container - Unlock (Device control transmit) • Reset container lock passcode (Device control transmit) • Delete container (Device control transmit) • Install container app (Device control transmit) • Run container app (Device control transmit) • Close container app (Device control transmit) • Delete container app data (Device control transmit) • Delete container app (Device control transmit) • Apply security policy (Device control transmit) • Distribute the latest app management profile (Device control transmit) • Check if a device has been rooted (Device control transmit) • Unlock EMM Client (Device control transmit) • Send a message (Device control transmit) • Delete an account (Device control transmit) • Lock screen (Device control transmit) • Collect Audit log - Client (Device control transmit) • Collect log -Client (Device control transmit) • Collect diagnosis information (Device control transmit) • Update user information (Device control transmit) • Update system app (Device control transmit) • Location (Device control transmit)

Event Category	Event Name
Device Command	• Apply security policy (Device control transmit) • Apply security policy - Deactivate (Device control transmit) • Transfer event information (Device control transmit) • Deactivate service (Device control transmit) • Invite program (Device control transmit) • Invite To Program (Response) • Check if an app has been installed (Device control transmit) • Activate event to time - Deactivate (Device control transmit) • Activate event to time - Activate (Device control transmit) • Notice of a fail to activate service (Device control transmit) • Request to activate visitor policy request (Device control transmit) • Deactivate visitor policy request (Device control transmit) • Agent Invalid protocol • Agent Invalid request • Agent Request to distribute device management profile (Device ⟶ Server) • Agent Respond to the request to distribute device management profile (Server ⟶ Device) • Agent Request to enable/disable event (Device ⟶ Server) • Agent Respond to the request to enable/disable event (Server ⟶ Device) • Agent Request to block Exchange (Device ⟶ Server) • Agent Respond to the request to block Exchange (Server ⟶ Device) • Agent Request to disable blocking Exchange (Device ⟶ Server) • Agent Respond to the request to disable blocking Exchange (Device ⟶ Server) • Agent Request to install app (Device ⟶ Server) • Agent Respond to the request to install app (Server ⟶ Device) • Agent Request to run app (Device ⟶ Server) • Agent Respond to the request to run app (Server ⟶ Device) • Agent Request to close app (Device ⟶ Server) • Agent Respond to the request to close app (Server ⟶ Device) • Agent Request to delete app data (Device ⟶ Server) • Agent Respond to the request to delete app data (Server ⟶ Device) • Agent Request to delete app (Device ⟶ Server) • Agent Respond to the request to delete app (Server ⟶ Device) • Agent Request to allow running app (Device ⟶ Server) • Agent Respond to the request to allow running app (Server ⟶ Device) • Agent Request to disallow running app (Device ⟶ Server) • Agent Respond to the request to disallow running app (Server ⟶ Device) • Agent Request to lock screen (Device ⟶ Server) • Agent Respond to the request to lock device (Server ⟶ Device)

Event Category	Event Name
Device Command	• Agent Request to unlock device (Device ⟶ Server) • Agent Respond to the request to unlock device (Server ⟶ Device) • Agent Request to reset lock device password (Device ⟶ Server) • Agent Respond to the request to reset lock device password (Server ⟶ Device) • Agent Request factory reset (Device ⟶ Server) • Agent Respond to the request for factory reset (Server ⟶ Device) • Agent Request to power off device (Device ⟶ Server) • Agent Respond to the request to power off device (Server ⟶ Device) • Agent Request to reboot device (Device ⟶ Server) • Agent Respond to the request to reboot device (Server ⟶ Device) • Agent Request to initialize external SD card (Device ⟶ Server) • Agent Respond to the request to initialize external SD card (Server ⟶ Device) • Agent Request to set CC mode (Device ⟶ Server) • Agent Respond to the request to set CC mode (Server ⟶ Device) • Agent Request to turn off CC mode (Device ⟶ Server) • Agent Respond to request to turn off CC mode (Server ⟶ Device) • Agent Request to collect device information (Device ⟶ Server) • Agent Respond to the request to collect device information (Server ⟶ Device) • Multiple devices distributed sending • Agent Request to update license (Device ⟶ Server) • Agent Respond to the request to update license (Server ⟶ Device) • Agent Request to update system app (Device ⟶ Server) • Agent Respond to the request to update system app (Server ⟶ Device) • Agent Request for SIM verification (Device ⟶ Server) • Agent Respond to the request for SIM verification (Server ⟶ Device) • Agent Request to lock container (Device ⟶ Server) • Agent Respond to the request to lock container (Server ⟶ Device) • Agent Request to unlock container (Device ⟶ Server) • Agent Respond to the request to unlock container (Server ⟶ Device) • Agent Request to reset lock container password (Device ⟶ Server) • Agent Respond to the request to reset container password (Server ⟶ Device) • Agent Request to delete container (Device ⟶ Server) • Agent Respond to the request to delete container (Server ⟶ Device) • Agent Request to install container app (Device ⟶ Server) • Agent Respond to the request to install container app (Server ⟶ Device) • Agent Request to run container app (Device ⟶ Server) • Agent Respond to the request to run container app (Server ⟶ Device) • Agent Request to close container app (Device ⟶ Server)

Event Category	Event Name
	• Agent Respond to the request to close container app (Server ⟶ Device) • Agent Request to delete container app (Device ⟶ Server) • Agent Respond to the request to delete container app (Server ⟶ Device) • Agent Request to delete container app (Device ⟶ Server) • Agent Respond to the request to delete container app (Server ⟶ Device) • Agent Request to report policy violation (Device ⟶ Server) • Agent Respond to the request to report policy violation (Server ⟶ Device) • Agent Request to reissue code to disable service (Device ⟶ Server) • Agent Respond to the request to reissue code to disable service (Server ⟶ Device) • Agent Request for Attestation Nonce (Device ⟶ Server) • Agent Respond to the request for Attestation Nonce (Server ⟶ Device) • Agent Request for Attestation verification (Device ⟶ Server) • Agent Respond to the request for Attestation verification (Server ⟶ Device) • Agent Request for app information (Device ⟶ Server) • Agent Respond to the request for app information (Server ⟶ Device) • Agent Request to collect diagnosis information (Device ⟶ Server) • Agent Respond to the request to collect diagnosis information (Server ⟶ Device)
Device Command	• Agent Request for work report (Device ⟶ Server) • Agent Respond to the request for work report (Server ⟶ Device) • Agent Request for command (Device ⟶ Server) • Agent Install profile (Server ⟶ Device) • Agent Delete profile (Server ⟶ Device) • Agent Search information on apps installed (Server ⟶ Device) • Agent Search device information (Server ⟶ Device) • Agent Search security information (Server ⟶ Device) • Agent Device lock (Server ⟶ Device) • Agent Reset password (Server ⟶ Device) • Agent Factory reset (Server ⟶ Device) • Agent Install app (Server ⟶ Device) • Agent Information on apps installed through MDM • Agent Delete app (Server ⟶ Device) • Agent Set app properties (Server ⟶ Device) • Agent Set the items included in app settings (Server ⟶ Device) • Agent Information on Settings of apps installed through MDM (Server ⟶ Device) • Agent Information on properties of apps installed through MDM (Server ⟶ Device)

Event Category	Event Name
Device Command	• Agent Feedback on settings of apps installed through MDM (Server ⟶ Device) • Agent Initialize information on blocking (Server ⟶ Device) • Agent Report status (Server ⟶ Device) • Agent Respond to the request to handle command (Device ⟶ Server) • Reset data usage (Device control transmit) • Reset number of calls (Device control transmit) • Agent Request to collect device and reset data usage (Device ⟶ Server) • Agent Respond to the request to collect device and reset data usage (Server ⟶ Device) • Agent Request to collect device and reset number of calls (Device ⟶ Server) • Agent Respond to the request to collect device and reset number of calls (Server ⟶ Device) • Client Perform Server Init logic (Device ⟶ Server) • Client Request to distribute the latest app management profile (Device ⟶ Server) • Client Respond to the request to distribute the latest app management profile (Server ⟶ Device) • Client Request for work report (Device ⟶ Server) • Client Respond to the request for work report (Server ⟶ Device) • Client Request to activate application of security policy (Device ⟶ Server) • Client Respond to the request to activate application of security policy (Server ⟶ Device) • Client Request to deactivate application of security policy (Device ⟶ Server) • Client Respond to the request to deactivate application of security policy (Server ⟶ Device) • Client Request to delete security policy profile (Device ⟶ Server) • Client Respond to the request to delete security policy profile (Server ⟶ Device) • Client Request to backup bookmarks (Device ⟶ Server) • Client Respond to the request to backup bookmarks (Server ⟶ Device) • Client Request to backup homepages (Device ⟶ Server) • Client Respond to the request to backup homepages (Server ⟶ Device) • Client Request to send Device control (EMM Agent) (Device ⟶ Server) • Client Respond to the request to send Device control (EMM Agent) (Server ⟶ Device) • Handle multiple devices by sending device control • Device command transmission for each area in multiple devices. • Insert command • Select command • Delete command • Update command

Event Category	Event Name
Device Command	• Command queue retransmission is in progress. • No target for command queue retransmission • Command queue retransmission • Command queue retransmission has started. • Command queue retransmission is finished. • Delete commands left due to unenrollment command • Duplicated Command • Delete records of policy violation (Device ⟶ Server) • Delete records of policy violation (Server ⟶ Device) • Agent Request for command (Device ⟶ Server) • Agent Request for command (Server ⟶ Device) • Client Request for command (Device ⟶ Server) • Client Request for command (Server ⟶ Device) • Custom device control (Send device control) • Request for command (Device ⟶ Server) • Distribute device management profile (Server ⟶ Device) • Collect device information (Server ⟶ Device) • Device lock (Server ⟶ Device) • Factory reset (Server ⟶ Device) • Custom device control (Server ⟶ Device) • Respond to the request to handle command (Device ⟶ Server) • Start SyncML Session (Device ⟶ Server) • Close SyncML Session (Server ⟶ Device) • Register Push (WNS PFN) (Server ⟶ Device) • Collect device and app information (Device control transmit) • Collect device information (Device control transmit) • Collect app information (Device control transmit) • Collect current location information (Device control transmit) • Collect audit information (Device control transmit) • Collect log information (Device control transmit) • Download content (Device control transmit) • Update E-FOTA Firmware Version (Device control transmit) • Agent Request to collect device and app information (Device ⟶ Server) • Agent Respond to the request to collect device and app information (Server ⟶ Device) • Agent Request to collect device information (Device ⟶ Server) • Agent Respond to the request to collect device information (Server ⟶ Device) • Agent Request to collect app information (Device ⟶ Server)

Event Category	Event Name
Device Command	• Agent Respond to the request to collect app information (Server ⟶ Device) • Agent Request to collect device and current location information (Device ⟶ Server) • Agent Respond to the request to collect device and current location information (Server ⟶ Device) • Agent Request to collect device and audit information (Device ⟶ Server) • Agent Respond to the request to collect device and audit information (Server ⟶ Device) • Agent Request to collect device and log information (Device ⟶ Server) • Agent Respond to the request to collect device and log information (Server ⟶ Device) • Agent Request to download content (Device ⟶ Server) • Agent Respond to the request to download content (Server ⟶ Device) • Agent Request to update fota firmware version (Device ⟶ Server) • Agent Respond to the request to update fota firmware version (Server ⟶ Device) • Deactivate MDM agent for synchronization between server and device • Flush command queue (Device control transmit) • H/W status (Device control transmit) • List of apps installed (Device control transmit) • Apply security policy (Device control transmit) • Send an INI File (Device ⟶ Server) • Get device status (Device ⟶ Server) • Send an INI File (Server ⟶ Device) • Get device status (Server ⟶ Device) • Collect Audit log - Client (Device control transmit) • Collect log -Client (Device control transmit) • Location (Device control transmit) • Check if a device has been rooted (Device control transmit) • Agent Report status (Server ⟶ Device) • Agent Invalid protocol • Agent Invalid request • Agent Request to distribute device management profile (Device ⟶ Server) • Agent Respond to the request to distribute device management profile (Server ⟶ Device) • Agent Request to install app (Device ⟶ Server) • Agent Respond to the request to install app (Server ⟶ Device) • Agent Request to run app (Device ⟶ Server) • Agent Respond to the request to run app (Server ⟶ Device)

Event Category	Event Name
Device Command	• Agent Request to close app (Device ⟶ Server) • Agent Respond to the request to close app (Server ⟶ Device) • Agent Request to delete app (Device ⟶ Server) • Agent Respond to the request to delete app (Server ⟶ Device) • Agent Request to lock screen (Device ⟶ Server) • Agent Respond to the request to lock device (Server ⟶ Device) • Agent Request factory reset (Device ⟶ Server) • Agent Respond to the request for factory reset (Server ⟶ Device) • Agent Request to power off device (Device ⟶ Server) • Agent Respond to the request to power off device (Server ⟶ Device) • Agent Request to reboot device (Device ⟶ Server) • Agent Respond to the request to reboot device (Server ⟶ Device) • Agent Request to collect device information (Device ⟶ Server) • Agent Respond to the request to collect device information (Server ⟶ Device) • Agent Request to update license (Device ⟶ Server) • Agent Respond to the request to update license (Server ⟶ Device) • Agent Request to update system app (Device ⟶ Server) • Agent Respond to the request to update system app (Server ⟶ Device) • Agent Request to reissue code to deactive service (Device ⟶ Server) • Agent Respond to the request to reissue code to deactive service (Server ⟶ Device) • Agent Request for app information (Device ⟶ Server) • Agent Respond to the request for app information (Server ⟶ Device) • Agent Request for work report (Device ⟶ Server) • Agent Respond to the request for work report (Server ⟶ Device) • Agent Request for command (Device ⟶ Server) • Agent Request for command (Server ⟶ Device) • Agent Request to collect device information (Device ⟶ Server) • Agent Respond to the request to collect device information (Server ⟶ Device) • Agent Request to collect app information (Device ⟶ Server) • Agent Respond to the request to collect app information (Server ⟶ Device) • Agent Request to collect device and current location information (Device ⟶ Server) • Agent Respond to the request to collect device and current location information (Server ⟶ Device) • Agent Request to collect device and log information (Device ⟶ Server) • Agent Respond to the request to collect device and log information (Server ⟶ Device) • Deactivate MDM agent for synchronization between server and device

Event Category	Event Name
Device Command	• Request for property sync of app auto deletion when deactivating (Device ⟶ Server) • Respond to property sync of app auto deletion when deactivating (Server ⟶ Device) • Request for profile deletion (Device ⟶ Server) • Respond to profile deletion (Server ⟶ Device) • Synchronize property of app auto deletion when deactivating (Device Command) • Request for custom control (Device ⟶ Server) • Respond to custom control (Server ⟶ Device) • Respond to Agent command (Server ⟶ Device) • Request for external SD card authentication (Device ⟶ Server) • Respond to external SD card authentication (Server ⟶ Device) • Authenticate external SD card (Device Command) • Uninstall Application (MTP) (Device ⟶ Server) • Uninstall Application (MTP) (Server ⟶ Device) • Uninstall Application (MTP) (Device control transmit) • Activate-Exception Profile • Deactivate-Exception Profile • Update event time (Device control transmit) • Device command transmission for each area in one device • Device command transmission for each area in multiple devices • Update SmartKey Token Request (Device ⟶ Server) • Update SmartKey Token Response (Server ⟶ Device) • Smartkey request for reservation info. (Device ⟶ Server) • Smartkey response for reservation info. (Server ⟶ Device) • Smartkey request for car info. (Device ⟶ Server) • Smartkey response for car info. (Server ⟶ Device) • Smartkey request for available car info. (Device ⟶ Server) • Smartkey response for available car info. (Server ⟶ Device) • Lock car door request (Device ⟶ Server) • Lock car door response (Server ⟶ Device) • Unlock car door request (Device ⟶ Server) • Unlock car door response (Server ⟶ Device) • Smartkey request for report (Device ⟶ Server) • Smartkey response for report (Server ⟶ Device) • Smartkey request for token expired (Device ⟶ Server) • Smartkey response for token expired (Server ⟶ Device) • Smartkey request for command (Device ⟶ Server)

Event Category	Event Name
Device Command	• Smartkey response for command (Server ⟶ Device) • Smartkey request for service deactivation (Device ⟶ Server) • Smartkey response for service deactivation (Server ⟶ Device) • CSM deactivate (Device control transmit) • CSM deactivation request (Server ⟶ Device) • CSM deactivation response (Device ⟶ Server) • Update SmartKey token request (Server ⟶ Device) • Update SmartKey token response (Device ⟶ Server) • Delete SmartKey token request (Server ⟶ Device) • Delete SmartKey token response (Device ⟶ Server) • Get car info.(Device control transmit) • Get car info. request (Server ⟶ Device) • Get car info. response (Device ⟶ Server) • Lock car door (Device control transmit) • Lock car door request (Server ⟶ Device) • Lock car door response (Device ⟶ Server) • Unlock car door (Device control transmit) • Unlock car door request (Server ⟶ Device) • Unlock car door response (Device ⟶ Server) • Client Request for policy summary (Device ⟶ Server) • Client Respond for policy summary (Server ⟶ Device) • Collect EMM Client information (Server ⟶ Device) • Update Agent User information (Server ⟶ Device) • Agent Device Control Fail on a Device • Client Device Control Fail on a Device • Agent Device Control Success on a Device • Client Device Control Success on a Device • Request for Google managed app permission (Server ⟶ Google) • Request for Management configuration of Google managed app (Server ⟶ Google) • Request for Google managed app installation (Server ⟶ Google) • Request for Google managed app uninstallation (Server ⟶ Google) • Request for user authentication password reset (Device ⟶ Server) • Response to user authentication password reset (Server ⟶ Device) • Contents deployment (Send device control) • Request for Agent contents deployment (Device ⟶ Server) • Response to Agent contents deployment (Server ⟶ Device) • Delete the audit logs elapsed over the retention period.

Event Category	Event Name
Device Command	• Collect Profile ID (Device ⟶ Server) • Collect Profile ID (Server ⟶ Device) • Collect Profile ID (Send device control) • Contents transfer • Factory Reset (only) (Send Device Command) • Agent Factory Reset (Only) request (Device ⟶ Server) • SafetyNet Attestation Nonce Request (Device ⟶ Server) • SafetyNet Attestation Nonce Request (Server ⟶ Device) • SafetyNet Attestation Nonce Request (Device command transfer) • SafetyNet Attestation Verification Request (Device ⟶ Server) • SafetyNet Attestation Verification Request (Server ⟶ Device) • SafetyNet Attestation Verification Request (Device command transfer) • Delete User Certificate for Work Profile (Device ⟶ Server) • Delete User Certificate for Work Profile (Server ⟶ Device) • Delete User Certificate for Work Profile (Device command transfer) • Delete CA Certificate for Work Profile (Device ⟶ Server) • Delete CA Certificate for Work Profile (Server ⟶ Device) • Delete CA Certificate for Work Profile (Device command transfer) • Delete All Users' CA Certificates for Work Profile (Device ⟶ Server) • Delete All Users' CA Certificates for Work Profile (Server ⟶ Device) • Delete All Users' CA Certificates for Work Profile (Device command transfer) • Remove Work Profile (Device ⟶ Server) • Remove Work Profile (Server ⟶ Device) • Remove Work Profile (Device control transmit) • Delete User Certificate (Device ⟶ Server) • Delete User Certificate (Server ⟶ Device) • Delete User Certificate (Device command transfer) • Delete CA Certificate (Device ⟶ Server) • Delete CA Certificate (Server ⟶ Device) • Delete CA Certificate (Device command transfer) • Delete All Users' CA Certificates (Device ⟶ Server) • Delete All Users' CA Certificates (Server ⟶ Device) • Delete All Users' CA Certificates (Device command transfer) • Lock screen (Device ⟶ Server) • Lock screen (Server ⟶ Device) • Lock screen (Device control transmit) • Push token initialization • Reset Push Token (Device ⟶ Server)

Event Category	Event Name
Device Command	• Reset Push Token (Server ⟶ Device) • Reset Push Token (Device control transmit) • Update EMM (Device control transmit) • Exit Kiosk (Device ⟶ Server) • Exit Kiosk (Server ⟶Device) • Exit Kiosk (Device command transfer) • Request for Profile Signature Certificate (Device ⟶Server) • Response to Profile Signature Certificate (Server ⟶ Device) • Update Terms And Policies (Device control transmit) • Agent Request to collect exposure notification information (Device -> Server) • Agent Respond to the request to collect exposure notification (Device -> Server) • Upgrade License (Device control transmit) • Agent Request to upgrade License (Device -> Server) • Agent Respond to the request to upgrade License (Server -> Device) • Apply the Latest App Managed Configuration (Device control transmit) • Agent requests to apply the Latest App Managed Configuration (Device -> Server) • Server responds to the request to apply the Latest App Managed Configuration (Server -> Device) • Agent sends the App Manged Configuration Feedback (Device -> Server) • Server sends the App Manged Configuration Feedback (Server -> Device) • Agent request to collect device and network usage information (Device ->Server) • Agent response to the request to collect device and network usage information (Server -> Device) • Insert Temporary Command Queue • Process Temporary Command Queue • Start Temporary Command Queue Scheduler • End Temporary Command Queue Scheduler
Device Enrollment Program	• Start DEP Device Sync Scheduler • End DEP Device Sync Scheduler • DEP Device Sync (Server) • Request Bulk Assigning Users (DEP) • Register Device with Sync DEP • Delete Device with Sync DEP • Load Bulk Assignment Data from Excel (DEP) • Add Bulk Assignment Device Data (DEP) • Request to activate MDM • Response to activate MDM

Event Category	Event Name
E-FOTA	• E-FOTA API - Get Token • E-FOTA API - Register CorpID • E-FOTA API - Get Firmware List • E-FOTA API - Restrict Firmware • E-FOTA API - check group version • E-FOTA API - view product, model, and agency • E-FOTA API - network error • E-FOTA API - Get License Information • E-FOTA history - Create Group • E-FOTA History - Edit Group • E-FOTA history - Delete group
Email	• Send Mail To Admin (Async) • Send Mail To Device (Async) • Send Mail To User (Async)
Enrollment	• Prevent reactivation (Device ⟶ Server) • Prevent reactivation (Server ⟶ Device) • EMM Enrollment Spec (Device ⟶ Server) • EMM Enrollment Spec (Server ⟶ Device) • Update KLM/ELM license during activation (Device ⟶ Server) • Update KLM/ELM license during activation (Server ⟶ Device) • Disable service -Android (Device ⟶ Server) • Disable service -Android (Server ⟶ Device) • Confirm Enrollment (Knox) (Device ⟶ Server) • Confirm Enrollment (Knox) (Server ⟶ Device) • Agent Request to activate MDM (Device ⟶ Server) • Agent Request to activate MDM (Server ⟶ Device) • Agent Request for SCEP profile (Device ⟶ Server) • Agent Request for SCEP profile (Server ⟶ Device) • Agent Request for MDM profile (Device ⟶ Server) • Agent Request for MDM profile (Server ⟶ Device) • Agent Request for check-in (Device ⟶ Server) • Agent Request for check-in (Server ⟶ Device) • Agent Request for token update (Device ⟶ Server) • Agent Request for token update (Server ⟶ Device) • Agent Request for check-out (Device ⟶ Server) • Agent Request for check-out (Server ⟶ Device)

Event Category	Event Name
Enrollment	• Deactivate service (Device ⟶ Server) • Deactivate service (Server ⟶ Device) • Request SOAP message • Respond to SOAP message • Request for discovery URL (Device ⟶ Server) • Respond to the request for discovery URL (Server ⟶ Device) • Request for spec to issue certificate (Device ⟶ Server) • Respond to the request for spec to issue certificate (Server ⟶ Device) • Request to verify On-premis equipment (Device ⟶ Server) • Respond to the request to verify On-premise equipment (Server ⟶ Device) • Request to verify Federated equipment (Device ⟶ Server) • Respond to the request to verify Federated equipment (Server ⟶ Device) • Verify Security token • Request to issue certificate (Device ⟶ Server) • Respond to request to issue certificate (Server ⟶ Device) • Respond to the request to set DM Client
Enrollment	• Generate OTP Code • UMC User Search Request • UMC User Search Response • UMC Enrollment Request • UMC Enrollment Response • UMC Enrollment Information Update Request • UMC Enrollment Information Update Response • UMC Unenrollment Request • UMC Unenrollment Response • UMC Enrollment Information Update Request • UMC Enrollment Information Update Response • UMC Unenrollment Request • UMC Unenrollment Response • Request create MDM Profile • Response create MDM profile
Exception Profile per User	• Start Scheduler for Exception Policy per User • Terminate Scheduler for Exception Policy per User

Event Category	Event Name
InventoryScheduler	• Start InventoryScheduler Monitoring • Terminate InventoryScheduler Monitoring • Start Inventory Collection Scheduler for iOS • Terminate Inventory Collection Scheduler for iOS • Start Inventory Collection Scheduler for Android • Terminate Inventory Collection Scheduler for Android
License Management	• Add Knox License • Revision Knox License • Delete Knox License • Sync Knox License • Interface Knox License • Start License Expired Check • End License Expired Check
Logs	• Audit Log Transfer to External • Audit Remote Log Server Connection Failure
Profiles	• The result of applying Agent device policy • Agent Policy Apply Success on a Device • Failed to Apply Agent Policy on Device • Start profile update • Terminate profile update
Provision	• Request for public key • Activate provisioning • Deactivate provisioning • Activate Knox provisioning • Request To Changing Device Status To Provisioning Activate Status • Request To Changing Device Status To Provisioning Deactivate Status • Activate Work Profile provisioning • Activate Android Enterprise provisioning • Exceeded The Number Of Device Per User • Nonce Verification Request for Mutual Authentication
Report Location	• Start Location Report Scheduler • End Location Report Scheduler
Service Profiles	• Eula Download • Profile Download
SmartKey	• Create SmartKey schedule info. • Update SmartKey schedule info. • Delete SmartKey schedule info.

Event Category	Event Name
SMS	• Send SMS To Admin (Async) • Send SMS To Device (Async) • Send SMS To User (Async)
Settings	• Upload IDP Metadata to server
Time Trigger	• Start registration of Time Trigger when server operates • Close registration of Time Trigger when server operates • Start Time Trigger sync • Close Time Trigger sync
TxHistory	• Error (Device command queue)
User Login	• User Authentication Failed • User Logged In • User Logged Out
VPP Management	• VPP Sync start • VPP Sync is terminated • Assign VPP App License to Device • Revoke Device's VPP App License • Update Device's VPP App License

Admin Portal audit events

The list of Admin Portal audit events while operating EMM is as follows:

Event Category	Event Name
AD/LDAP Sync	• Request issue OAuth token • Delete Existing Sync Service Settings • Add New Sync Service Settings • Renew Existing Sync Service Settings • Delete Synced Device Information (User/Organization) • Add Synced Device Information (User/Organization) • Renew Synced Device Information (User/Organization) • Delete Sync Exception Subject (User/Organization) • Add Sync Exception Subject (User/Organization) • Restore Sync Exception Subject (User/Organization) • Change Sync Service Scheduled Status • Delete Existing Multiple Sync Services • Delete Existing Sync Service • Delete Existing Sync Service Mapping Information • Add New Sync Service • Add New Sync Service Mapping Information • Run Sync Service • Modify Sync Service • Start single item (User/Organization) sync • Start sync test • Delete Existing Sync Service • Add New Sync Service • Modify Sync Service • Create Log for Sync Entity • Create Log for Sync Service • Check sync object number • Add external sync service • Update external sync service • Delete external sync service • Change External Sync Service Status • Search external sync service • Search external sync service list • Request issue OAuth token • Search external sync map settings • Search external sync object properties

Event Category	Event Name
Admin Login	• Admin User Logged In • Admin User Logged Out • Admin Session Terminated Due To Timeout • Admin User Locked Due To Login Attempt Failed • The account is deleted • The account is blocked for 10 minutes
Administrators	• Update Administrator Information • Delete Administrator • Update Administrator's Status (Activate/Deactivate) • Change administrators (activate/deactivate) • Create Administrator Login Account • Modify password after account has been created or password has been reset • Update Password In Administrator Management Page • Admin Configuration Information Gets Reset When Admin Account Is Created • Update Administrator Configuration Information • Delete Administrator Configuration Information. • This Action Occurs Only When Logging In. Update Administrator Configuration Information. • Determine Super Status Of Selected Administrator • Insert Admin Organization • Add Admin Organization (through organization) • Modify Public Push • Modify Log Level • Modify Google Account • Tech. support activation & service period setting • Reset Support Admin password • Upload APNs Push Token • Modify APNs Authentication Type • Download Export File • Select Async Task
Alerts	• Delete Alert Settings Created By Each Admin • Add Alert Settings Created By Each Admin • Update Alert Settings Created By Each Admin • Update Multiple Audit Events For Alerts • Reset Audit Events For Alerts • Create temporary alert (for test only) • Delete Audit Event For Alerts

Event Category	Event Name
Alerts	• Add Audit Event For Alerts • Update Audit Event For Alerts
Android Enterprise	• Android Enterprise Registration • Android Enterprise Unregistration
Applications	• Add/Modify Google Account • Enter Multilingual Information When Adding App • Modify Multilingual Information When Modifying App • Modify Internal App Status • Delete Internal App • Delete Internal App • Add Internal App • Modify App (Internal/Public) Category • Modify Internal App • Upload Internal App File • Register Internal App Icon • Register Internal App Screenshot • Delete System App • Add System App • Modify System App • Upload System App File • Add Category Multilingual Information • Update Category Multilingual Information • Delete Category • Add Category • Modify Category • Modify Category Order • Delete Public App • Add Public App • Modify Public App • Delete System App File • Delete Internal App File • Delete Public App • Add Public App • Modify Public App • Delete System App File • Delete Internal App File

Event Category	Event Name
Applications	• Create Control App • Delete Kiosk App • Add Kiosk App • Register Kiosk App Physical File • Delete Control App • Add Control App • Modify Control App • Public App Sync • Create Category Temporary ID • Delete Applications Comment • Create Application Download List • Delete App Temporary File • Create App Temporary ID • Create Kiosk App Temporary ID • Update Kiosk App • Delete App Temporary File • Create App Temporary ID • Upload Control App • Create Public App Temporary ID • Check Google Account Validity • Add EMM Apps From Other Tenant • Delete EMM App Temporary File • Create EMM App Temporary ID • Update App Version • Update App Version details • Create Kiosk Wizard App Temporary ID • Add Kiosk Wizard App • Update Kiosk Wizard App • Delete Contents File Event • Register Contents File Event • Delete Kiosk Image File Event • Modify content files • Profile Manager creates an owned profile • Unassign a profile assigned to a profile manager • Deleting a profile created by a profile manager • Assign a profile to a profile manager

Event Category	Event Name
Applications	• Assign App • Unassign App • Modify App Settings • Request Access to Managed Google Play Apps (Device) (Server ⟶ Google) • Request Access to Managed Google Play Apps (Group/Organization) (Server ⟶ Google) • Delete Category • Delete Application • Add Public Application • App Wrapping failed • Reset to Basic Store Layout
Certificates	• Register Certificate Profile Template • Modify Certificate Profile Template • Delete Certificate Profile Template • Discard Certificate • Issue Certificate • Register CA Event • Modify CA Event • Delete CA Event • Register ExternalCert Event • Modify ExternalCert Event • Delete ExternalCert Event • Modify APNS Event • Modify ExternalCert Event (File) • Issue Device Certificate • ReIssue Device Certificate • ReNew Device Certificate • Key Generation Error • Request Issue Device Certificate • Request ReIssue Device Certificate • Request ReNew Device Certificate • Register CA Event • Modify CA Event • Delete CA Event • Register Certificate Profile Template • Modify Certificate Profile Template • Delete Certificate Profile Template

Event Category	Event Name
Certificates	• Change iOS certificates status of Deleted • Register CA Event • Modify CA Event • Modify DB Connector • Delete DB Connector • Add DB Connector • Add DB Connector Service Field • Add DB Connector Service Metadata • Add DB Connector Output By XML • Add REST Connector • Modify REST Connector
Certificates	• Delete REST Connector
Connectors	• Modify Service Log Configuration • Add Service Management Time • Modify Service Management Time • Delete Service Management Time • Add Service Group • Modify Service Group • Delete Service Group • Add Service Role Map • Delete Service Role Map • Update Service Authority • Add Role • Modify Role • Delete Role • Delete Directory Service • Delete Return Data Mapping Information Set In Directory Service • Save New Directory Service • Add Return Data Mapping Information Set In Directory Service • Renew Existing Directory Service
Content	• Assign Content • Unassign Content • Send Content Deployment To All Devices

Event Category	Event Name
Dashboard	• Add Report Condition • Modify Report Condition • Delete Report Condition • Add Report Query Fields • Delete Report Query Fields • Add Report Query • Modify Report Query • Delete Report Query • Add Report Condition • Modify Report Condition • Delete Report Condition • Modify Report Status • Download Report Result • Download Report Chart • Add Report Condition
Dashboard	• Delete Report • Add Report • Modify Report • Add Dashboard • Modify Dashboard • Delete Dashboard • Modify Dashboard Status • Modify Dashboard Main Page • Initiate dashboard main page
Device Command	• Try to Send Device Command To Multiple Devices in User&Organization or Group Menu • Try to Send Device Command To Single Device in Device Detail Menu • Try to Send “update visitor profile” device command • Try to Send Device Command To Multiple Devices in Device Command Popup • Try to Send Device Command To Single Device in Device Command Popup • Try to Send Device Command To Own Device in User Portal • Delete google managed Application • Install google managed Application • Delete Temporary Command Queue • Delete All Temporary Command Queue • Download Temporary Command Queue

Event Category	Event Name
Device Enrollment Program	• Create Apple DEP profile • Define default Apple DEP profile • Assign default Apple DEP profile • Define Apple DEP Profile to DEP Server • Assign Apple DEP Profile to DEP Server • DEP Device Sync (Console) • Upload DEP Server Token • Download Public Key • Assign User • Unassign User • Edit Bulk Assignment Device Data (DEP)
Devices	• Delete Device • Register Device • Update Device Status • Download Device List • Reset Device Status • Modify Device List • Deactivate device • Download visitor list • Send Visitor deactivation code • Download device log • Delete device log file • Download device log file • Delete device log file • Modify device log file • Download App List • Download KME Device List • View Device Location • View Device Location By User&Group • Update Device License • View Device License • View Device Location by Dashboard • Add Multiple Device Tags • Delete Device • Download App List • Download Device List • Download Location History (GPX)

Event Category	Event Name
Devices	• Force Unenroll Device • Refresh Device Status • Add Device Tag • Update Device License • Add Multiple Device Tags • Change Mobile Number (Tizen Wearable) • Download KME Device List • Add Device • Add Multiple Devices • Delete API Users
E-FOTA	• Create E-FOTA Group • Delete E-FOTA Group • Update E-FOTA Group • Check E-FOTA group existence • Update E-FOTA configurations • Valid E-FOTA license check • Update E-FOTA license • Get License Information (Config) • Update E-FOTA configurations • Valid E-FOTA license check • Update E-FOTA license • Display update status by device • View the number of status updates • List of target device list • List of E-FOTA Applied List • Add all to E-FOTA list • Remove all from E-FOTA list • Initialize device assignment list • View E-FOTA license expiration date • Updated E-FOTA Group List • Save list of E-FOTA devices • Add to E-FOTA list • Remove from E-FOTA list • Display whether E-FOTA application list is included • Delete E-FOTA License • Resend update E-FOTA firmware version Device command • Deploy E-FOTA Configuration File

Event Category	Event Name
Email	• Delete Mail Template • Modify Mail Template • Add Mail Template • Send Mail To User • Update SMTP Settings • Send Tizen Wearable Installation Info. • Send Enrollment Email/SMS
Groups	• Delete Group Components (Device/User) • Add Group Components (Device/User) • Manually Delete Device/User From Group • Manually Add Device/User From Group • Delete Selected Group Filter Information • Add Selected Group Filter Information • Delete Selected Group Filter Information • Add Selected Group Filter Information
Groups	• Delete Existing Group • Add New Group • Update Existing Group Information • Delete Device Group Component (Device/User) • Add Device Group Component (Device/User) • Execute synchronization
Integrations	• Add DB Connection • Modify DB Connection • Delete DB Connection • Delete DB Connection List • Test DB Status • Test Every DB Status • Delete Directory Connection Information • Save New Directory Connection Information • Renew Existing Directory Connection Information

Event Category	Event Name
Logs	• Device Audit Log Download • Download Audit Log • Modify Audit Configuration • Modify Audit Use • Download device diagnosis • Add Audit Storage • Revision Audit Storage • Delete Audit Storage • Delete Old Audit Data (Audit Limit)
Notices	• Delete Notice • Add Notice • Modify Notice • Add Notice Multilingual Information • Modify Notice Multilingual Information
Organization	• Delete Existing Organization • Add Organization Into Organization Chart • Update Existing Organization Information • Renew Group Member's Organization Information • Delete Existing Organizations

Event Category	Event Name
Profiles	• Save General Settings • Save KNOX Settings • Delete General Settings • Delete KNOX Settings • Create KNOX • Delete KNOX • Save Client App Control Policy • Save Client Browser Policy • Save Client Policy • Save General Policy • Save KNOX Policy • Save Samsung Knox Policy • Save Trigger General Policy • Save Trigger KNOX Policy • Delete Client App Control Policy • Allocate EMM Profile To Group • Allocate EMM Profile To Organization • Create EMM Agent Profile • Delete EMM Agent Profile • Create Trigger • Delete Trigger • Create app management profile • Delete Application Management Profile • Export Application Management Profile • Import Application Management Profile • Modify Application Management Profile • Copy Application Management Profile • Modify KNOX Workspace Info • Save Visitor Policy • Save Group Mapping Info of Profile • Save Org Mapping Info of Profile • Export Device Management Profile • Save Samsung Knox Policy

Event Category	Event Name
Profiles	• Import Device Management Profile • Modify Device Management Profile • Copy Device Management Profile • Modify Event Priority • Modify Event Info • Modify Event Priority • Select the profile setting in the Pool • Select the Knox setting in the Pool • Upload file • Create Knox Workspace pool • Delete Knox Workspace pool • Create policy of SecuCamera • Create policy of Knox portal • Create general policy of Windows • Select the policy in the Pool • Create the Windows Event Policy • Modify priority of User-Exception Profile • Delete User-Exception Profile • Add User-Exception Profile • Modify User-Exception Profile • Delete Pool • Select the Event policy in the Pool • Request a retransmission handling of Command Transmission Queue • Delete Device Command in Queue • Save Policy • Start all SmartKey MQTT server • Stop all SmartKey MQTT server • Start SmartKey MQTT Server • Stop SmartKey MQTT Server • Delete SmartKey reservation info • Delete SmartKey reservation detail info • Request to send Profile Update device command • View Profile policy • Save Profile policy • Save profile update schedule • View installed Google managed apps on device • Install Google managed app (send Device command) • Uninstall Google managed app (send Device command)

Event Category	Event Name
Profiles	• Delete Android Enterprise Configuration • Save Android Enterprise Configuration • Save Android Enterprise policy • Save Android Enterprise Event policy • Save the policy for Multi Client App Control • Retrieves a summary of policies and settings for a device management profile • Retrieves the device management profile applied to the devices • Retrieves a summary of existing device management profiles assigned to the groups and new device management profiles • Retrieves a summary of existing device management profiles assigned to the organizations and new device management profiles • Changes the priorities of device management profiles and retrieves a summary of device management profiles assigned to the groups or organizations • View Device Mgt. Profile List • Delete Device Mgt. Profile • Create Device Mgt. Profile • Create Device Mgt. Profile (Clone Profile) • Modify Device Mgt. Profile • View Device Mgt. Profile List • Change Device Mgt. Profile Priority • Retrieves a list of devices that are assigned a device management profile • Retrieves by profile ID the group or organization that is assigned a device management profile • Assign Device Mgt. Profile • Unassign Device Mgt. Profile • Retrieves a list of groups that are assigned a device management profile • Retrieves a list of organizations that are assigned a device management profile • Retrieves a list of groups and organizations that are assigned a device management profile • Retrieves by profile ID a list of groups and organizations that are assigned a device management profile • Save Device Mgt. Profile Policy • View Device Mgt. Profile Policy Platform List • Retrieves a list of profile settings including drafts • Retrieves detailed information of a profile settings including drafts • Save Draft Settings • Delete Draft Settings
Service Profiles	• Modify basic information of service profile • Modify Service Profile

Event Category	Event Name
Settings	• Activate API User • Deactivate API User • Delete API User • Add API User • Invalidate API User Tokens • Modify API User • APNs Certificate Signing Request Download • APNs Certificate Upload • APNs Certificate Download • APNs Certificate Import • Add Master Data • Modify Master Data • Delete Master Data • Create IMEI • Delete IMEI • Update IMEI • Upload IMEI file • Modify Profile Update Settings Basic Info • View Profile Update Settings List • View Profile Update Settings • Save Profile Update Settings • Delete Profile Update Settings • Modify Keep-Alive Settings Basic Info • View Keep-Alive Settings List • View Keep-Alive Settings • Save Keep-Alive Settings • Delete Keep-Alive Settings • View EMM Agent Policy List • View EMM Agent Policy • Save EMM Agent Policy • Delete EMM Agent Policy • View Target Group/Organization List

Event Category	Event Name
Settings	• Change APK Download URL in QR Code • Select list of Secure Browser Policy • Select Secure Browser Policy • Save Secure Browser Policy • Delete Secure Browser Policy • Select list of SecuCamera Policy • Select SecuCamera Policy • Save SecuCamera Policy • Delete SecuCamera Policy • Select list of Knox Portal Policy • Select Knox Portal Policy • Save Knox Portal Policy • Delete Knox Portal Policy • Deleting policies by deleting EMM Application • Select Summary of EMM Application Policy • Select list of EMM Client Policy • Select EMM Client Policy • Save EMM Client Policy • Delete EMM Client Policy • Modify Location Report Interval Setting • Save Location Report Interval Setting • Delete Location Report Interval Setting
SMS	• Send SMS To User • Change SMS settings
System Configuration	• Modify Authentication Setting • Modify Server Configuration • Modify Login/Header Image • Modify Logo/Notification Text • Modify Server Configuration • Modify End-User License Agreement • Generate Android Enterprise Signing URL

Event Category	Event Name
User Management	• Modify User Authority • Delete User Authority • Create User Authority • Delete User Device Bookmark • Insert User Device Bookmark • Insert User Device Bookmark • Modify User Device Bookmark • Modify User Device Bookmark • Deactive User
User Management	• Delete User • Add User • Modify User Information • Reset Password (By User) • Reset Password (By Admin) • Confirm User Password • Activate User • Upload Excel Regarding User/Device Information • Update mobile mail status • Update security camera status • Create users • Initialize user password • Create synchronized users • Delete multiple users
VPP Management	• Upload VPP token information downloaded from Apple webpage. • Assign or withdraw VPP Application-specific licenses to users. • View VPP Application on the Apple webpage and update the number of licenses per app. • Upload the VPP Redemption xls (xlsx) file downloaded from Apple webpage. • Access the Apple webpage and update the VPP user information. • Register the user on the Apple webpage, and send invitation mail. • Register the user on the Apple webpage. • Remove and retire the VPP user from the Apple webpage. • Grant the license by user ID • Retrieve the license by user ID • Insert VPP Application

Event Category	Event Name
Windows	• Delete Configuration Service Provider • Add Configuration Service Provider • Modify Configuration Service Provider • Delete PPKG File • Add PPKG File • Modify PPKG File

System audit events

A list of system audit events, whose event target is the system, is as follows:

Event Category	Event Name
Cryptographic Support	• Failure of the Cryptographic Support • Failure of the key zeroization process • Failure of the key generation activity • Failure of cryptographic signature • Failure in Cryptographic Hashing for Non-Data Integrity • Failure of encryption or decryption • Failure of hashing function • Failure of the randomization process
Device Enrollment Program	• Start DEP Scheduler Monitor • End DEP Scheduler Monitor

Event Category	Event Name
EMM System	• Start Up EMM Server • Shut Down EMM Server • EMM Server Update File List • Server Certificate expired • Server Certificate revoked • Created File • Deleted File • Modified File • Renamed File • Integrity Error • Unauthorized Package • EMM Self Test Pass • Self test for cryptographic module • Start MDM scheduler monitor • Stop MDM scheduler monitor
Logs	• Start Audit Logging • Stop Audit Logging
Network Usage	• Network Inventory Scheduler Start • Network Inventory Scheduler End • Network Inventory Batch Start • Network Inventory Batch End
Push	• Request to register PUSH SA (EMM Server ⟶ Push SA) • Respond to the request to register PUSH SA (Push SA ⟶ EMM Server) • Request to verify PUSH Device(Push SA ⟶ EMM Server)
VPP Management	• VPP Sync Scheduler start • VPP Sync Scheduler end

Audit log fields in an exported log file

Administrators can see the audit events that have occurred on devices and EMM servers in the Admin Portal. You can also export the displayed audit events information into a XLS file. The following are descriptions of the excel file items:

Item	Description
Log Date And Time	Date and time when logs are recorded
Type	Target for which events happen • Console: Audit events for the Admin Portal • Server: Audit events, such as external requests and scheduling of the EMM server and devices. • Device: Audit events for the user device • System: Audit events for the EMM server, but not Server events, such as EMM server start-up, device inventory, etc.
User ID	ID for the administrator who performed the task • Console: An Admin or User ID • Server: A device user ID when an event request is sent from the device to the EMM server; a System or Batch user ID for scheduling • Device: A device user ID
Mobile ID	For audit events related to device control, the mobile ID of an event target. • Console: A mobile ID for audit log collection • Server: A mobile ID when an event request is sent from the device to the EMM server; a mobile ID or Batch user ID for scheduling • Device: A mobile ID
Client IP	An IP address for a device that an administrator has used to perform a task
Event Category	For more information about the Event Category, see Lists of audit events.
Event	A type of an occurred event
Result	The execution results of the occurred events.
Level	Severity of the event • Critical: An event of the greatest severity, such as a system interruption • Error: General error events • Warning: Only cautions about an event. This is not an actual error. • Notice: An event that has occurred under conditions that an administrator should know about. • Info: General events that an administrator needs. No action required. • Debug: An event that is defined in detail, which is needed for a developer.

Item	Description
Request History	This is a detailed history about requesting the audit events. For example, if an event is "Save General Policy," all policies that are applied when the profile is changed are displayed.
Result Code	Success or failure as a result of the event
Result History	This information is a result of the audit event. For example, if the event is a "Package deletion failure," a package name and cause of the event that has failed to be removed is displayed.
Log Data	Log data is recorded in the following cases: • 'Console' type event where the data sent to the server is greater than 4000 bytes • 'Server' type event and the event category is 'Device command' and the event is 'Agent Request to lock screen (Device ⟶ Server),' 'Agent Request to unlock device (Device ⟶ Server),' or 'Agent Request for work report (Device ⟶ Server)' • 'Device' type event and the event category is 'Device command' and the event is 'Device Diagnosis Information' or 'Device Lock/Unlock History'

Audit logs of Push and AppTunnel

Audit events generated by Push and AppTunnel Server are recorded in a log file for each server. The audit records contained in these files are not exported through the EMM Admin Portal and are not available for export through syslog. These audit records must first be exported using a secured RDP connection to the Windows server platform on which the EMM, Push and/or AT server are running, then the audit data must be exported through that RDP connection.

Check the Audit log files generated under the folder by remote access to the server.

- `ATR: {ATR_HOME}/LOGS/at/relay/audit*`
- `ATS: {ATS_HOME}/LOGS/at/server/audit*`
- `Push Proxy: {Proxy_HOME}/LOGS/audit/*`
- `Push CM: {Push_HOME}/LOGS/audit/*`
- `Push SA: {EMM_HOME}/log/push/audit/*`

Audit events

Lists of the audit events recorded in the log file of the Push and AppTunnel server are as follows:

Server	Event
AppTunnel	• STARTUP • SHUTDOWN • TLS_HANDSHAKE_START • TLS_HANDSHAKE_COMPLETED • TLS-TERMINATED • TLS_HANDSHAKE_ERROR • CORRUPTION_CHECK_FAIL • KEY_GENERATION_FAIL • ENCRYPT_FAIL • DECRYPT_FAIL • MAKE_SIGNATURE_FAIL • VERIFY_SIGNATURE_FAIL • DIGEST_FAIL • CERT_EXCEPTION • RANDOM_FAIL • CRYPTOJ_SELFTEST_START • CRYPTOJ_SELFTEST_FINISHED • CRYPTOJ_SELFTEST_PASSED • CRYPTOJ_SELFTEST_FAILED • CRYPTOJ_SELFTEST_FORCED_TO_FAIL

Server	Event
Push	• STARTUP • SHUTDOWN • TLS_HANDSHAKE_START • TLS_HANDSHAKE_COMPLETED • TLS-TERMINATED • TLS_HANDSHAKE_ERROR • CORRUPTION_CHECK_FAIL • KEY_GENERATION_FAIL • ENCRYPT_FAIL • DECRYPT_FAIL • MAKE_SIGNATURE_FAIL • VERIFY_SIGNATURE_FAIL • DIGEST_FAIL • CERT_EXCEPTION • RANDOM_FAIL • CRYPTOJ_SELFTEST_START • CRYPTOJ_SELFTEST_FINISHED • CRYPTOJ_SELFTEST_PASSED • CRYPTOJ_SELFTEST_FAILED • CRYPTOJ_SELFTEST_FORCED_TO_FAIL

Audit log fields

Description of audit log items of the Push and AppTunnel server are as follows:

Item	Description
Log Date And Time	Date and time when logs are recorded
Class name	Class information recording logs with 'INFO [c.s.p.l.a.i.ServerAuditLogger:60]' fixed as its value.
Events	Audit event name that Push and AppTunnel server records. For more details, see Audit events.
Source type	Information of the server components, such as PUSH-DA, PUSH-SERVER, PUSH-SA, AT-Client, AT-SERVER, AT-RELAY.
Initial value	Its value set initially • instanceId=value • N/A • PkiMode=true or PkiMode=false(In this case, it is located the end in Details item.)

Item	Description
Level	Severity of the event • Critical: An event of the greatest severity, such as a system interruption • Error: General error events • Warning: Only cautions about an event. This is not an actual error. • Notice: An event that has occurred under conditions that an administrator should know about. • Info: General events that an administrator needs. No action required. • Debug: An event that is defined in detail, that is necessary for developers.
Details	Detailed log contents. These are different by event. For more information, see Audit log details.
Created Date and Time	Date and time when log data is created

Audit log details

Items of the audit log are separated by a comma except the 'Log Date And Time' item and the 'class name' item and the items of details are separated by '&.'

Event	Detail by case
STARTUP	• `tcpPort`=TCP listening port • `eTcpPort`=External TCP listening port`&iTcpPort`=Internal TCP listening port • `tcpPort`=TCP listening port`&UdpPort`=UDP listening port • `UdpPort`=UDP listening port • `SAIID`=SA instance ID`&SAGID`=SA group ID
SHUTDOWN	• CAUSE=reason of shut down • N/A
TLS_HANDSHAKE_START	• remote-host=Connection host&remote-port=Connection port • remote-host=Connection host `remote-host`=Connection host`&remote-port`=Connection port`&CHID`=Channel ID
TLS_HANDSHAKE_COMPLETED	• remote-host=Connection host&protocol=TLS protocol&ciphersuite=CipherSuite name of configured TLS • remote-host=Connection host&protocol=TLS protocol&ciphersuite=CipherSuite name of configured TLS&CHID=Channel ID
TLS_TERMINATED	• remote-host=Connection host • CHANNELID=Channel ID&EXCEPTION OCCURRED=Content error • CHANNELID=Channel ID&Cause=Content error • remote-host=Connection host&remote-port=Connection port&CHID=Channel ID

Event	Detail by case
TLS_HANDSHAKE_ERROR	• remote-host=Connection host&remote-port=Connection port&cause=Error class&ERR=Error message • remote-host=Connection host&cause=Error class&ERR=Error message • remote-host=Connection host&cause=Error class and message • ERR=Error message • remote-host=Connection host&remote-port=Connection port&CHID=Channel ID&cause=Error class and message
CORRUPTION_CHECK_FAIL	• jar file path=Not Signed • jar file path=is Corrupted • jar file path=is not signed By Push
KEY_GENERATION_FAIL	• cert=Error code and message • EX=Error class&MSG=Error message
ENCRYPT_FAIL	• EX=Error class&MSG=Error message
DECRYPT_FAIL	• EX=Error class&MSG=Error message
MAKE_SIGNATURE_FAIL	• EX=Error class&MSG=Error message
VERIFY_SIGNATURE_FAIL	• cert=Error code and message • EX=Error class&MSG=Error message
DIGEST_FAIL	• EX=Error class&MSG=Error message
CERT_EXCEPTION	• ERRCODE=Error code&MSG=Error message
RANDOM_FAIL	• EX=Error class&MSG=Error message
CRYPTOJ_SELFTEST_START	• testName=Test target name&testId=Test ID
CRYPTOJ_SELFTEST_FINISHED	• testName=Test target name&testId=Test ID
CRYPTOJ_SELFTEST_PASSED	• testName=Test target name&testId=Test ID

Admin Portal access error codes

The following is the list of error codes that can occur on devices or the Samsung SDS EMM server. See the instructions below when an error occurs. You can contact the IT admin for more details.

Log in

Code	Description	Log path
session	The account is already in use.	emm.log
disable	The account is locked.	
accountDeleted	Account access is not authorized based on the policy.	
accountLocked	Account access is not authorized based on the policy.	
continousFailure	The account is locked for 10 minutes.	

Report

Code	Description	Log path
1101	Parameter is invalid.	emm.log
1102	Data not found.	
1103	Service is disabled.	
1104	Internal reports cannot be modified.	
1120	SQL exception.	
1121	Datasource Pool not found.	
1199	Runtime error occurred.	

Open API

Code	Description	Log path
-102	Null or Empty string.	emm.log
-103	Null object.	
-104	Not a number (integer).	
-105	The number must be greater than %d.	
-106	The number must be less than &d.	
-107	The number must be between %d and %d.	
-108	The string length must be greater than %d.	
-109	The string length must be less than %d.	
-110	The data must be in a %s format.	
-111	The start-date should be before the end-date.	
-112	The string should match %s.	
-113	The subsequent strings should not contain or match %s.	
-114	The string is not equal to %s while being case-sensitive.	
-115	The string is not equal to %s while being case-insensitive.	
-116	The string is configured with whitespace or tab only.	
-117	The string's length must be greater than %d (bytes).	
-200	The number of licenses has been exceeded.	
-201	Duplicate data exists.	
-202	There are no results.	
-203	Relevant data has an error.	
-204	Enrolled device exists.	
-205	Cannot be found.	
-206	Already registered to the selected group.	
-999	Unknown error code.	

Certificate

Code	Description	Log path
3000	Certificate generation request failed.	emm.log
3001	Certificate verification request failed.	
3002	Client initialization failed.	
3003	Certificate enrollment transaction failed.	certlog.log
3004	Certificate enrollment request failed.	
3005	The maximum retries of certificate enrollment exceeded.	
3006	Certificate enrollment failed.	
3007	CRL request failed.	
3008	CA chain request failed.	
LEGO_ERR_0001	Provider load failed.	
LEGO_ERR_1100	Wrong CA type.	
LEGO_ERR_1101	CA type does not exist.	
LEGO_ERR_1102	Root Certificate lookup data not found.	
LEGO_ERR_1103	CA lookup data not found.	
LEGO_ERR_1104	Managed CA does not exist.	
LEGO_ERR_1105	CN and password are required for entry registration.	
LEGO_ERR_1106	Ext CERT lookup data not found.	
LEGO_ERR_1107	CERT lookup data not found.	
LEGO_ERR_1108	Template lookup data not found.	
LEGO_ERR_1109	Batch lookup data not found.	
LEGO_ERR_1200	The certificate number does not exist.	
LEGO_ERR_1201	CN information does not exist.	
LEGO_ERR_1202	File storage path does not exist.	
LEGO_ERR_1203	Entity ID does not exist.	
LEGO_ERR_1204	CA information, CertProfileName, and, EndEntityProfile information are required if the template ID does not exist.	
LEGO_ERR_1205	The certificate to revoke does not exist.	
LEGO_ERR_1206	Error occurred when saving certificate revoke information.	
LEGO_ERR_1207	Error occurred while performing ReIssue.	
LEGO_ERR_1208	Error occurred while saving ReNew information.	
LEGO_ERR_1300	Template ID does not exist.	

Code	Description	Log path
LEGO_ERR_1301	Tenant ID does not exist.	
LEGO_ERR_1302	Updated data not found on DB.	
LEGO_ERR_1400	The certificate name already exists.	
LEGO_ERR_1401	The tenant ID already exists.	
LEGO_ERR_1500	CERT verification failed: Start date is after the current date.	
LEGO_ERR_1501	CERT verification failed: Expiration date is before the current date.	
LEGO_ERR_1502	CERT verification error: Error occurred when verifying CA root Init.	
LEGO_ERR_1503	CERT verification error: Signature error occurred.	
LEGO_ERR_1504	Lookup data not found.	
LEGO_ERR_1505	Pkcs12 CERT import failed.	
LEGO_ERR_1506	The CA Cert does not exist in the file.	
LEGO_ERR_1900	Error occurred when creating a file.	
LEGO_ERR_1901	File does not exist.	
LEGO_ERR_2001	CRL creation failed.	
LEGO_ERR_2002	CRL request creation failed.	
LEGO_ERR_2003	CRL verification failed.	certlog.log
LEGO_ERR_2004	CRL information on the last executed file does not exist.	
LEGO_ERR_2005	CRL request for the last executed file failed.	
LEGO_ERR_2006	Save CRL information failed.	
LEGO_ERR_2101	CRL BATCH SCHEDULE addition failed.	
LEGO_ERR_2102	CRL BATCH SCHEDULE information update failed.	
LEGO_ERR_2103	CRL BATCH SCHEDULE deletion failed.	
LEGO_ERR_3000	Scep message creation failed: Certificate request creation failed.	
LEGO_ERR_3001	Scep message creation failed: Wrong trandsId.	
LEGO_ERR_3002	Scep message creation failed: Wrong senderNonce.	
LEGO_ERR_3003	Scep verification failed: Signer value does not exist.	
LEGO_ERR_3004	Scep verification failed: Wrong digest algorithm.	
LEGO_ERR_3005	Scep verification failed: Wrong CA signer.	
LEGO_ERR_3006	Scep verification failed: Wrong signature certlog.log.	
LEGO_ERR_3007	Scep verification failed: FailInfo is included in ScepRequestMessage	
LEGO_ERR_3008	Scep verification failed: Wrong message type.	

Code	Description	Log path
LEGO_ERR_3009	Scep verification failed: pkiStatus does not exist in ScepRequestMessage.	
LEGO_ERR_3010	Scep verification failed: Success message does not exist.	
LEGO_ERR_3011	Scep verification failed: Wrong Response status.	
LEGO_ERR_3012	Scep verification failed: Wrong SenderNonce.	
LEGO_ERR_3013	Scep verification failed: Wrong recipientNonce.	
LEGO_ERR_3014	Scep verification failed: Wrong Transaction.	
LEGO_ERR_3015	Scep connection failed: Wrong responseCode.	
LEGO_ERR_3016	Scep connection failed: Wrong content type.	
LEGO_ERR_3017	Scep connection failed: Response data does not exist.	
LEGO_ERR_3018	Scep connection failed: Response byte conversion failed.	
LEGO_ERR_4000	Cmp connection failed: HTTP connection failed.	
LEGO_ERR_4001	Cmp connection failed: Wrong responseCode.	
LEGO_ERR_4002	Cmp connection failed: Content type does not exist.	
LEGO_ERR_4003	Cmp connection failed: Wrong Content type.	
LEGO_ERR_5000	WebService connection verification failed.	
LEGO_ERR_5001	WebService connection failed.	certlog.log
LEGO_ERR_5002	Error occurred during FIND ENTITY.	
LEGO_ERR_5003	Error occurred while chaining entity.	
LEGO_ERR_5004	Error occurred while registering entity.	
LEGO_ERR_5005	Entity is already registered.	
LEGO_ERR_6000	Root CA conversion failed.	
LEGO_ERR_6001	Root CA conversion failed: X509Certificate conversion failed.	
LEGO_ERR_6002	Root CA conversion failed: Wrong algorithm.	
LEGO_ERR_6003	Root Cert does not exist.	
LEGO_ERR_8000	Certificate verification failed: PKIMeesage configuration failed.	
LEGO_ERR_8001	Certificate verification failed: PKI Header configuration failed.	
LEGO_ERR_8002	Certificate verification failed: Failure may be due to a wrong issuer sign value or revoked certificate.	
LEGO_ERR_8003	Certificate verification failed: Wrong senderNonce.	
LEGO_ERR_8004	Certificate verification failed: Wrong transactionID.	
LEGO_ERR_8005	Certificate verification failed: Wrong algorithm.	
LEGO_ERR_8006	Certificate verification failed: Signature is unprotected.	

Code	Description	Log path
LEGO_ERR_8007	Certificate verification failed: Password is unprotected.	certlog.log
LEGO_ERR_8008	Certificate verification failed: Algorithm is invalid.	
LEGO_ERR_8009	Certificate verification failed: CA signature is not verified.	
LEGO_ERR_8010	Certificate verification failed: Wrong PBE hash.	
LEGO_ERR_8011	Certificate verification failed: Signature verification failed.	
LEGO_ERR_8012	Certificate configuration failed: PKIBody configuration failed.	
LEGO_ERR_8013	Certificate configuration failed: CertRepMessage configuration failed.	
LEGO_ERR_8014	Certificate configuration failed: CertResponse configuration failed.	
LEGO_ERR_8015	Certificate configuration failed: CertReqId configuration failed.	
LEGO_ERR_8016	Certificate configuration failed: PKIStatusInfo configuration failed.	
LEGO_ERR_8017	Certificate configuration failed: Wrong Status Value.	
LEGO_ERR_8018	Certificate configuration failed: CertifiedKeyPair configuration failed.	
LEGO_ERR_8019	Certificate configuration failed: CertOrEnCert configuration failed.	
LEGO_ERR_8020	Certificate configuration failed: X509CertificateStructure configuration failed.	
LEGO_ERR_8021	Certificate configuration failed: Certificate encoding failed.	
LEGO_ERR_8022	Certificate configuration failed: X509Certificate configuration failed.	
LEGO_ERR_8023	Certificate configuration failed: SubjectDN is inconsistent.	
LEGO_ERR_8024	Certificate configuration failed: IssuerDN is inconsistent.	
LEGO_ERR_8025	Certificate configuration failed: X509Certificate verification failed.	
LEGO_ERR_9000	Wrong URL information.	
LEGO_ERR_9002	Http connection failed.	
LEGO_ERR_9003	Response data from CA does not exist.	
LEGO_ERR_9004	Wrong host information.	
LEGO_ERR_9005	Socket connection failed.	
LEGO_ERR_9006	HOST information does not exist.	
LEGO_ERR_9007	Contingency occurred while converting ASN1 InputStream.	
LEGO_ERR_9008	Contingency occurred while converting DER OutputStream.	
LEGO_ERR_9009	Provider does not exist.	
LEGO_ERR_9010	Algorithm does not exist.	
LEGO_ERR_9011	X509Certificate conversion failed.	
LEGO_ERR_9012	X509Certificate encoding failed.	

Code	Description	Log path
LEGO_ERR_9013	Error occurred while creating KeyStore.	certlog.log
LEGO_ERR_9014	Error occurred while converting class.	
LEGO_ERR_9015	Contingency occurred while converting InputStream.	
LEGO_ERR_9016	Keystore password is inconsistent.	
LEGO_ERR_9017	Error occurred while creating SecretKey.	
LEGO_ERR_9018	Revoke reason is undefined.	
LEGO_ERR_9019	Error occurred while converting Object to byte.	
LEGO_ERR_9020	Error occurred while converting byte to Object.	
LEGO_ERR_9100	Certificate corresponding to the alias does not exist.	
LEGO_ERR_9101	Error occurred while extracting KeyStore PrivateKey.	
LEGO_ERR_9102	Error occurred while extracting KeyStore Certificate.	
LEGO_ERR_9103	Error occurred while extracting KeyStore Aliases.	
LEGO_ERR_9104	Error occurred while saving PKCS12-type KeyStore.	
LEGO_ERR_9105	Contingency occurred while deleting KeyStore: KeyStore error occurred.	
LEGO_ERR_9106	Contingency occurred while deleting KeyStore: File does not exist.	
LEGO_ERR_9107	Contingency occurred while deleting KeyStore: Error occurred while restoring.	
LEGO_ERR_9108	File InputStream is empty.	
LEGO_ERR_9109	Error occurred while converting Object to Map.	
LEGO_ERR_9110	Error occurred while converting Map to Object.	
LEGO_ERR_9111	Batch type does not exist.	
LEGO_ERR_9112	Template does not exist.	
LEGO_ERR_9200	Compulsory input is missing: Serial number.	
LEGO_ERR_9901	Encryption failed.	
LEGO_ERR_9902	Decryption failed.	
LEGO_ERR_999	Unexpected error occurred. Please contact the IT Administrator.	

CA certificate access test

Module	Code	Description	Log path
Certificate ADCS CA	ERROR_ROOT_CHAIN_TEST	Root chain import failed.	emm.log
	ERROR_ROOT_CERT_PW	Wrong certificate password.	
	ERROR_Android_ISSUE_TEST	Issuing certificate failed. (Android)	
	ERROR_Android_KEY_ALG	Key algorithm error. (Android)	
	ERROR_Android_DOMAIN	Domain error. (Android)	
	ERROR_Android_CES_URL	Webservice URL error. (Android)	
	ERROR_Android_CA_SERVER	CA server settings error. (Android)	
	ERROR_Android_KERBEROS_REALM	Kerberos settings error. (Android)	
	ERROR_Android_KEY_TABEL	Keytab settings error. (Android)	
	ERROR_Android_CERT	Certificate error. (Android)	
	ERROR_iOS_ISSUE_TEST	Issuing certificate failed. (iOS)	
	ERROR_iOS_KEY_ALG	Key algorithm error. (iOS)	
	ERROR_iOS_DOMAIN	Domain error. (iOS)	
	ERROR_iOS_CES_URL	Web service URL error. (iOS)	
	ERROR_iOS_CA_SERVER	CA server settings error. (iOS)	
	ERROR_iOS_KERBEROS_ REALM	Kerberos settings error. (iOS)	
	ERROR_iOS_KEY_TABEL	Keytab settings error. (iOS)	
	ERROR_iOS_CERT	Certificate error. (iOS)	
Certificate SCEP CA	ERROR_ROOT_CHAIN_TEST	Root chain import failed.	emm.log
	ERROR_ISSUE_TEST	Issuing certificate failed.	
	ERROR_SCEP_MSGSIGN ERCERT_ TEST	Creating SCEP Message Signer certificate failed.	
Certificate NDES CA	CONNECTION_FAIL	Wrong Challenge URL.	emm.log
	CERTSRV_ADMIN_UNAUTHORIZED	Wrong ID or password.	
	CERTSRV_ADMIN_URL_INVALID	Wrong challenge URL.	
	NDES_NOT_PERMISSION	Wrong domain.	
	NDES_CHALLENGE_NOT_FOUND	Challenge password cannot be found. Need to check NDES server settings.	
	NDES_CHALLENGE_FAIL	Challenge password cannot be found.	

Policy

Module	Code	Description	Log path
Common	0000000	Success.	Console
	9999999	Failure.	
	9000001	Component already exists.	
	9000002	Component ID and type are inconsistent.	
	9000003	Error occurred in mandatory parameter.	
	9000004	Component value already exits.	
	9000005	MDM license is invalid.	
	9000006	Config type already exists.	
	9000007	VPN app ID already exists.	
	9000008	Special characters are not allowed.	
	9000009	The admin ID has not been approved.	
	9000010	DB service error.	
	9000011	URL information is invalid.	
	2000000	OTC code is invalid.	mdm_otc.log, mdm.log
	2000001	This device platform does not support OTC.	
	2000002	Enter the OTC code.	
	2000003	Enter the device ID to transfer.	
	2000004	A device token for the iOS Agent does not exist.	
	2000005	Enter the Push App ID information.	
	2000006	OTC message creation failed.	
	2000008	Enter the OTC parameter information.	
	2000010	Push magic for iOS device does not exist.	
	2000011	UMP App ID is invalid.	
	2000012	There is no device registered for the user.	
Common	2000013	There is no device to send OTC to the user.	mdm_otc.log, mdm.log
	2000014	Device token for iOS Client does not exist.	
	2000015	Device token for iOS Agent is invalid.	
	2000016	Device token for iOS Client is invalid.	
	2000017	Screen Lock OTC is not applicable.	
	2000018	Exception error occurred when handling OTC Enqueue.	
	2000019	Device tenant ID to transmit OTC does not exist.	

Module	Code	Description	Log path
Profile	0100001	A profile applied to a device cannot be deleted.	Console
	0100002	Profile ID does not exist.	
	0100003	Visitor profile ID.	
	0100004	Profile component does not exist.	
	0100005	Profile element does not exist.	
	0103001	Hash value creation failed.	
	0103002	Hash value is inconsistent.	
	0103003	Profile type is inconsistent.	
	0103004	Reading profile file when importing failed.	
	0103005	Saving profile file when exporting failed.	
	0103006	File extension of the profile is inconsistent when importing.	
	0199001	Profile has not been assigned to a device.	
	0199002	Profile has not been assigned to a user.	
	0199003	Profile has not been assigned to an organization.	
	0199004	Profile has not been assigned to a group.	
	0199005	Device has not been assigned to a profile.	
	0199010	Group does not exist.	
	0199012	Profile has already been assigned to the group.	
	0199020	Organization does not exist.	
	0199022	Profile has already been assigned to the organization.	
Knox	0210001	Knox Workspace Alias already exists.	Console
	0210002	The maximum number of Knox Workspaces to be created has been exceeded.	
	0210003	Knox Workspace of this type cannot be created.	

Module	Code	Description	Log path
EVENT	0301500	Exceeded the priority of the event policy range.	Console
	0301501	Priority of the event policy deletion error.	
	0301502	Priority of the event policy already exists.	
	0301503	Profile event does not exist.	
	0301504	The priority of the event policy has been changed by other users.	
	0301505	SIM card change event can be created only once.	
	0301506	Roaming event can be created only once.	
	0301507	Exception profile per user event can be created only once.	
	0320001	Event used as components cannot be deleted.	
POLICY	0410001	Only a Boolean value is allowed for this policy.	Console
	0410002	Only an integer value is allowed for this policy.	
	0410003	Exceeded the policy range.	
	0420001	Minimum value error occurred when comparing policies.	
	0420002	Maximum value error occurred when comparing policies.	
	0430001	Exceeded the number of internal app policies. **NOTE** The maximum number of policies is 15 for each platform.	
CONFIGRATION	0510000	A certificate used in a profile. **NOTE** Deletion is prohibited.	Console
	0510001	A certificate for iOS use. **NOTE** Deletion is prohibited.	mdm_ios_agent.log, mdm.log
	0530001	Not in an XML format.	Console
FCM Push	2002000	[FCM] Server information does not exist.	mdm_otc.log, mdm.log
	2002001	[FCM] Authentication failed.	
	2002002	[FCM] Internal server error.	
	2002003	[FCM] Service outage.	
	2002004	[FCM] Too many messages sent at a time (1000).	
	2002005	[FCM] Too many messages sent to one device (100).	

Module	Code	Description	Log path
FCM Push	2002006	[FCM] Missing device registration ID.	mdm_otc.log, mdm.log
	2002007	[FCM] Invalid device registration ID.	
	2002008	[FCM] Mismatch between the registered sender ID and device ID.	
	2002009	[FCM] Cancel device registration or alarm use.	
	2002010	[FCM] Exceeded the maximum transmission message length (4KB).	
	2002011	[FCM] Missing sender ID.	
	2002012	[FCM] Message transmission error (FCM server error).	
	2002013	[FCM] Message format error (FCM server error).	
	2002014	[FCM] Invalid message TTL.	
	2002015	[FCM] Push key does not exist.	
	2002016	[FCM] Internal exception occurred.	
	2002017	[FCM] Unknown error.	
APNS Push	2003000	[APNS] Server information does not exist.	mdm_otc.log, mdm.log
	2003001	[APNS] Internal processing error.	
	2003002	[APNS] Missing token.	
	2003003	[APNS] Missing topic in the certificate.	
	2003004	[APNS] Missing message.	
	2003005	[APNS] Token size error.	
	2003006	[APNS] Topic size error.	
	2003007	[APNS] Exceeded the maximum transmission message length.	
	2003008	[APNS] Invalid token.	
	2003009	[APNS] Server down.	
	2003010	[APNS] Protocol error.	
	2003011	[APNS] Internal exception occurred.	
	2003012	[APNS] Unknown error.	
	2003013	[APNS] Payload creation error.	
	2003014	[APNS] Agent push key does not exist.	
	2003015	[APNS] Client push key does not exist.	

Module	Code	Description	Log path
WNS Push	2004000	[WNS] No server information.	mdm_otc.log, mdm.log
	2004001	[WNS] Invalid request.	
	2004002	[WNS] Invalid token.	
	2004003	[WNS] Requested channel does not have the permission to send.	
	2004004	[WNS] Invalid channel.	
	2004005	[WNS] Invalid http method.	
	2004006	[WNS] Load exceeded.	
	2004007	[WNS] Channel expired.	
	2004008	[WNS] Exceeded the maximum message length (5 KB).	
	2004009	[WNS] Internal server error.	
	2004010	[WNS] Service outage.	
	2004011	[WNS] Internal exception occurred.	
	2004012	[WNS] Unknown error.	
	2004013	[WNS] Push key does not exist.	
	2004014	[WNS] Device channel URL information does not exist, but the queue information is created in the command queue to be processed later.	
	2004015	[WNS] WNS server information does not exist, but the queue information is created in the command queue to be processes later.	
iOS MDM	1500000	Request for the command more than ten times.	mdm_ios_agent.log, mdm.log
	1500001	MDM profile assigned does not exist.	
	1500002	Device with a corresponding device ID does not exist on the device information table.	
	1500003	Profile cannot be created.	
	1500004	Certificate file cannot be found.	
	1500005	Certificate file cannot be read.	
	1500006	Check-in authentication failed.	
	1500007	Not iOS.	
	1500008	User is not activated.	
	1500010	Device is not in an active (A) or provision (P) state.	
	1500011	Device cannot be updated. UDID already exists.	
	1500013	Device ID pertinent to the tenant ID does not exist.	

Module	Code	Description	Log path
iOS MDM	1500014	Send push failed.	mdm_ios_agent.log, mdm.log
	1500015	Reactivation prevention. **NOTE** Reactivation is prevented in case the activated device is reactivated due to a factory reset.	
	1500016	Activation failed. **NOTE** Activation failed due to an activation attempt with a different mobile ID (device ID) using the same tenant in the same device.	
	1500017	Profile signing failed.	
	1500018	Activation failed. **NOTE** Activation failed due to an activation attempt with a same mobile ID (device ID) using the same tenant in a different device.	
	1500020	Parameter information error.	
	1500024	Activation profile cannot be created.	
	1500029	App information lookup failed.	
	1500030	Device activation failed.	
	1500031	Device deactivation failed.	
	1500032	Token update failed.	
	1500033	App installation is prohibited.	
	1500034	App installation failed.	
	1500035	Whitelisted and blacklisted app lookup failed.	
	1500036	Unable to fetch the app info from the app auto- delete property sync when deactivated.	
	1500101	Unable to execute command now.	
	1500102	MDM command format is invalid.	

Module	Code	Description	Log path
Android MDM	1900000	Profile cannot be copied.	mdm.log
	1900001	Profile cannot be changed to JSON string.	
	1900002	Profile cannot be changed to JSON string.	
	1900003	Profile cannot be changed to JSON string.	
	1900004	Profile code invalid.	
	1900005	Profile type is invalid.	
	1901000	Category for settings in general area is invalid.	
	1901001	Category for settings in Knox Workspace area is invalid.	
	1901010	Information required by a device cannot be checked.	mdm_android_agent.log, mdm.log
	1901011	Request message from a device cannot be parsed.	
	1901012	EMM Agent request message cannot be checked.	
	1901013	Undefined command code.	
	1901014	Error occurred when creating file.	
	1901015	Version of the requested protocol is invalid.	
	1901016	A request message from a device cannot be checked.	
	1901017	ELM license and Knox license cannot be found.	
	1901018	Tenant ID cannot be found.	
	1901019	Command parameter is invalid.	
	1901020	EMM Client and EMM Agent app information cannot be found.	
	1901021	Profile cannot be created.	
	1901022	Profile assigned to a device cannot be found.	
	1901024	Device status cannot be updated.	
	1901025	Device status cannot be updated (UpdateDeviceInformation Command).	
	1901026	Error occurred when processing KeepaliveRequest.	
	1901027	Error occurred when processing LockDeviceRequest.	
	1901028	Error occurred when processing UnlockDeviceRequest.	
	1901029	Error occurred when processing LocknoxContainerRequest.	
	1901030	Error occurred when processing InstallKnoxAppRrrequest.	
	1901031	Error occurred when processing UninstallKnoxAppRequest.	

Module	Code	Description	Log path
Android MDM	1901032	Error occurred when processing RemoveKnoxAppInternalDataRequest.	mdm_android_agent.log, mdm.log
	1901033	Error occurred when processing StartKnoxAppRequest.	
	1901034	Error occurred when processing StopKnoxAppRequest.	
	1901035	Result of the EMM Agent message is not successful and cannot be processed.	
	1901036	Result of a message from EMM Agent cannot be checked.	
	1901037	Parameter of EnrollmentSpecRequest is not appropriate.	
	1901038	Error occurred when processing InstallAppRequest.	
	1901039	Error occurred when processing TriggerRequest.	
	1901040	Error occurred when processing handlingReportRequest.	
	1901041	Error occurred when processing ResetPasswordRequest.	
	1901042	Error occurred when processing ResetExternalSdCardRequest.	
	1901043	Error occurred when processing AuthorizeExternalSDCardRequest.	
	1901044	Error occurred when processing WipeDeviceRequest.	
	1901045	Error occurred when processing RebootDeviceRequest.	
	1901046	Error occurred when processing PowerOffDeviceRequest.	
	1901047	Error occurred when processing UninstallAppRequest.	
	1901048	Error occurred when processing RemoveAppInternalDataRequest.	
	1901049	Error occurred when processing StartAppRequest.	
	1901050	Error occurred when processing StopAppRequest.	
	1901051	Error occurred when processing AppInfoRequest.	
	1901052	Error occurred when processing UnlockKnoxContainerRequest.	
	1901053	Error occurred when processing ResetKnoxContainerPasswordRequest.	
	1901054	Error occurred when processing RemoveKnoxContainerRequest.	
	1901055	Error occurred when processing StartCCModeRequest.	
	1901056	Error occurred when processing StopCCModeRequest.	
	1901057	EMM Agent profile does not exist.	
	1901058	Requested app information cannot be found.	

Module	Code	Description	Log path
Android MDM	1901059	App file not found at path.	mdm_android_agent.log, mdm.log
	1901060	Keepalive information cannot be imported (Included in Settings).	
	1901061	Requested Knox app information cannot be found.	
	1901062	Knox file not found at path.	
	1901063	Error occurred when processing InstallAppRequest.	
	1901064	Basic device information cannot be searched with a device ID.	
	1901065	Device is not activated.	
	1901066	Device status cannot be checked.	
	1901067	System app information cannot be found.	
	1901068	EMM Agent app information cannot be found.	
	1901069	Error occurred when processing UpdateAgentRequest.	
	1901070	Device status is neither provisioned nor activated.	
	1901071	File path cannot be imported.	
	1901072	App ID in command parameter does not exist.	
	1901073	Package name in command parameter does not exist.	
	1901074	Device status is not provisioned.	
	1901075	Device status cannot be changed to unmanaged.	
	1901076	Device status cannot be changed to managed.	
	1901077	Device has already been activated.	
	1901079	Offline deactivation code cannot be updated.	
	1901080	Error occurred when processing LockEasRequest.	
	1901081	Error occurred when processing UnlockEasRequest.	
	1901082	Status of device is neither Activated nor Disconnected.	
	1901083	Data is invalid (InvalidCommandData as shown in the result of a policy).	
	1901084	Error occurred when processing GetAttestationNonceRequest.	
	1901085	Error occurred when processing VerifyAttestationDataRequest.	
	1901086	Attestation server address cannot be found.	
	1901087	Attestation API key cannot be found.	
	1901088	Attestation Parameter is invalid.	

Module	Code	Description	Log path
Android MDM	1901090	EMM Client app information cannot be found.	mdm_android_agent.log, mdm.log
	1901091	EMM Agent app information cannot be found.	
	1901092	Error occurred when processing AuthorizeSimRequest.	
	1901093	Error occurred when handling UpdateUnenrollCodeRequest.	
	1901094	Device status is disconnected.	
	1901095	Error occurred when processing EnableAppRequest.	
	1901096	Error occurred when processing DisableAppRequest.	
	1901097	Failed to decrypt the ELM license.	
	1901098	Error occurred when processing ReportPolicyViolationRequest.	
	1901099	AndroidForWork app information cannot be found.	
	1901100	AndroidForWork app file not found in path.	
	1901101	Error occurred when processing InstallAfwAppRequest.	
	1901102	Error occurred when processing UninstallAfwAppRequest.	
	1901103	Device status cannot be changed to disconnected.	
	1901104	Failed to check if the device already exists.	
	1901105	The information of a device activated with the same equipment already exists.	
	1901106	Error occurred when processing UpdateDiagnosisRequest.	
	1901107	Unable to find the app auto-delete settings information when deactivated.	
	1901108	Unable to fetch the next command.	
	1901109	Failed to create the command message.	
	1901110	Failed to delete the command.	
	1901111	MDM old protocol communication usage.	
	1901112	Error occurred when processing the Update Device Inventory (request).	
	1901113	Error occurred when processing the Update App Inventory (request).	
	1901114	Error occurred when processing the Update Current Location Inventory (request).	
	1901115	Error occurred when processing the Update Audit Inventory (request).	

Module	Code	Description	Log path
Android MDM	1901116	Error occurred when processing the Update Log Inventory (request).	mdm_android_agent.log, mdm.log
	1901117	Content ID does not exist in the requested parameter.	
	1901118	Content information cannot be found.	
	1901119	Error occurred when processing the download content request.	
	1901120	Error occurred when processing the Update Device and App Inventory (request).	
	1901121	Model number does not exist in the requested parameter.	
	1901122	Customer code does not exist in the requested parameter.	
	1901123	Permitted firmware version cannot be found.	
	1901124	Permitted firmware version does not exist.	
	3100003	Android Enterprise device is not supported.	
	3100004	Android Legacy device is not supported.	

Module	Code	Description	Log path
Client	1600000	Information on the parameter of Header does not exist.	mdm_ai_client.log, mdm.log
	1600001	Compression failed.	
	1600002	Encryption failed.	
	1600003	The command does not exist.	
	1600004	Invalid version.	
	1600005	The device ID does not exist on the server.	
	1600006	Invalid device ID. (not A.P)	
	1600010	Failed to check the device ID DB.	
	1601001	OTC transfer failed.	
	1601002	Failed to check the application DB.	
	1601003	Failed to check the Knox ID DB.	
	1601004	Client ID does not exist in the request parameter.	
	1601005	App ID does not exist in request parameter.	
	1601006	Package name does not exist in the request parameter.	
	1601007	Knox ID does not exist in the request parameter.	
	1601008	Knox Workspace ID matching the parameter Knox ID does not exist.	
	1601009	App information corresponding to the parameter App ID does not exist.	
	1601010	Invalid OTC code.	
	1601011	Application is not included in the whitelist/blacklist.	
	1601012	profileId cannot be found in AndroidForWork.	

Module	Code	Description	Log path
Client	1601020	User ID does not exist in the request parameter.	mdm_ai_client.log, mdm.log
	1601021	Inserting webpage information failed.	
	1601022	User ID does not exist in request parameter.	
	1601023	Bookmark index does not exist in request parameter.	
	1601024	Failed to insert bookmark information DB.	
	1601030	Failed to update the device token DB update.	
	1601031	Failed to check the profile DB.	
	1601032	Failed to check the app information DB.	
	1601033	Failed to create profile.	
	1601034	Failed to update DB for the time of the last update of profile.	
	1601035	Failed to check the app information DB.	
	1601036	Failed to update the EMM Client package information.	
	1601040	Failed to update DB related to location and jailbreak information, etc.	
	1601041	Invalid report type.	
	1601060	Device ID does not exist.	
	1601061	It has not been activated (A).	
	1601062	It has not been deactivated (I).	
	1601063	Visitor Profile cannot be created.	
	1601064	Profile to enable deleting visitor profiles cannot be created.	
	1601065	Failed to delete visitor profile.	
	1601066	Failed to check device.	
	1601070	Failed in Knox CheckEnrollment.	
	1601080	Failed to fetch the command.	
	1601081	Failed to delete the command.	
	1601082	No more commands.	
	1601083	Failed to create the command message.	
	1601090	Unable to get the INI configuration file.	

Module	Code	Description	Log path
Kiosk	1700001	Failed to obtain server key.	mdm.log
	1700002	Decryption failed.	
	1700003	Encryption failed.	
	1700004	There is no HTTP body.	
	1700005	A value not supported by HTTP header has been entered.	
	1700006	Compulsory factor in EMM Message has not been entered.	
	1700007	Protocol version not available.	
	1700008	Failed to check device information.	
	1700009	The device has not been activated.	
	1700010	Failed to check app information.	
	1700011	This OTC code is not available.	
	1700012	OTC transfer failed.	
	1700013	Failed to check Kiosk Launcher information.	
	1700014	Kiosk Launcher cannot be created through Wizard.	
	1700015	Failed to check the current time.	
	1700016	Compression failed.	
	1700017	Failed to cancel compression.	
	1700018	Failed to create EMM Message.	
	1700019	Failed to transfer HTTP Response.	
Provision	1001	There is no Public Key on the server.	mdm_ provision. log
	1002	Error in server GetPublicKey Runtime.	
	1003	There is no device information on the server.	
	1004	There is no device registered to the server.	
	1005	The device has been Disconnected.	
	1008	Error in server provision runtime	
	1009	There is no Private Key on the server.	
	1011	The status of the server does not allow initProvision.	
	1018	There is no device matching for InitProvision.	
	1019	A device has already been provisioned on the server.	
	1021	Error in server InitProvision Runtime.	
	1022	User ID cannot be found.	
	1023	Authentication failed due to inconsistent ID or password.	

Module	Code	Description	Log path
Provision	1024	Network communication error.	mdm_ provision. log
	1025	The number of devices automatically registered has been exceeded.	
	1026	The value of the device ID is not valid.	
	1031	Failed to read license information.	
	1032	The device has been disconnected.	
	1033	The number of devices allowed to be registered for each user has been exceeded.	
	1034	The platform information transferred from the device does not match the platform information stored in the server.	
	1035	The device is not exclusively for Wi-Fi, but it does not have a Mac address and IMEI information.	
	1036	The device is exclusively for Wi-Fi and does not have serial number information.	
	1037	Mac address information is missing for a Windows device.	
	1038	ProvisionIdentifier is duplicated for the Windows device.	
	1039	When there is no device activated by the same ProvisionIdentifier in the general area when attempting Knox Provisioning.	
	1040	User information is not available during Knox provisioning.	
	1041	The KME devices do not match.	

EMM AppWrapper

EMM AppWrapper (hereinafter “AppWrapper”) is an application containing the EMM SDK features that does not change the application codes. Using the AppWrapper in the Admin Portal allows you to reconstruct internal applications through app wrapping, which enables you to add new features without overall knowledge of app platform development.

This chapter explains how to install and run AppWrapper on the IT admin's PC and how to change the icons and the default home screen image of the EMM Agent on the Android app other than using the AppWrapper features provided in the Admin Portal.

This chapter explains the following topics:

- Installing AppWrapper for Android apps
- Running AppWrapper for Android apps
- Change the EMM Agent image resource for Android apps
- Installing AppWrapper for iOS apps
- Running AppWrapper for iOS apps

Prepare the following before using AppWrapper.

- Installation environment for AppWrapper on Android: Windows with JDK 1.8 or later
- Installation environment for AppWrapper on iOS: Mac OS 10.7 or later

Installing AppWrapper for Android apps

Install AppWrapper on the IT admin's PC and convert Android applications. Following the directions from the Samsung SDS support team, download AppWrapper and install it as follows.

To install the donwloaded EMM_AppWrapper.exe file, complete the following steps:

1. Log in with the IT admin's Windows account and click the EMM_AppWrapper.exe file.
2. Select the language for installation and click **OK**.
3. When the InstallShield Wizard starts, click **Next**.
4. Read the EULA for using AppWrapper and click **I accept the terms in the license and agreement** and click **Next**.

5. Click **Install** to start the installation.

6. When the installation of EMM AppWrapper is complete, click **Finish**.

Deleting AppWrapper for Android apps

If you no longer use AppWrapper, delete the program via the Windows Control Panel.

- **Navigate to Windows** > **Control Panel** > **Program** > **Remove Program**.
  Or, select AppWrapper in Change and right-click to click **Remove**.

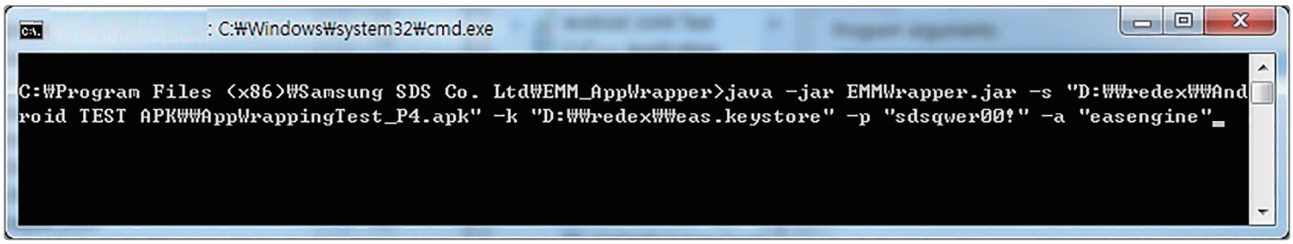
Running AppWrapper for Android apps

IT admin can implement AppWrapper to wrap applications. The applications that are created with the EMM SDK and the applications applied with the security logic that checks the signing key are impossible to wrap. Also, conversions of the downloaded apps from app stores may incur copyright issues.

To implement AppWrapper, complete the following steps:

1. Navigate to the folder installed AppWrapper.

2. In Windows Command Prompt, execute the `EMMWrapper.jar` file and run the commands necessary for AppWrapping.



- The descriptions and examples of parameters for the AppWrapping command are shown as follows: For more information about required items and commands for wrapping, see AppWrapper parameters for Android apps.
  -s: APK file of the internal application to be wrapped.
  -k: Keystore file path of the internal application. Only mandatory for signing.
  -p: Keystore file password. Only mandatory for signing.
  -a: Keystore file alias. Only mandatory for signing.
  -sign false: Without signing

```
java -jar EMMWrapper.jar
-s "D:\\redex\\AppWrappingTest.apk"
-k "D:\\EMM.keystore"
-p "sdspasswd!!"
-a "aliase"
```

AppWrapper parameters for Android apps

Tag	Parameter	Description	Mandatory	Value
srcAPKPath	-s	Absolute path for the original APK file of the internal application that is to be wrapped.	O	
needSiging	-sign	Whether the application must be signed.		• true (default) -sign true: Do not have to input • false
keyStorePath	-k	Absolute keystore file path. • Only mandatory for signing.		
storePass	-p	Keystore file password. • Only mandatory for signing.		
keyPass	-kp	Key Password • Only when the passwords of the keystore and key are different.		
alias	-a	Keystore file alias. • Only mandatory for signing.		
destAPKpath	-dpath	Absolute path for the original APK file of the internal application that is to be wrapped.		/Current folder/ redex.apk
tempSpacePath	-tpath	• Temporary folder for the ReDex process to reduce the app size. • Prepared as a tmp folder.		/Current folder/ tmp

Tag	Parameter	Description	Mandatory	Value
kioskMode	-kmode	• True for Kiosk mode. False for other. • In Kiosk mode add 'android.intent.category.HOME'/'android.intent.category.DEFAULT'.		• true • false (default)
unSignedApkPath	-upath	Absolute path for APK file signing.		/Current folder/redex.apk
storeType	-ktype	• Storetype of keystore file. • Null when not in use.		null
jdkBinPath	-jpath	• Path for the bin folder for jdk that contains the jarsigner.exe file. • If null, the file path for the server environment variable is used.		Server environment variable
proxyDexPath	-dex	Absolute path for the dex file for proxy.		installer installation/current folder/sdsemm.dex
multiDexPath	-mdex	Absolute path for multidex.		installer installation/current folder/multidex.dex
soLibDir	-so	• Absolute path for the folder of .so files. • Even if there are no .so files to add, the path must exist.		installer installation/current folder/libs
frameworkResDir	-res	Absolute path for the resources_framework.arsc file		installer installation/current folder/res
packagePrefix	-pre	• Prefix to be added to the existing package names. • Not used if isRePackage is false.		emmsds

Tag	Parameter	Description	Mandatory	Value
isRePackage	-ispre	True if a prefix is added to the existing package name. If not, false.		• true • false (Default)
isEMMSecureFileMode	-sfile	Whether file I/O are supported via secure file.		• true • false (Default)
isEMMSdkExistCheckMode	-isemm	Whether the API operates to check the existence of the emm sdk.		• true • false (Default)
whiteLabelReplacePath	-w	Absoulte path for the folder of new image resources for EMM Agent icon.		

Change the EMM Agent image resource for Android apps

IT admin can change both the EMM Agent app icon and the home image on the EMM Agent main page to another image resource. For more information about required items and commands for wrapping, see AppWrapper parameters for Android apps.

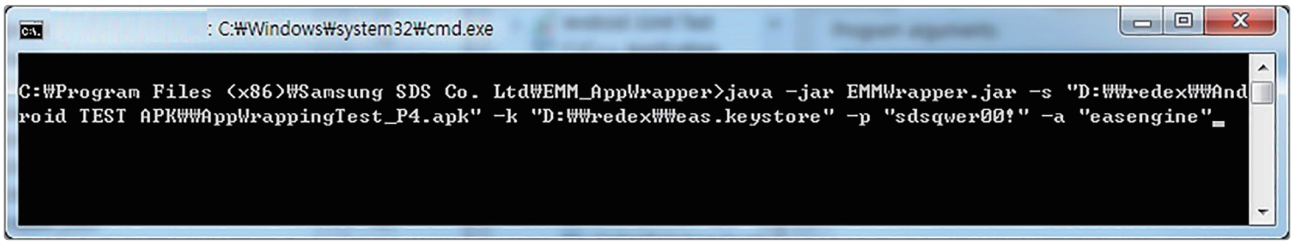
To change the EMM Agent app icon and the home image on the EMM Agent main page, complete the following steps:

1. Prepare your image resources with the name and path below depending on the image resolutions in your local PC.

Item	File name	File path	Resolution
EMM App Icon	ic_sds_launcher.png	res\mipmap-mdpi\	48x48
		res\mipmap-hdpi\	72x72
		res\mipmap-xhdpi\	96x96
		res\mipmap-xxhdpi\	144x144
EMM Home image	img_home.png	res\drawable-xxhdpi\	580x580

2. Navigate to the folder installed AppWrapper.

3. In Windows Command Prompt, execute the `EMMWrapper.jar` file and run the commands necessary for AppWrapping.



4. Check the parameters that are needed for wrapping to change the EMM Agent app icon and the home image on the EMM Agent main page and enter them as below:

   - Parameters

     -s: Absolute path for EMM Agent APK file.

     (ex. `-s "D:\\redex\\AppWrappingTest.apk”`)

     -sign false: Not signing.

     -k: Absolute path for EMM Agent keystore. Only mandatory for signing.

     (ex. `-k "D:\\test.keystore"`)

     -p: The password of keystore. Only mandatory for signing.

     -a: The nickname of keystore. Only mandatory for signing.

     -w: Absolute path for the folder of image resources prepared in Step 1.

     (ex. `-w "D:\\redex\\newImages"`)

   - ex) With signing

```
java -jar EMMWrapper.jar -s
"D:\\redex\\AppWrappingTest.apk" -k "D:\\test.keystore"
-p "passwd" -a "aliase" -w "D:\\redex\\newImages"
```

   - ex) Without signing

```
java -jar EMMWrapper.jar -s
"D:\\redex\\AppWrappingTest.apk" -w
"D:\\redex\\newImages" -sign false
```

Error codes for Android apps

The following table shows error codes that can be displayed when using AppWrapper. See the description and check points below to troubleshoot simple errors that can occur during wrapping.

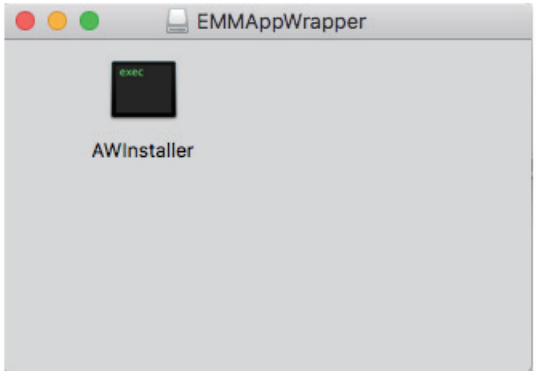
Code	Definition	Description	Check point
0	SUCCESS	Wrapping successful.	
SUCCESS + 1	EMM_SDK_EXIST	EMM SDK is included in the apk file when in EMM check mode.	
SUCCESS + 2	EMM_SDK_NOT_EXIST	EMM SDK is excluded in the apk file when in EMM check mode.	
-1000	SRC_APK_NOT_EXIST	Original apk file to wrap not found in path.	Check whether the original APK file exists.
SRC_APK_NOT_EXIST -1	TMP_DIR_NOT_EXIST	The tmp folder required for a redex process does not exist.	Check whether a tmp folder for the ReDex process exists.
SRC_APK_NOT_EXIST -2	KEYSTORE_FILE_NOT_EXIST	KeyStore file for signing not found in path.	Check whether the keyStore file exists.
SRC_APK_NOT_EXIST -3	DEX_FILE_NOT_EXIST	sdsemm.dex file does not exist in the Wrapper installed folder.	Check whether the sdsemm.dex file exists in the Wrapper installation folder.
SRC_APK_NOT_EXIST -4	SO_LIB_DIR_NOT_EXIST	SO lib folder for INI Push use not found in path.	Check whether the SO file exists under the Wrapper installation folder/libs.
SRC_APK_NOT_EXIST -5	FRAMEWORK_RES_FILE_NOT_EXIST	resource_framework.arsc file not found in path.	Check whether the resources_framework.arsc file exists under Wrapper installation folder/res.
SRC_APK_NOT_EXIST -6	EMM_SDK_ALREADY_INCLUDED	EMM SDK is included in the apk file to wrap.	Wrapping is not possible since the APK file includes EMM SDK.
SRC_APK_NOT_EXIST -7	SIGNING_FAILED	Signing failed for the wrapped apk file.	Check the information of storePass, alias, storeType, and jdkBinPath. • Error log (‘Runtime.getRunTime0.execresult:’ log)
SRC_APK_NOT_EXIST -10	APPWRAPPER_VER_CHECK	The apk file has a record of being wrapped with an identical AppWrapper version.	Wrapping is not possible on this APK file.
-99999	UNKNOWN		

Installing AppWrapper for iOS apps

Install AppWrapper on the IT admin's PC and convert iOS applications. Following the directions from the Samsung SDS support team, download AppWrapper and install it as follows.

To install the donwloaded `EMMAppWrapper.dmg` file, complete the following steps:

1. On the macOS terminal, click the `EMMAppWrapper.dmg` file.
2. Run `EMMAppWrapper.dmg` and click **AWInstaller** in the "EMMAppWrapper" window to install the AppWrapper.



3. Check if the EMM AppWrapper is successfully installed.

Deleting AppWrapper for iOS apps

If you no longer wish to use AppWrapper, enter the following command in the macOS terminal to delete `EMMApprWrapper.app` completely.

- `rm -r / Applications/ EMMApprWrapper.app/`

```
bas1-quebec13-70-30-184-42:~ daehyeogim$
rm -r /Applications/EMMAppWrapper.app/
```

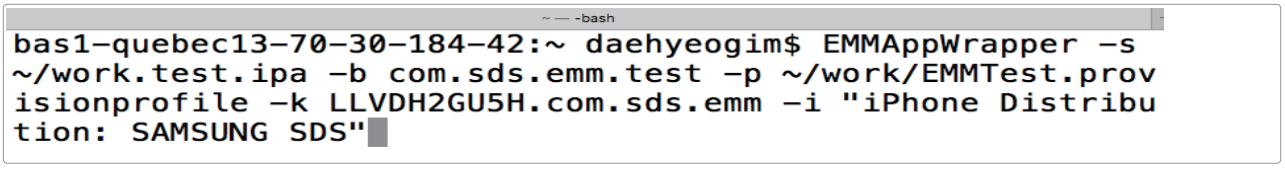
Running AppWrapper for iOS apps

IT admin can implement AppWrapper to wrap applications. The applications that are created with the EMM SDK and applications applied with the security logic that checks the signing key are impossible to wrap. Also, conversions of the downloaded apps from app stores may incur copyright issues.

To implement AppWrapper, complete the following steps:

1. Run the macOS terminal.

2. Enter the necessary commands for AppWrapping in the terminal.



- The descriptions and examples of mandatory parameters for AppWrapping commands are as follows: For more information about the required items and commands for wrapping, see AppWrapper parameters for iOS apps.

  -s: `ipa` file of the internal application for wrapping

  -b: Bundle ID of an iOS app

  -p: Provisioning profile file for an iOS app

  -k: Keychain group

  -i: Name of distribution certificates

```
EMMAppWrapper
-s ~/work/test.ipa
-b com.sds.emm.test
-p ~/work/EMMTEST.provisionprofile
-k LLVDH2GU5H.com.sds.emm
-i “iPhone Distribution:SAMSUNG SDS”
```

AppWrapper parameters for iOS apps

Tag	Parameter	Description	Mandatory	Value
srcAPKPath	-s	Absolute path for the original IPA file of the internal application for wrapping.	O	
bundle_id	-b	App Bundle ID, which must match the app ID registered in the provisioning profile. • E.g. EMM Biz app ID is com.sds.emm.*. All internal applications for wrapping must have an app ID that starts with com.sds.emm.	O	
provisioning_profile	-p	Provisioning profile for app signing. • The prefix value is used for the app ID and keychain sharing.	O	
keychain_group	-k	Keychain group for the keychain sharing feature. • The keychain group must match the group name set in the EMM client. (Default: LLVDH2GU5H.com.sds.emm) • The prefix for the keychain group must match the prefix of the provisioning_profile.	O	
ios_certificate	-i	Certificate used for app signing.		
client_scheme	-c	URL scheme of the EMM Client.		EMMClient
fcrypto	-f	Set whether to use file encryption.		• true • false(Default)
dpath	-d	Absolute path for the original IPA file of the internal application for wrapped.		/Current folder/redex.ipa
tpath	-t	Temporary directory to decompress an internal application.		/Current folder/tmp

Error codes for iOS apps

The following table shows error codes that can be displayed when using AppWrapper. See the description and check points below to troubleshoot simple errors that can occur during wrapping.

Code	Definition	Description	Check point
0	SUCCESS	Wrapping successful.	
-1000	SRC_APK_NOT_EXIST	Original IPA file to wrap not found in path.	Check whether the IPA file exists in the path.
SRC_APK_NOT_EXIST -6	EMM_SDK_ALREADY_INCLUDED	EMM SDK is included in the IPA file to wrap.	Wrapping is not possible since the IPA file includes EMM SDK.
SRC_APK_NOT_EXIST -7	SIGNING_FAILED	Signing failed for the wrapped IPA file.	• Check the expiration period of the certificates and the provisioning profile. • Check whether the certificate matches the certificate on in the provisioning profile. • Check whether the app Bundle ID matches the app ID in the provisioning profile.
SRC_APK_NOT_EXIST -10	APPWRAPPER_VER_CHECK	The IPA file has a record of being wrapped with an identical version of App Wrapper.	Wrapping is not possible for this IPA file.
SRC_APK_NOT_EXIST -11	PROVISIONFILE_NOT_EXIST	Provisioning profile for app signing not found in path.	Check whether the provisioning profile file exists in the entered path.
SRC_APK_NOT_EXIST -12	BUNDLEID_NOT_MATCHED	The entered app bundle ID does not match the app ID of the provisioning profile.	Check whether the entered app Bundle ID matches the app ID in the provisioning profile.
SRC_APK_NOT_EXIST -13	KEYCHAIN_NOT_MATCHED	The entered prefix value of the keychain group does not match the prefix value of the provisioning profile.	Check if the entered prefix for the keychain group matches the prefix of the provisioning profile.
-99999	UNKOWN		

CAC Sign-In

The EMM Admin Portal supports Common Access Card (CAC) Sign-In. CAC is a personal identity card that stores user certificates, and is used by active duty military, US Department of Defense (DoD), and civilian employees.
CAC Sign-In provides two-factor authentication by inserting a card and entering a PIN number. Active Directory Domain Service (AD DS) server environment must be configured on the client's system. You can perform CAC Sign-In to the EMM Admin Portal with a user account registered in AD DS.

Preparing for CAC Sign-In

To do CAC Sign-In, prepare the following:

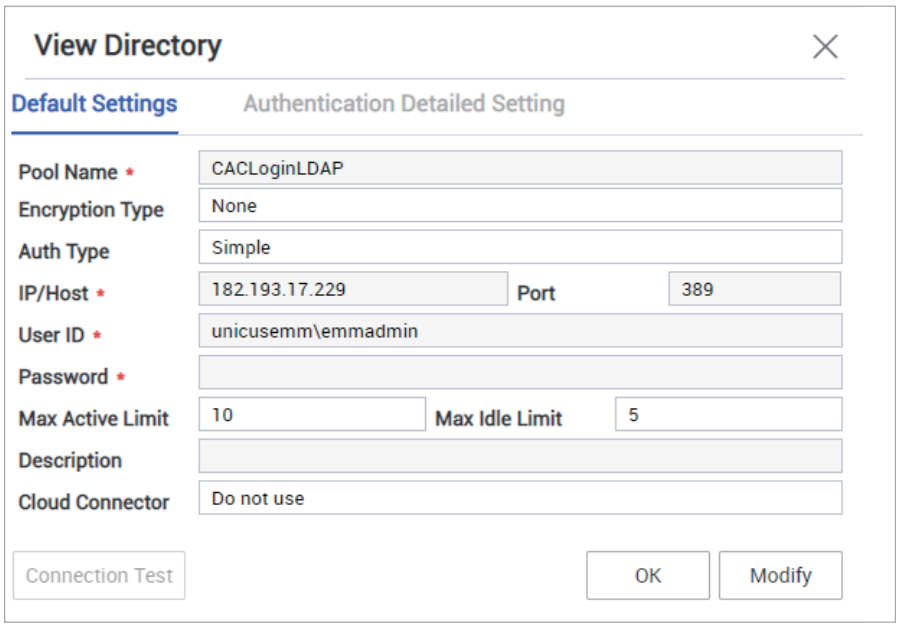
- Preparing the CAC card and PIN number
  : Prepare CAC where the user certificate issued by the client's CA server is stored. A PIN number is also generated when issuing a CAC user certificate to CAC.
- Adding Tomcat server configuration
  : To perform CAC Sign-In in the EMM Admin Portal, the CAC user certificates list on the PC must be able to be checked through the client authentication https communication between the web browser and the Tomcat server. There should be no relay server, such as a web server or a proxy server, between the web browser and the Tomcat server.
  Add <Connector>, which defines the port for client authentication https as follows in the Tomcat configuration file `apache-tomcat\conf\server.xml`.

```
< !-- Define an SSL/TL HTTP1.1 Connector on prot 8443-->
< Connector port = "8443" porotocol="org.apache.coyote.
http11.Http11NioProtocol" max Threads="15" SSLEnabled="true"
scheme="https" secure="ture" clientAuth="true" protocols="TLSv1.2"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA256,........"
truststorFile="C"EMM_DEV/Apache24/bin/localhost-rootca.jks"
truststorePass="..." keystoreFile="C"EMM_DEV/Apache24/bin/
localhost-server.jks" keystorePass="....">
</Connector>
```

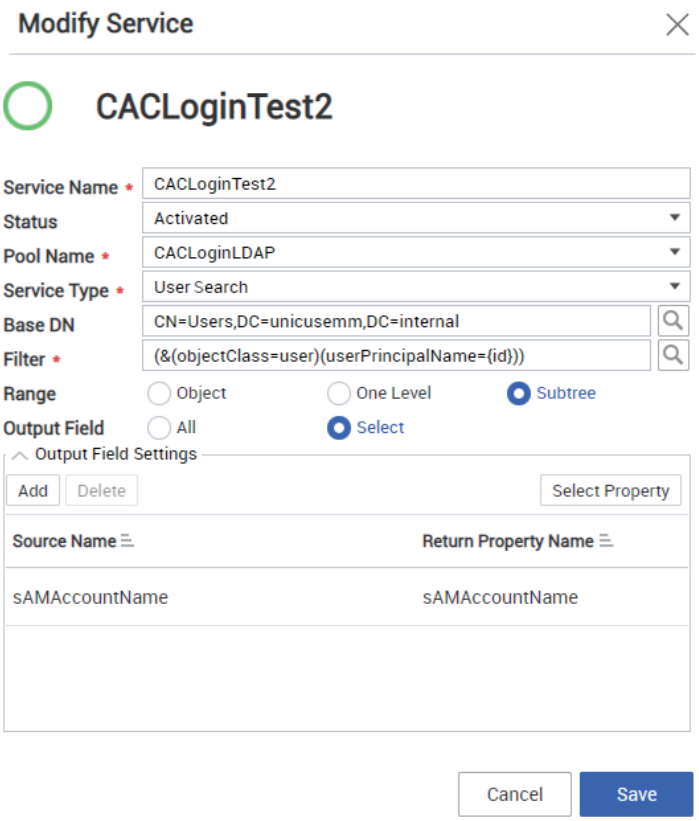
- For client authentication https support, set as follows: `port="8443"`(port value is arbitrary), `SSLEnabled="true", scheme="https" secure="true" clientAuth="true"`.
- Enter `truststoreFile= "..." truststorePass= "..."` for the CAC CA certificate store path and access password respectively so that the CAC user certificate delivered from the web browser can be chain-validated on the Tomcat server. Enter `keystoreFile= "..." keystorePass= "..."` for the Tomcat server certificate store path and access password respectively so that the Tomcat server certificate can be chain-validated on the web browser.
- For the Tomcat TLS version and Cipher settings, see the Appendix of the "Samsung SDS installation Guide".
- Restart the Tomcat server after the settings have been applied.

- Configuring a connector pool for a directory service

  Create a connector pool in **System > Integration > Directory** in the EMM Admin Portal. Enter the server address and port to connect to by LDAP in IP/Host. For more information, see Adding a directory server.



- Creating a directory service that searches for user information from AD DS by User Principal Name (UPN)
  Navigate to **System > Connector > Directory** in the EMM Admin Portal to add a directory service. For more information, see Adding a directory connector.



  - Select a connector pool for the directory service form the Pool name, and select **User Search** for **Service Type**.
  - In **Base DN**, select the search starting location of the directory server.
  - **Filter** must be entered as `(&(objectClass=user)(userPrincipalName={id}))`. When entering it, do not change the keyword "id" to another name.
  - **Output Field** shows the results searched through the filter on the Directory server.
    Select the following properties as the output field as needed. You can set Output Field to "All" to include all the properties below.
    - **sAMAccountName**: This is a required property value and must be included always. This value is used as the admin account ID when signing in to the Admin Portal.
    - **accountExpires**: This is an optional property value. When this is selected, it checks whether the AD DS user account is expired. If expired, then it wouldn't try to sign in to the Admin Portal, with an error message exposed.
    - **userAccountControl**: This is an optional property value. When this is selected, it checks whether the AD DS user account is a lockout status or disabled. If a lockout status or disabled, then it wouldn't try to sign in to the Admin Portal, with an error message exposed.

- Registering an administrator on the EMM Admin Portal
  : Add as an administrator in **Setting > Admin Console > Administrator**. For more information, see Adding an administrator. You must register the "User Logon Name" value among the user attributes that are registered in AD DS as an Admin to sign in to the Admin Portal.
- Configuring the environments for CAC Sign-In on the EMM Admin Portal
  : Configure CAC Sign-In in the **Setting > Server > Configuration**. For more information, see Setting the CAC Sign-In.

Glossary

Use the following glossary to understand terms and abbreviations used in this manual.

A

No.	Terminology	Definition
1	Activate EMM Agent	Activating the EMM Agent is used to activate the EMM Agent on user devices. Once activated, the EMM Server will communicate with, control, and monitor user devices.
2	AD (Active Directory)	Active Directory is a directory service implementation that provides functions like authentication and authorization. It supports the Lightweight Directory Access Protocol (LDAP). For more information, see LDAP(lightweight directory access protocol).
3	AD/LDAP Sync Services	The AD/LDAP sync services allow you to sync the information of a company's existing users, groups, and organizations with EMM. For more information, see LDAP(lightweight directory access protocol).
4	AES (Advanced Encryption Standard Algorithm)	Advanced Encryption Standard (AES) is a symmetric-key algorithm standardized in the United States. It encrypts the electronic data transmitted to user devices through a VPN tunnel.
5	AIDL (Android Interface Definition Language)	AIDL is an IDL (a specification language for describing the interface of a software component) for Google Android mobile device platforms.
6	Air Command	Air command is one of Samsung’s mobile device functions. When you place the S Pen near the device screen and press the S Pen button, the Air command menu will open.
7	Air View	Air view is one of Samsung’s mobile device functions. You can preview emails, messages, or photos by placing the S Pen on the device screen.
8	Android Beam	Android Beam is used to transfer data, such as web bookmarks, contact information, YouTube videos, and other data onto another device via NFC. For more information, see Near Field Communication (NFC).
9	Android Enterprise	An enterprise device management mode for employees using mobile devices, supported on Android 5.0 Lollipop and later. With Android Enterprise, organizations can use features such as device mode settings, work profile creation, and app deployment.
10	Android Legacy	Android Legacy is a devices management mode supported on Android 2.2 and later, do not support work profiles.
11	Anti-Malware	Anti-Malware is a vaccine software to detect and remove any virus or malware on mobile devices.

No.	Terminology	Definition
12	AP (Access Point)	AP is a system that wirelessly transmits network signals. Once connected to AP, it is allowed to use the Internet within the transmission range.
13	APK (Android Application Package)	APK is a file format used for deploying and installing application software and middleware in Google Android.
14	App Wrapper	EMM AppWrapper is to wrap applications into applications with the EMM SDK feature, without modifying the application code.
15	APNs (Apple Push Notification service)	Apple Push Notification service (APNs) helps facilitate sending commands to iOS devices through Apple's push notifications. For more information, see iOS.
16	API (Application Programming Interface)	Application Programming Interface (API) is a language or message used for communication between operating systems and applications. It provides an interface for applications to interact with hardware components, operating systems, or web-based services.
17	Area	Area is a space within the device that administrators can have a control over. Administrators can install applications or configure device settings for the selected area. The area types differ based on the device platform. For more information, see General area, Knox Workspace area, Work area, and Personal area.
18	Attestation	Attestation is a process that verifies the integrity of a device. It can evaluate measurements derived from the kernel, kernel modules, kernel data structures, and Android data structures to ensure that the device is operating properly in a trusted environment.
19	Audit	Audit is to check events in the EMM server, applied policies, compromising and compliance violations, etc., and it records monitoring devices in real time.
20	Authentication	Authentication is a process to recognize the user by a PIN, password, pattern, finger print, or smart card.

B

No.	Terminology	Definition
1	Base DN	Base DN is a starting point of identification for searches in the sync service. You can set the default value or users can change it. For more information, see Sync services.
2	Blacklist	Blacklist is to block execution or registration. You can block applications, IP addresses, Wi-Fi SSID APs, domain names, etc.
3	Bulk Enrollment	Bulk enrollment is to enroll devices in bulk by using a CSV file or scanning their IMEI numbers through NFC.

No.	Terminology	Definition
4	BYOD (Bring Your Own Device)	Bring Your Own Device (BYOD) refers to personal devices used for business, such as smartphones, laptops, and tablet PCs.

D

No.	Terminology	Definition
1	Deactivate EMM Agent	Deactivating the EMM Agent is used to deactivate the EMM Agent on user devices. EMM will become unavailable. To reactivate a deactivated device, see Activate EMM Agent.
2	Device Command	A device command is a command that is sent to a device to manage it.
3	DEP (Device Enrollment Program)	Device Enrollment Program (DEP) is an Apple service for activating corporate-owned iOS devices quickly and easily. You can activate iOS devices in EMM through DEP.
4	Device-Wide VPN	Device-Wide VPN allows Android Legacy devices to use both the general area and the Knox Workspace area through a VPN.
5	DeX	DeX is an interface to use mobile devices as desktops. Samsung Dex enlarges mobile device related functions. When you connect a keyboard, mouse, etc. to the Dex docking station, the device operates like a desktop. Applications used in the Dex mode can be controlled by setting application execution blacklist.
6	Direct Boot	Direct Boot mode runs when the device has been powered on but the user has not unlocked the device. Only applications that recognize this mode can be accessed.
7	DO (Device Owner)	Device Owner (or Fully Managed devices) is one of the Android Enterprise devices. It is a mode to control corporate-owned devices.
8	DRM (Digital Rights Management)	DRM refers to the technologies and services designed to prevent unauthorized use of digital content to protect the rights and interests of content providers. It also provides techniques to protect from illegal duplication and modification.
9	Dual DAR	Dual DAR is a solution to encrypt data through two layers of encryption on Android Legacy or Android Enterprise devices. EMM fully protects data in Dual DAR Workspace with dual encryption.

E

No.	Terminology	Definition
1	E-FOTA (Enterprise Firmware-Over-The-Air)	Knox E-FOTA (Enterprise Firmware-Over-The-Air) is a corporate solution to control the firmware version of Samsung mobile devices. IT admins can selectively update the OS version compatible with the company's internal applications on user devices.
2	EMM (Enterprise Mobility Management)	Enterprise Mobility Management (EMM) is a comprehensive solution for mobile device management to enhance the security of corporate data. It helps to manage users and device data safely by setting device policies and deploying business applications.
3	EMM Agentl	The EMM Agent is a set of applications installed on mobile devices to control and monitor them.
4	EMM Server	The EMM server provides the EMM services, and offers functions to manage and control enterprise mobile devices.
5	Exchange ActiveSync	Exchange ActiveSync is a synchronization protocol that enables mobile device users to access email, calendar, contacts, and tasks from their organization's Exchange server. For more information, see Sync services.

F

No.	Terminology	Definition
1	Factory reset	Factory reset is used to initialize a device.
2	Fail Level	Information provided in the audit event list. Refers to a failed audit event severity.
3	FBE (File Based Encryption)	File Based Encryption (FBE) is to encrypt files independently by using AES-256-XTS and a different encryption key derived from the primary key.
4	FCM (Firebase Cloud Messaging)	Firebase Cloud Messaging (FCM) is a free push notification service by Google. You can send messages for each application installed on user devices.
5	FIPS (Federal Information Processing Standards)	FIPS stands for “Federal Information Processing Standards.” It encrypts all data using the FIPS 140-2 authentication module between the server and the EMM client.
6	FIPS 140-2	FIPS 140-2 is one of the Federal Information Processing Standards. It is required to protect encryption module for the confidentiality and integrity of the information in the security system. This standard specifies the security requirements of the encryption module.
7	Firewall	Firewall is a security system that blocks illegal intrusion through the Internet to prevent security problems, such as information leakage, and system failure.

No.	Terminology	Definition
8	Full Tunneling	Full tunneling is a method that routes all outgoing traffic from the VPN client through a VPN tunnel and through the VPN server.
9	Fully Managed	Fully Managed is an Android Enterprise device type. It is also called Device Owner (DO) and a mode to control corporate-owned devices.
10	Fully Managed with Work Profile	Fully Managed with Work Profile is an Android Enterprise device type. It is a combination of Fully Managed and Work Profile and a mode to control corporate-owned devices. EMM can control work apps and data in the Work Profile area and the personal area but not the applications in the personal area.

G

No.	Terminology	Definition
1	Gateway	Gateway is a network node to access multiple computers or LAN (local area network) to a public communication network.
2	GDPR (General Data Protection Regulation)	General Data Protection Regulation (GDPR) is a regulation implemented May 25, 2018 on data protection and privacy in the European Union. All enterprises, organizations, e-commerce that handle the personal information of EU residents must observe it.
3	General area	General area is an area that administrators can control through EMM on Android Legacy devices. Administrators can remotely apply device commands or policies in the general area.
4	GPS (Global Positioning System)	The Global Positioning System is a space-based satellite navigation system that provides location and time information regardless of weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
5	Group	Group is a unit to apply policies and settings on devices or to manage application authorities on EMM.

H

No.	Terminology	Definition
1	HTML5	HTML5 is the core markup language of the World Wide Web and offers an alternative to the older versions, HTML4 and XHTML 1.0. HTML5 aims to reduce the demand for plugin-rich Internet apps, such as Adobe Flash, Microsoft Silverlight, and Sun JavaFX.

I

No.	Terminology	Definition
1	IMEI (International Mobile Equipment Identity)	International Mobile Equipment Identity (IMEI) is the numerical identifier for every mobile device. It is used by service providers to identify valid devices.
2	IPSec (Internet Protocol Security)	IPsec is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

J

No.	Terminology	Definition
1	JAR (Java Archiver)	JAR is a format that aggregates multiple Java class files into a single file for more efficient distribution. JAR can be easily managed in a local device and can directly use the files that are downloaded remotely through a Hypertext Transfer Protocol (HTTP) while a Java program is running.
2	JDK (Java Development Kit)	The JDK is a development tool designed to help developers make Java applets and other apps more easily. The JDK includes a Java app Interface (API) that links between various operating systems and apps, class libraries, Java Virtual Machine, and so on.
3	JRE (Java Runtime Environment)	JRE is an environment for running the Java-based programs on a computer.
4	JSON/XML (JavaScript Object Notation/ Extensible Markup Language)	JSON/XML stands for “JavaScript Object Notation/Extensible Markup Language.” Both JSON and XML are standardized formats used to transfer structured documents on the web.

K

No.	Terminology	Definition
1	Keepalive	Keepalive is a signal to maintain the connection between the EMM server and a device. It regularly checks the connection status between a device and the EMM server. If a device is lost or disconnected from the server, you can take measure for device security.
2	Kiosk (Software)	Kiosk is a device or computer that has a touch screen. In EMM, it indicates a software that limits access to the device system.
3	Kiosk Applications	Kiosk applications are applications used in Kiosk mode. If Kiosk applications are installed on a device through a profile or a device command, the applications can only be opened in Kiosk mode. EMM provides the Kiosk wizard to help to utilize Kiosk applications.
4	Kiosk Browser	Kiosk Browser is a browser application that can only access certain URLs. Devices that the Kiosk Browser policy is applied become Kiosk mode and can be accessed via a company's website or a certain URL. Kiosk Browser is provided by EMM.
5	Kiosk Mode	Kiosk mode is a mode that limits access to the device system, so that the user cannot close Kiosk applications, Kiosk Browser, etc. In this mode, the user cannot use other device features or change the settings. Kiosk was originally used for information supply, but now, it is also used in industries, such as service, sales, and healthcare.
6	KME (Knox Mobile Enrollment)	Knox Mobile Enrollment (KME) is a Samsung service to bulk register multiple devices in EMM.
7	Knox Workspace Area	Knox Workspace area is an independent virtual container to protect work apps and data on Android Legacy devices. Administrators can remotely apply device commands or policies in the Know Workspace area.

L

No.	Terminology	Definition
1	LDAP (Lightweight Directory Access Protocol)	Lightweight Directory Access Protocol (LDAP) is a protocol to search for users, organizations, domains, server information, and so on in the directory server. The company saves information, such as users, systems, networks, services, and applications, based on the directory server as the tree structure and view or manage the information.
2	Level	Level indicates the degree of the occurrence of an audit event. You can select the audit event level among the six log levels and the audit event result among success or failure. When an audit event occurs, the system records the log according to the level and result.

No.	Terminology	Definition
3	LKM (Loadable Kernel Module)	Loadable Kernel Module (LKM) is a code to dynamically add a new feature to the device kernel at run time but not at build time. The driver for integrated hardware components is included. TIMA verifies if there is no damage while the module is being loaded.
4	Log4j	Log4j is a Java-based logging utility. It is also widely used as a debugging tool. The latest version of Log4j defines the six log levels. Log4j can designate the levels for each target, for each package in Java, in the configuration file and can record the logs above the designated level.

M

No.	Terminology	Definition
1	Master Data	Master data is the information that defines the criteria of data related systems necessary for the EMM Admin Portal operation. It includes the user's location, security level, device status, and so on.
2	Mobile Admin	Mobile admins of EMM are the administrators of the Admin Portal in the mobile environment. They manage device command, device usage, etc. in the mobile environment.
3	MAM (Mobile Application Management)	Mobile Application Management (MAM) is a system to manage only work apps and related data. Administrators can remotely install or update applications.
4	MBI (Mobile Business Integrator)	The MBI refers to the interface that supports the customization of protocols or business logics that are not supported by existing connectors.
5	MBS (Mobile Business Service)	MBS is a development method that standardizes the modules an enterprise uses, such as approval, email, and scheduling modules, and exposes only the externally linked interface, through which it recycles the modules in device apps. Changes in the business logic of the MBS do not affect the existing device apps. The SEMP currently uses MBS for groupware connectors.
6	MCM (Mobile Contents Management)	A content management strategy that is capable of storing and delivering content and services to mobile devices.
7	MDM (Mobile Device Management)	Mobile Device Management (MDM) is a software that allows you to remotely deploy applications of an organization or group to personal-owned or corporate-owned devices. Recently, it is evolved to EMM.
8	MDM (Mobile Device Management Profile)	Through MDM profiles, you can set in advance policies and settings, such as policies, Wi-Fi, and VPN, to control devices more easily.

No.	Terminology	Definition
9	MFA (Multifactor Authentication)	Multifactor Authentication (MFA) proves a user's identity using various methods including password, biometric data, or RSA tokens.
10	Mobile Web App	The mobile web app is an application type that combines the advantage of the mobile web and a native app. It is displayed through a browser, so it can be accessed via any device platform.
11	Mobile Web	The mobile web refers to the website that displays the functions running on the desktop browser but fits the UI size of a mobile device. It is displayed through a browser, so it can be accessed in any device platform.

N

No.	Terminology	Definition
1	Native Application	Native application is a type of applications. It is developed in a language optimized for mobile devices so has high performance. However, as it is developed using the API of the device platform, its range of use is limited.
2	NFC (Near Field Communication)	Near-field communication (NFC) is a technology of short-range contactless communication. NFC allows smartphones and other devices to establish radio communication with each other by touching them together or bringing them into close proximity, typically a distance of 10 cm (3.9 in) or less.
3	NTP (Network Time protocol)	Network Time Protocol (NTP) is a protocol used to synchronize clock information over a connected network. The clock information from the NTP server is synchronized within one thousandth of a second and provided to devices.

O

No.	Terminology	Definition
1	OCSP (Online Certificate Status Protocol)	OCSP is an Internet protocol that uses X.509 to determine the revocation status of a digital signature certificate. It can replace the certificate revocation list (CRL) and is used for verifying the revocation list of certificates made by public key information.
2	On-Demand VPN	It is a feature to allow access through VPN only when the assigned application is running. It is used when to set per app VPN.
3	OTA (Over the Air)	OTA refers to the general methods of installing and changing mobile apps or firmware in a wireless network environment. OTA is provided via an HTTP-based URL.

No.	Terminology	Definition
4	OTG (On-The-Go)	It is an abbreviation for USB On-The-Go and also called USB OTG or OTG. It is a USB standard that enables communication by connecting cables between digital devices, such as digital audio devices, digital cameras, mouses, keyboards, and smartphones, without computer intervention.
5	OTKEY (One Time Key)	An OTKey is a symmetric key used when encrypting/decrypting a data message and is generated for each message.
6	OTP (One Time Password)	OTP is a one-time password.
7	Organization	Organization is a unit to apply a policy to devices or manage applications and users in the Admin Portal. It is composed of a vertical relationship like a company department, and administrators can distribute policies, applications, and contents to user devices by organization.

P

No.	Terminology	Definition
1	Per-app VPN	Per-app VPN is a feature to set whether to access through VPN or not by application.
2	Personal Area	Personal area is an area that administrators cannot remotely control on personal Android Enterprise devices (Bring-Your-Own-Device).
3	PO (Profile Owner)	Profile Owner (PO) is one of the Android Enterprise devices. It is a mode to control personal devices (Bring-Your-Own-Device). On devices of the Work Profile type or Fully Managed Device with Work Profile type, EMM can manage device settings in virtual areas.
4	Podcast	A podcast is a service that provides audio, video, digital radio, and PDF files to subscribers and can be downloaded through web syndication or streamed online to a computer or mobile device.
5	Private Key	Profile Owner (PO) is one of the Android Enterprise devices. It is a mode to control personal devices (bring-your-own-device). On devices of the Work Profile type or Fully Managed Device with Work Profile type, EMM can manage device settings in virtual areas.
6	Profile	Profile defines a company policy to remotely control user devices. Profiles allow you to control device functions and install the Wi-Fi, VPN, and Exchange settings of your company on user devices.
7	Protocol	Protocol is an agreement about communication rules and methods for facilitating information exchange between the server and the devices.
8	Provising	It is the process of activating the device in the EMM server through the authentication of the device in which the EMM is installed.

No.	Terminology	Definition
9	Public Key Certificate	In cryptography, a public key certificate is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct.
10	PKC (Public Key Cryptography)	Public key cryptography (PKC) consists of a pair of keys: a private key and a public key. The two keys are cryptographically related. After creating the two keys, the owner keeps the private key safe and opens the public key to others. The information encrypted with a private key can be decrypted by the paired public key. The information encrypted with a public key can be decrypted by the paired private key. Asymmetric key encryption types are RSA, ECC, and so on.
11	PKI (Public Key Infrastructure)	A public key infrastructure (PKI) is an algorithm pattern used to decrypt the message encrypted by the private key. It is also used to encrypt the message that can be decrypted only by the paired private key. Users will broadcast their public key to anyone they need to exchange encrypted messages with. For more information, see PKC (Public key Cryptography).
12	Push	Push provides information the users want automatically from the server. It is an automatic technology for users to receive certain information without making a request every time.

R

No.	Terminology	Definition
1	RS Viewer (Remote Support Viewer)	RS Viewer is a program used when Android device users request remote support. The administrator can share the user's device screen through the Remote Support Viewer (RS Viewer); and remotely perform tasks on a given screen. And the administrators can also support multiple users remotely at the same time.
2	Router	A router is a device that reads the receiver's address in the sending information (the packet), finds the best communication route, and sends the data to the receiver when exchanging information on LAN. A router is necessary for the network configuration. Routers select the ideal network path to send packets through. This process is called “routing.” Generally, routers have multiple inputs and outputs and are used when exchange functions are required.
3	Routing	Routing is a software function of a router. This function reads the address information in a packet and sorts the data by destination. Routing is supported by most routers and is implemented using the software installed on the router. When exchanged across a network, data is formatted in packets to which various information data are added, such as the sender information, destination, and receipt status in the beginning and end of the data.

S

No.	Terminology	Definition
1	SA (Service Agent)	Service Agent (SA) is an agent installed in the application server to send and receive messages. When you use the Samsung SDS Push service, SA sends messages from the application server (integrated system, Samsung SDS EMM server, or other mobile services) to devices.
2	Samsung SDK	Samsung SDK is a Java API library that enables developers to create the enterprise solution (EMM) that manage Samsung Android devices.
3	SLM (Samsung License Management System)	Samsung License Management (SLM) system is a web server that manages the entire lifecycle of EMM licenses, including KPE license's ordering, license generation, activation tracking, validation, and quantity checking.
4	SCEP (Simple Certificate Enrollment Protocol)	SCEP is one of the most common certificate management protocols.
5	Scheduler Job Class	The scheduler job class is the execution class for performing scheduled tasks.
6	Schema	This term refers to the logical structure of a database that describes the organization, content, and the logical and physical characteristics of the data stored in the database. Generally, the database uses many layers of schemata to maintain data independence.
7	SDK (Software Development Kit)	Software Development Kit (SDK) is a set of API libraries, sample applications, documents, and tools used when developers program applications.
8	Service Broker	Service broker monitors data transmission between devices and the server (database and the EMM server) when using the database connector. It allows to encrypt and transmit the communication of devices and the server.
9	Service Channel	A service channel refers to the internal service information assigned to each device to access the internal server from the VPN client via the VPN communication.
10	Short Message Service (SMS)	SMS is a text messaging service that allows wireless devices to exchange short texts with each other.

No.	Terminology	Definition
11	SOAP (Simple Object Access Protocol)	SOAP is a protocol that exchanges XML-based messages on computer networks using HTTP, HTTPS, and SMTP. SOAP provides a foundation for sending basic messages across a web service. SOAP relies on a number of message patterns, but the most common pattern is the Remote Procedure Call (RPC) that a network node (client) sends a request message to another node (server), and the server immediately responds to the message. SOAP has adopted the envelope, header, body structure, and transport method, as well as the interaction neutrality concept used in XML-RPC and WDDX. SOAP is based on an XML design pattern which combines a header and a body. The header is an optional element that contains meta data, such as repetition, security, and transaction data. The body includes the relevant message data.
12	Secure Sockets Layer (SSL)	Secure Sockets Layer (SSL) is a protocol that maintains security of the Internet by encrypting personal information (data) between applications to prevent data hacking or compromising. It uses the network layer encryption and functions in HTTP, NTTP, and FTP. Basically, SSL guarantees authentication, encryption, and integrity. Recently, it has been replaced to Transport Layer Security (TLS).
13	SSO (Single Sign On)	Single Sign On (SSO) is an authentication process that allows you to enter one user ID and password for the access to multiple applications or systems. AD SSO is supported to access EMM.
14	SQL (Structured Query Language)	SQL is a programming language designed to access a database. SQL is a type of database query language that includes a data definition language (DDL) and a data manipulation language (DML). Originally, only IBM's relational database systems used SQL, but it became popular for other database systems because of its universality.
15	Sync Services	Administrators can connect directory services with EMM in order to sync user, organization, and group information. Registered sync services can be operated automatically.
16	System Port	The system port is the service channel information that is set by default when installing the VPN for the service broker and full tunneling.
17	Symmetric-key Algorithm	Symmetric-key algorithm refers to the algorithm that uses the same cryptographic key for encryption and decryption. The same cryptographic key is shared and the types of symmetric-key encryption are AES and DES.

T

No.	Terminology	Definition
1	TCP (Transmission Control Protocol)	TCP/IP are protocols to transmit the data of devices and the EMM server in packets. Data is divided in packets and delivered, and then it is reassembled at the destination. Data order and delivery is ensured.

No.	Terminology	Definition
2	Tethering	Tethering is a feature to use devices as modems. With tethering on devices, other devices, tablet, or laptops can access the wireless Internet through Wi-Fi, Bluetooth, or USB.
3	Three-Tier	Three-Tier refers to user interface, business logic, and database. Each tier can be developed simultaneously by separate development teams and can be updated or extended without affecting the other tiers as needed.
4	TIMA (TrustZone-based Integrity Measurement Architecture)	TrustZone-based Integrity Measurement Architecture (TIMA) is an architecture to measure integrity based on TrustZone. It is a software that guarantees and monitors continuously the integrity of the Linux kernel.
5	Tizen	Tizen is the Linux kernel-based open source operating system used in Samsung wearables, TVs, and home appliances.
6	TLS (Transport Layer Security)	Transport Layer Security (TLS) is a protocol that protects personal information between applications communicating on the Internet by encrypting data to prevent hacking or compromising. It can be replaced to Secure Sockets Layer (SSL).
7	TLS (Transport Layer Security) VPN	TLS VPN authenticates users using the TLS protocol and delivers encrypted data when using VPN.
8	Token	A token is a unit to separate a string. It is used when compilers and assemblers analyze words. An access token is used to authorize users to access specific features or data in systems or software. For example, the web service provider creates an access token using the user's ID, password, or application information and sends it to the user. The user can use the access token to access the web service. This method prevents personal information leakage and allows to provide the web service safely.
9	TrustZone	TrustZone is a technology used to store process and data that need to be secured in a hardware-separated CPU and memory.
10	TTE (Time To Expire)	TTE refers to the term of validity for messages.
11	Tunnel	Tunnel is connection secured by data encryption between devices and a network resource.
12	Two-Factor Authentication	Two-factor authentication is a method used to verify a user's identification using two different methods including password, biometric data, or RSA token.

U

No.	Terminology	Definition
1	UI	UI stands for “User Interface.”
2	UI Component	A UI component, also known as a widget, is a Graphical User Interface (GUI) element that displays information in various ways. The typical examples include buttons, check boxes, text boxes, sliders, and selected fields.
3	UI Framework	UI Framework is a newly developed framework for hybrid app development. It uses HTML5, JavaScript, and CSS. The UI Framework is based on jQuery Mobile and provides an environment for developing various mobile web apps, such as mobile widgets, page history management, and touch event management.
4	UEM (Unified Endpoint Management)	Unified Endpoint Management (UEM) is a software that comprehensively manages wearables, IoT devices, other digital devices, mobile phones, and tablets in Enterprise Mobility Management (EMM). UEM allows IT departments to remotely provision, control, and protect everything from smartphones, tablets, laptops, desktops, and even IoT devices.
5	UMC (Universal MDM Client)	Universal MDM Client (UCM) is pre-installed on Samsung devices and acts as a substitute for proprietary Mobile Device Management (MDM) client software.
6	UMP (Unified Messaging Platform)	UMP is a platform that supports reliable and safe message transmission between the app server and the client. It provides differentiated transmission quality, depending on the message properties, and it supports the two-way push function between the servers and devices. UMP is run on every environment including the on-premise and cloud type.
7	USIM (Universal Subscriber Identity Module)	A USIM is a smart card that is inserted into a terminal of the Wideband Code Division Multiple Access (WCDMA). It refers to a technique that implements various functions, such as user authentication, billing, global roaming, and e-commerce, in a single card.

V

No.	Terminology	Definition
1	VPN (Virtual Private Network)	Virtual Private Network (VPN) is a mechanism to create secure connection between devices and network. Secure connection uses encryption to protect enterprise or personal data.
2	VPN Chaning	VPN Chaning is the ability to transmit data with double encryption. When using more than one VPN service, data secured with the first VPN can be secured with the second VPN.
3	VPN Client	A VPN client is an application that the VPN vendor provides. It can be installed on user devices,

No.	Terminology	Definition
4	Volume Purchase Program (VPP)	Apple's Volume Purchase Program is a service that purchases and deploys public applications that are used in an organization or company, and then efficiently deploy them to a large number of iOS devices at once. After 2020, VPP has been integrated into Apple Business Manager. In Apple Business Manager, you can make bulk purchases at the same price or make applications downloadable in certain organizations.
5	VPP Applications	Applications distributed through Apple's Volume Purchase Program (VPP).

W

No.	Terminology	Definition
1	WAP (Wireless Access Point)	Wireless Access Point (WAP) is a networking device that allows wireless devices to connect to a wired network. Adding WAP to the existing wired network is helpful when accepting other devices that support only wireless connections.
2	WAP (Wireless App Protocol)	Wireless App Protocol (WAP) is an architecture for mobile phone that can connect to any wireless networks, such as GSM, TDMA, and CDMA. A WAP browser is a web browser for mobile devices, such as mobile phones, that use the protocol.
3	WAS (Web App Server)	A WAS provides an environment for the execution of web apps.
4	Web Clip	A web clip is an icon installed on an iOS device. It contains a website URL that directs users to a website via Safari when it is tapped.
5	Whitelist	Whitelist is to permit execution or registration. You can enroll applications, IP addresses, Wi-Fi SSID APs, domain names, etc.
6	Work Profile	Work Profile is an Android Enterprise device type. It is also called Profile Owner (PO) and a mode to control bring-your-own devices.
7	Work Profile Area	The Work Profile area is an area to manage work apps and data on Android Enterprise devices. If a device is activated as the Work Profile type, the device is divided into the work area and personal area and separately used.
8	Work Profile on company-owned	Work Profile on company-owned is an Android Enterprise device type. It is a combination of Fully Managed and Work Profile and a mode to control corporate-owned devices. EMM can control work apps and data in the Work Profile area and the personal area but not the applications in the personal area. From Android 11, Fully Managed with Work Profile has been replaced to Work Profile on company-owned and personal information protection has been enhanced.

No.	Terminology	Definition
9	WSDL (Web Services Description Language)	WSDL, which is presented in XML format, refers to the web service description language and the file that includes the definition. The WSDL is used to describe the service details, such as service locations, service message format, protocol, and so on.

X

No.	Terminology	Definition
1	X.509 Certificate	An X.509 certificate is a digital certificate that is based on the public key infrastructure (PKI) and contains the information defined by the X.509 standard. It uses the cryptographic key to encrypt or decrypt data and is used to manage identity and security in Internet communications and computer networking.

Realize your vision SAMSUNG SDS

www.samsungsds.com