SAMSUNG
Knox Manage

User's Guide

Solution version 19.9

Published: September 2019

Manual version 19.9.1

Preface

Users of this guide

This guide is for users of SAMSUNG Knox Manage (hereinafter "Knox Manage") . It covers Application store and instructions for Knox Manage. Please read this guide before using Knox Manage, and keep it handy for further use.

Summary of this guide

This guide consists of the following chapters:

- **Chapter 1. Outline of SAMSUNG Knox Manage**
  Outlines SAMSUNG Knox Manage and this User Guide.
- **Chapter 2. Installing**
  Explains SAMSUNG Knox Manage installation and system requirements.
- **Chapter 3. Getting started**
  Explains how to log-in and set up the Knox Manage on the device and home screen layout.
- **Chapter 4. Using applications**
  Explains how to use the Application Store provided in Knox Manage application.
- **Chapter 5. Remote Support**
  Explains how to install and start the tool for remote support.
- **Appendix A. Resolving issues**
  Explains how to resolve issues those are the device lock and forgotten device password.

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 additional information such as tips, recommendations, exceptions, and limitations.

Note: 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
2.0	2.0a	October 2017	Original issue.
2.0.1	2.0.1a	November 2017	Added Knox container notification.
2.0.2	2.0.2a	February 2018	Added viewing all policies configured for the device.
2.0.2	2.0.2b	March 2018	Added constraints when reinstalling Knox Manage on Windows 10.
2.1	2.1a	April 2018	- Added a configuration auto-installation. - Added a method for enrolling DEP devices. - Updated the Remote Support application.
2.1.1	2.1.1a	May 2018	- Updated the Knox Manage app icon. - The Service Desk provides Remote Support App download link.
2.1.2	2.1.2a	June 2018	- Improved a configuration auto-installation with Wi-Fi and Bookmark settings. - Added sending messages to a locked device screen.
2.1.3	2.1.3a	August 2018	Added installing the VPP applications.
2.1.4	2.1.4a	October 2018	Added the Contents menu.
2.1.5	2.1.5a	November 2018	- Added support for the Android Enterprise service. - Added a feature to run Remote Support automatically
2.1.7	2.1.7a	January 2019	Added Knox container password reset function.
2.2.0	2.2.0a	March 2019	Added support for Android Enterprise feature.
19.4	19.4.1	April 2019	- Improved security with Lock Task mode - Added option for App review feature
19.5	19.5.1	May 2019	Updated Android Enterprise activation type naming.
19.9	19.9.1	September 2019	- Admin Portal UX renovation(App, Profile, AE manage type) - Added support for ZTE

Solution version	Manual version	Manual revised date	Revised details

Table of Contents

1 Outline of SAMSUNG Knox Manage

SAMSUNG Knox Manage (hereinafter "Knox Manage") is the enterprise EMM (Enterprise Mobility Management) solution that provides strong security in Corporate-Owned Personally Enabled (COPE) and Bring Your Own Device (BYOD) environments. End Users are able to separate their personal and business data on the same mobile device using Knox Manage. This ensures that they gain the convenience of using their own device while maintaining the highest levels of security.

Key features of Knox Manage

With Knox Manage, companies and end users can adopt policies, distribute and manage applications, and manage the internal security of applications while copying and pasting text and deleting information.

In addition, they can manage device policies by sending them to the Knox Manage sever using via the 3rd party push service. If necessary, users can receive technical support for inquiries by sharing the device screen.

Knox Manage provides vertical UI by default. It supports both mobile phones and tablets across Android ™ , and iOS ™ , and Windows platforms. Functionality can vary according to OS. For more details, see Installation and system requirements and Getting started.

2 Installing

This chapter describes the requirements to use Knox Manage and the ways to install Knox Manage application on your devices. Please refer to the platform-specific guidelines on how to correctly install Knox Manage.

Installation and system requirements

The supported devices and OS are as follows:

- Android™: Android 5.0 (Lollipop) or higher
  - Android Enterprise : Android 6.0 (Marshmallow) or higher
    (For Fully Managed with Work Profile type : Android 8.0 (Oreo) or higher)
- iOS™: iOS 9.0 or higher
- Windows: A desktop computer on which Microsoft Windows 10 Version 1703 or higher is installed (Pro/Enterprise/Home)

Supported language

The Knox Manage supports the following languages, and you select the language in the device settings. If a user chooses a language that is not supported on user device, then the Knox Manage is displayed in English.

- English
- Portuguese
- Spanish
- French
- German
- Italian
- Korean

Installing Knox Manage

Knox Manage supports various device platforms. You can install Knox Manage app via the public app store of your platform such as Google Play Store and Apple App Store. To enroll the bulk devices, use the Knox Mobile Enrollment (KME), Device Enrollment Program (DEP) or Zero Touch Enrollment (ZTE).

- General installation guide for Android(Legacy), iOS, and Windows devices.
- Android Enterprise devices installation guide.
- Bulk enrollment with KME (For Samsung devices).
- Bulk enrollment with DEP (For iOS devices).
- Bulk enrollment with ZTE (For non-Samsung Android devices).

Note: Introduce required authorities for the service after installing Knox Manage. Knox Manage application does not work if you do not agree to required access.
- Photos, media, files
- Location
- record audio
- SMS messages
- phone calls

General installation guide for Android(Legacy), iOS, and Windows devices

To enroll a single device to Knox Manage, install Samsung Knox Manage app from the public app store of your device platform. Knox Manage installation information is sent via the following methods:

- An administrator sends the installation information and the user ID via SMS or email to all users via the Admin Portal.
  - To receive an SMS, your mobile number must be registered in user information.
  - Click the appropriate URL or scan the QR code for your device platform, because the email is delivered with the installation URL or QR code for all platforms.
- Or, you can directly search for and download Samsung Knox Manage app in the public app store.

To access Knox Manage, tap **Open** in the public store or tap the  icon located on the home screen of your device.

Note:
- If you have previously installed Knox Manage on a device running Windows 10 and thus have a .ppkg file on it, you must delete the .ppkg file beforehand.
  - Go to **Settings > Accounts > Access work or school > Add or remove a provisioning package** on the Windows 10 device, and delete the installed provisioning package (ppkg) file.
- For iOS devices, you should install MDM profile in settings.

Android Enterprise devices installation guide

For Android Enterprise devices, Knox Manage supports three manage types: Fully Managed, Fully Managed with Work Profile, Work Profile.

The Fully Managed and Fully Managed with Work Profile types are normally enrolled on the corporate-owned devices, and the devices should be factory reset in advance. Once logged in to the Knox Manage app, these devices are enrolled as Android Enterprise devices in the Admin Portal. Then, the configured policies and applications are deployed immediately.

Fully Managed

In Fully Managed type, the device is fully controlled by Knox Manage. In general, Corporate-owned devices in factory reset mode will be activated in Fully Managed. There are several ways to enroll devices in Fully Managed type:

- Enrolling devices using Knox Manage token
- Enrolling devices using a QR code
- Enrolling devices using ZTE
- Enrolling devices using KME

Note: After the device enrollment, users must configure the screen lock password in accordance with the password policy has been applied.
If the security level of password on device is lower than the level of policy, the device will be stayed as Lock Task Mode where users can not use any other functions of device.

Enrolling devices using Knox Manage token

When enrolling devices in Fully Managed type and entering account, you need to enter a token. Enter "afw#KnoxManage" as the token. Then, the device is automatically identified as an EMM provider and the Knox Manage app is installed.

- Supported devices: Android 6.0 (Marshmallow) or later

To enroll your device by entering a token, follow the steps below:

1. After the device factory reset, tap **START**.
2. Select a Wi-Fi network, then tap **NEXT**.
3. Agree to EULA&Diagnostic Data Terms and Conditions, and then tap **NEXT**.
4. On the "Sign in with your Google account" screen, enter "afw#KnoxManage" into the Email or phone field, and tap **NEXT**.
5. Read the Google services notice, and tap **NEXT**.
6. To proceed to install the Knox Manage Agent, tap **INSTALL**.
7. To complete the installation, agree to Terms and Conditions.
8. To configure the device, tap **SET UP**.
9. After the Knox Manage app completes the installation and the device restarts, the app is launched automatically.
10. Enter the **User ID** and **Tenant ID** in the form of UserID@TenantID and tap **SIGN IN**.

Enrolling devices using a QR code

When you scan the QR code that the administrator has sent, your device can be enrolled in Fully Managed type.

- Supported devices: Android 7.0 (Nougat) or later

To enroll your device by scanning a QR code, follow the steps below:

1. After factory resetting your device and turning it on, tap the screen six times on the welcome screen to launch the QR code enrollment flow.
2. The QR Reader app is automatically downloaded, and the device launches the camera to scan QR code. Scan the QR code of Android Enterprise which has been sent by email.
   - The Knox Manage access URL and Tenant information in the QR code are automatically detected.
3. Connect to a Wi-Fi or mobile network, tap **Next**.
4. On the setting up device screen, tap **Accept & continue** after reading Samsung Knox Privacy Policy and Google Policy from the link.
5. Check EULA and Privacy Policy agreement for Samsung app permissions, and tap **Next**.

6. On the Knox Manage Sign-in screen, enter your password and then finish enrolling your device.

Enrolling devices using ZTE

Once you turn your Android(non-Samsung) device on and connect to a Wi-Fi network, the Zero Touch Enrollment (ZTE) service automatically starts running. The device then goes into Managed Device type. Note that only the devices that administrators have already enrolled in the ZTE Portal can be enrolled using ZTE. For more information, see Zero Touch Enrollment section in the *SAMSUNG Knox Manage Administrator Guide*.

Enrolling devices using KME

Once you turn your Android(Samsung Galaxy only) device on and connect to a Wi-Fi network, the Knox Mobile Enrollment (KME) service automatically starts running. The device then goes into Managed Device type. Note that only the devices that administrators have already enrolled in the KME Portal can be enrolled using KME. For more information, see Knox Mobile Enrollment section in the *SAMSUNG Knox Manage Administrator Guide*.

Fully Managed with Work Profile

In Fully Managed with Work Profile, Knox Manage can control business applications and data within the device's work area and also use device commands within the personal area at the same time. The user can install and use personal applications within the personal area using their personal Google account. In this case, Knox Manage cannot control personal applications.

The Corporate-owned devices in factory reset mode can be activated in Fully Managed with Work Profile. And the device enrollment method is identical to the Fully Managed type.

When enrolling a device using one of the following ways of Fully Managed, once you log in to Knox Manage during the last device enrollment step, the policies are applied in accordance with the Android Enterprise enrollment type specified in the profile applied, and then the Work Profile is installed automatically.

- Enrolling devices using Knox Manage token
- Enrolling devices using a QR code
- Enrolling devices using ZTE

- Enrolling devices using KME

Only devices running Android 8.0(Oreo) or later can be activated in Fully Managed with Work Profile type. If you enroll devices running versions earlier than Android 8.0(Oreo) by selecting one of ways of Fully Managed with Work Profile above, then they remain as Fully Managed type.

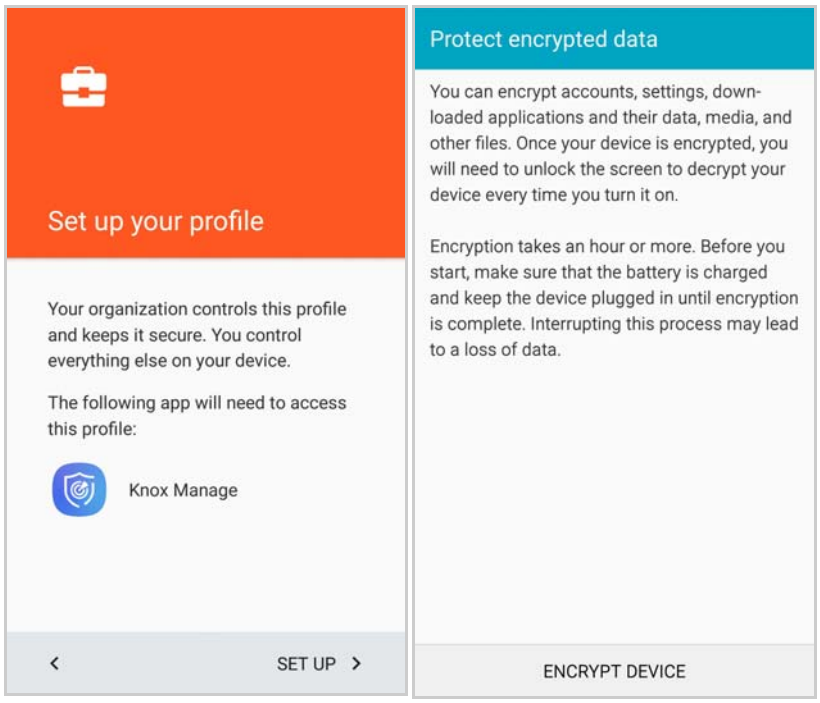
Note: After the device enrollment, users must configure the screen lock password in accordance with the password policy has been applied.
If the security level of password on device is lower than the level of policy, the device will be stayed as Lock Task Mode where users can not use any other functions of device.

Work Profile

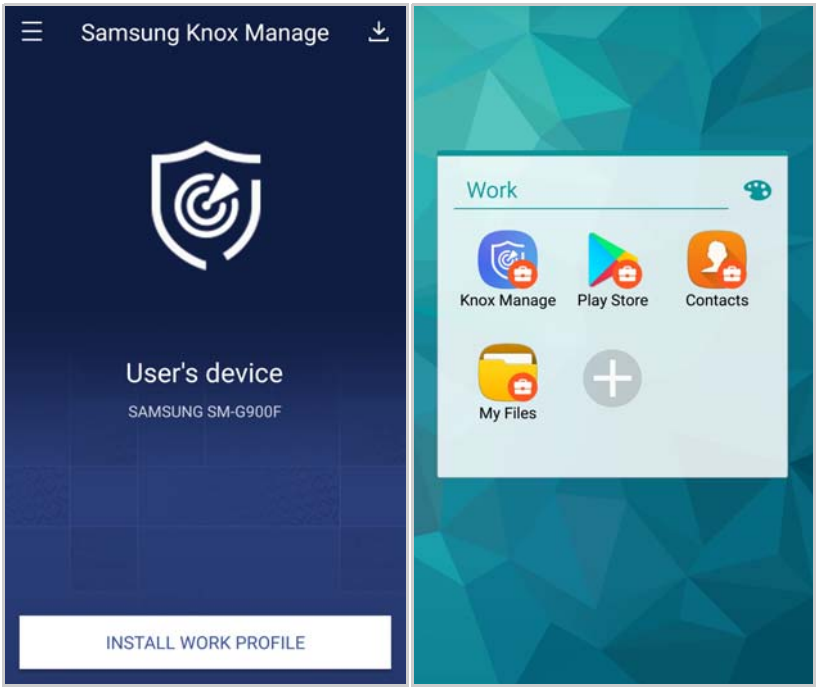
When you enroll a device in Work Profile type, Knox Manage can control the device's area separated as a Work area. You can install Knox Manage in the same way as you would in Android (Legacy).

To enroll your device in Work Profile, follow the steps below:

1. In the text message sent to your device, tap the installation URL.
   - Alternatively, search for Samsung Knox Manage in Play Store and install it.
2. Go to Play Store, search for the Samsung Knox Manage app, and install it.
3. Enter your user ID and password, and sign in to Knox Manage.
4. When the "Set up your profile" screen appears, read the Terms and Conditions, then tap **Agree**.
5. Check that Knox Manage is the app that needs to access your profile, and tap **SET UP**.
6. Tap **ENCRYPT DEVICE**. To start Work Profile type, you need to encrypt your device.
   - The encryption process takes time. Make sure to check your battery level before you tap **ENCRYPT DEVICE**.
   - This option doesn't appear on devices running on a later version than Android 6.0 (Marshmallow) because they encrypt data by default.



7. Once the encryption is complete, the device restarts.
8. Tap the message on your device's notification bar or tap the **INSTALL WORK PROFILE** button in the Knox Manage app to complete the Work Profile setup process.
9. Accept the Terms and Conditions, check your account in the Knox Manage app, and then tap **SIGN IN**. Business applications with a briefcase badge icon appear on your device.
    - You can control data from business applications marked with a briefcase badge icon using Knox Manage.
10. During the initial installation, the Knox Manage app is installed in both the Work Profile and the personal area, but when you sign in to the Knox Manage app in Work Profile, the removal pop-up appears automatically to delete the Knox Manage in the personal area.
    - If you did not delete the app through a pop-up, you can click the app icon in the personal area to see the deletion pop-up and remove the app.



Bulk Enrollment with KME (Samsung devices only)

If you are using a device preregistered by the administrator for the KME connection, the Knox Manage application is automatically downloaded and installed, and its login screen is displayed when the device is initially booted for the first time or connected to Wi-Fi. KME only supports Samsung Galaxy devices running Knox 2.4 or later.
For more information about setting KME, see KME in the SAMSUNG *Knox Manage Administrator Guide*.

1. Tap **Next**, when the Mobile Enrollment Guide appears.
2. After reading the Knox Security Policy and Privacy Policy, select the **I accept all of the above information** checkbox and tap **Next**.
3. After guiding you through the authentication and registration process, Knox Manage is activated.

Bulk Enrollment with DEP (iOS devices only)

According to the iOS settings support procedure, after the DEP service is enabled, the MDM Profile, which is used to control devices via Knox Manage, is installed on DEP iOS devices that have already been bulk-enrolled by an administrator. The configuration processes for languages, countries, regions, etc., are based on the

settings of the DEP profile, and the items that the administrator didn't choose to skip are shown on the screen. To configure the DEP settings, see the Apple Device Enrollment section in the *Samsung Knox Manage Administrator Guide*.

To enroll DEP-enrolled devices, read the following:

1. Select supported languages, and then countries or regions.
2. Once you connect to a Wi-Fi or mobile network, the device activation process begins.
3. To manage the DEP settings for the devices through Knox Manage, go to the Remote Support screen, then tap Apply Configuration.
4. Once the settings are configured, go to **Settings > General > Profiles**, select the installed MDM Profile, and check whether the MDM Profile can't be deleted.
   - The MDM Profile could be deleted depending on the administrator's settings.
5. If Supervised mode has been enabled in the deployed profile, go to **Settings > General > About**, and check whether Supervised mode is enabled. Under the Name, the "This iPhone is supervised" message is shown."

Bulk Enrollment with ZTE (non-Samsung Android Enterprise devices only)

If you are using a device preregistered by the administrator for the ZTE connection, the Knox Manage application is automatically downloaded and installed, and its login screen is displayed when the device is initially booted for the first time or connected to Wi-Fi. ZTE only supports Android Enterprise devices for non-Samsung devices running Android 8.0 (Oreo) or higher.

For more information about setting ZTE, see ZTE in the SAMSUNG *Knox Manage Administrator Guide*.

1. Tap **Start** on the Zero Touch Device Enrollment screen**.**
2. On the “Set up your device” screen, tap **Accept & continue**. The device will get account information for Knox Manage.
3. On the “Google Services” screen, tap **Accept**. The Knox Manage app will be installed and launched automatically on the device.
4. On the Knox Mange log-in screen, enter a Knox Mange user ID and password to log in.
5. On the Knox Mange terms and agreements screen, read the terms of use, privacy policy, and end-user license agreement, tap the checkbox next to **Agree all**, and then tap **NEXT**.
6. On the “Display over other apps” page, if required, tap **All display over other**. The device will be registered and enrolled in the Knox Manage Portal.

3 Getting started

User needs to log in to Knox Manage application after installation for the security policy to take effect on your device. If an administrator has already assigned a profile to you, then the security policy is applied immediately upon login.

Self-testing Knox Manage Agent start-up

The device application uses OpenSSL (Secure Socket Layer) in the device for self-testing. Samsung Knox Manage Agent also carries out self-testing, whenever the device is powered on, to make sure that MDM Agent is working properly .

Once the device is turned on, Knox Manage Agent communicates with the Knox Manage server for a registry check-up. If the device registry is compromised, the server blocks communication between Knox Manage Agent and server to disable the device. In addition, Knox Manage Agent checks the integrity of policies and other application data applied on the device. When the device is enrolled on the Knox Manage server or logged into Knox Manage Agent, the Agent receives the policies and other application data from the server, and the Agent saves those policies and data.

The policies and application data are stored in a secure storage area in the following cases:

- Data objects get hash value by using SHA 256
- Encrypt the data object with AES 256
- Double encrypt the data with AES 256 and the hash value for absolute security

When the device is turned on, the Knox Manage Agent reads the encrypted policies and application data and performs an integrity check as follows:

1. Decrypt the double encrypted data and hash value
2. The decrypted data gets hash value by using SHA 256
3. Compare the hash values of when they are saved and when they are used

If policies or other application data are compromised, Knox Manage server blocks communication between Knox Manage Agent and Server to disable the device.

Logging in Knox Manage

After Knox Manage installation is completed on your device, enter your **User ID** and **password** to log in. The initial login might take longer than expected because the Tenant ID needs to be verified by server.

Logging in manually

To log in to the Knox Manage manually, follow the steps below:

1. Tap the icon installed on user's device to launch the Knox Manage.
2. Enter the **User ID** and **Tenant ID** in the form of UserID@TenantID, and **password** you received from the administrator, and then tap **Log In**. When logging in for the first time, your **password** is the same as your **User ID**.
3. Read the End User License Agreement and tap **Yes**.
4. On the "Activate device administrators" screen, tap **Activate**.
5. When the "Privacy Policy" window appears, select the check box, and then tap **Confirm**.
6. To change your temporary password, enter your current **password** (your current user ID), enter your new password in the **New password** and **Confirm new password** fields, and then tap **Change**.
7. Set a screen lock password. For more details about how to set lock password, see Setting screen lock password.
   - The screen lock password can be set at login only when the administrator sets the Knox Manage Agent Policy> Use Lock Screen as Use.
8. To log in Knox Manage on an iOS device, go to **Settings > General > Profile** to register your device, install your profile, and then launch the Knox Manage app again.

Note:
- The **user ID** must be registered to the Admin Portal by the administrator to log in to Knox Manage.
- For Android device users, the administrator must include access to the Knox Workspace in the device policies so that they can install the Knox container after installing the Knox Manage app.

Setting screen lock password

User must have a screen lock password for private data protection. Screen lock password policy may be different depending on the policy set up on the Admin Portal. For Fully Managed or Fully Managed with Work Profile, user must configure the screen lock password as strong as the password policy which has been applied to the device

by administrator. If not, the device will be locked in the Lock Task mode, and cannot move to other screen.

To set screen lock password, follow the steps below:

1. Enter a screen lock password
   - Enter a password between 6 to 20 characters combining letters, numbers, special characters, and upper case letters.
   - Password rules can be changed depending on the policies configured on Admin Portal.
2. Re-enter the password to confirm, then tap OK.

Note: You enter an incorrect password 5 consecutive times, (limit on the number of failed attempts could vary depending on the policy set up on Admin Portal) Knox Manage will perform one or more of the following actions:
- No control.
- Lock the device.
- Factory reset & SD card initialization
- Only the device is factory reset.
- Sign out of Knox Manage.

Auto-installing configuration and checking apps

After logging in to Knox Manage on the device, the profile assigned to the user is deployed. The device is controlled according to the profile settings. The configuration and apps that are installed automatically are as follows:

Auto-installing configuration

If the configuration registered for a device management profile,

such as Wi-Fi or VPN settings can be installed automatically on the device without user interaction. After the configuration runs automatically, either the Installed or Pause result notification message is shown.

Even if the configuration can be installed automatically, a Wi-Fi connection needs to be established in Settings on the device because it can't connect to an AP automatically.

To install the configuration automatically, you need to prepare the following:

- For the Wi-Fi 802.1xEAP and VPN settings, install Credential Storage (CS) where trusted certificates can be stored beforehand. CS installation means locking the device screen using an option more secure than a password.
- The Generic VPN setting requires installation of the Vendor Client beforehand.
- The Email and Exchange settings require installation of the Samsung Email app that is provided by default, and the user must agree to receive notifications from the Email app. (Galaxy S8 or later)
- To install settings in the Knox container, the VPN Vendor Client must be installed in the General area first.

Auto-installing apps

When you log in to Knox Manage, a notification will appear if there is an application that to be installed on your mobile device, and the application will be automatically installed. When there are multiple applications, they will be automatically installed one by one.

Note:
- Depending on the settings configured by the Admin Portal, you may not be permitted to uninstall applications.
- If Kiosk mode has been set by the administrator, Kiosk mode starts after installing all the applications.

Exploring the Knox Manage home

Exploring on an Android or iOS device

When you launch the Knox Manage app, the Knox Manage Home screen will appear. For Samsung Galaxy devices running on Android, if the administrator has already registered a Knox Workspace in the Profile, then the Knox Workspace is installed automatically when the profile is applied. If you cancel the installation of the Knox Workspace, then a message appears in the Notification bar or an Install button appears on the Home screen.

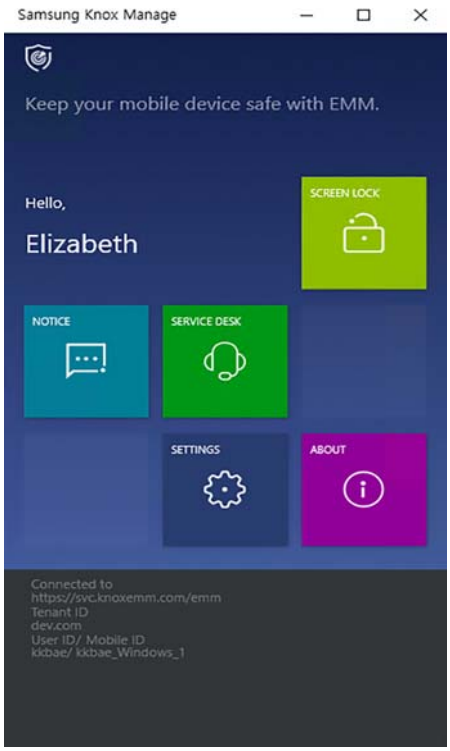
At the center of the home screen are the user ID and the device model in place.
In the upper-right corner of the Home screen, there is a badge that shows the number of downloadable configurations. Tap  to open the **Download Configuration** menu.

Note: If you use Knox of your Samsung device, tap **INSTALL KNOX** of the lower home screen to install a Knox Workspace. If you are not a Knox user, the **INSTALL KNOX** button will not appear at the bottom of the Home screen. In addition, if the device is rooted, the Knox Workspace cannot be properly installed according to Knox specifications.

- The notification for Knox Workspace installation is displayed on the device notification bar. This notification disappears once a Knox Workspace is installed.

Exploring on a Windows 10 device

When you launch the Knox Manage app, the Knox Manage Home screen appears as follows:

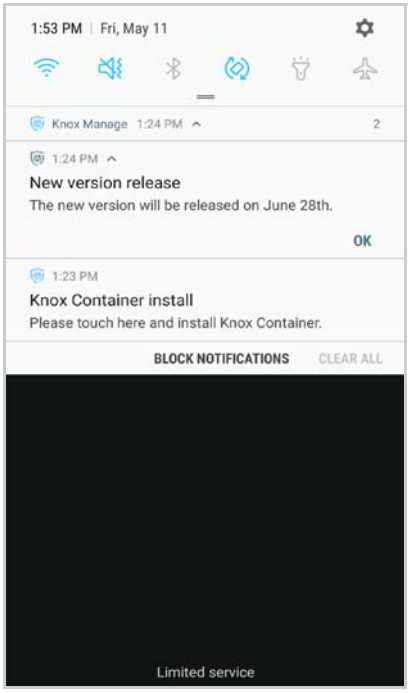


In the center of the Knox Manage Home screen, you can see the lock screen, notices, customer support, settings, and version information.

- **SCREEN LOCK**: Tap it will lock your device immediately. The screen will be unlocked when you enter the screen lock password.
- **NOTICE** : You can check notices posted by Knox Manage administrators.
- **SERVICE DESK**: This provides a phone number and email address of the customer service center. It also provides a log transfer feature to send information about errors to administrators.
- **SETTING**: You can change the Knox Manage screen lock password from this menu.
- **ABOUT**: This contains information on the current Knox Manage version, Term of Use, Open Source License. Use the Update button at the bottom to move to the public store for updating Knox Manage.

Receiving notifications

If the Knox Manage server sends a notification to the user's device or the user's action and confirmation are required, the notification bar in the device will display the message as follows. To delete a notification, tap **OK** on the notification bar.



Exploring the side menus

Tap the ☰ at top left corner of Knox Manage home screen to see its side menu. Menus provided by Knox Manage are described below.

However, on Windows 10 devices, the Home screen provides the side menu contents.

- **Basic information**: You can view connected user ID and mobile ID. Tap ⌄ to view a tenant ID and connection server information.
- **Notices**: Users can check notices posted by administrators.
- **View policies**: You can view a list of all policies applied to the user's device. If the administrator has allowed **Show all policies applied** under Knox Manage Agent Policy in the Admin Portal, the policies applied will be displayed. This menu may not be available depending on the browser policy.
- **Application store**: You can view internal apps provided by Knox Manage and public apps and download the apps you want. For more details, see Using App Store:

  Note:
  - Knox users can use the Knox Manage App Store in Knox Workspace.
  - Android Enterprise users can tap Play Store to move to Managed Google Play Store.

- **Content**: This menu is only available on Android devices. The file distributed by the administrators can be checked on the devices from this menu. For more information, see Viewing content.
- **Download Configuration**: This menu is applicable for Android devices only. You can install the security applications deployed by your administrator, such as Wi-Fi and VPN Exchange. You can move to the same function menu by tapping the top-right corner  of the Knox Manage Home screen. For more information, see Downloading configuration.
- **Settings**: Set an alarm related to Knox Manage, change screen lock passcode, and cancel service subscription. Depending on the area Knox Manage installed, the Settings items can be different.
- **Service Desk**: This provides a phone number and email address of the customer service center. It also provides a log transfer feature to send information about errors to administrators. An Android user can tap the Remote Support App download link and install the application.
- **About**: This contains information on the current Knox Manage version , Term of Use, and Open Source License. Use the Update button at the bottom to go to the public store of each platform to the most recent version.

Locking the screen and obtaining new policies

In the middle of the Knox Manage side menu, there are two items:  **Lock screen** and  **Reload policies**. The screen lock is shown according to the policy of app management profile in the Admin Portal

- When you do not use a device over a set period of time or when you tap  **Lock** screen on the middle of the Knox Manage Home screen, the screen will be locked immediately.
  - To unlock the screen, tap  at the bottom of the screen and enter your screen lock password.
  - You can change the screen lock password by tapping **Services > Screen lock** in the side menu.
- If the administrator-defined policy has not been applied to your device, tap  **Reload policies** in the middle of the Knox Manage side menu to request the latest policy from the administrator.

Providing service desk information and sending activity log

The **Service Desk** in the side menu provides an email address and phone number so that users can get support in using Knox Manage. If an error occurs while you are using Knox Manage, activity log will be immediately sent to the server to make sure

that administrators are able to take proper actions. It might not be possible to send the log, if the log has not been collected.

Downloading and running the Remote Support app

Service Desk in the side-menu provides Knox Manage Remote Support App

download link. Tapping **Download Remote Support App** downloads the application to the device and installs it automatically. Once installed, the link changes to **Run Remote Support App**, which the user can tap to launch the application. This menu is only available on Android devices.

Viewing version information and updating

In the **About** from side menu, the current version of Knox Manage can be found. Tap **Update** to be directed to Play store to update Knox Manage app.

- Tap **Privacy Policy** to be directed to the web site for the company privacy policy.
- Tap **Open source licenses** to check notices on open source license used by Knox Manage app.

Viewing content

This is a content management menu available only on Android devices. When an administrator uploads a content file to device, users can find the installation progress from notification bar, and view the content file upon installation complete. This content file also can be accessed from the **Content** menu in the Knox Manage app.

- Downloaded content is saved in **My Files > Internal storage > Download > Knox Manage > Content**.
- The user can check the downloaded content by directly opening the file in the folder where it is saved under **My Files**, or by clicking the file name from the file list of the **Content** menu in the Knox Manage app.
  Content is automatically opened using an appropriate file viewer installed on the device.
- Tapping the Refresh button in the upper-right corner updates the list to the latest version of the content list on the Admin Portal. Content deleted from the device can be downloaded again if it's redistributed from the Admin Portal.

Downloading configuration

This is a menu for the security environment provided only for Android devices. Tap  , the top-right corner of the Knox Manage Home screen, or tap **Download Configuration** on the

side menu to read the environmental security details deployed by the administrator, and you can install or remove the setting.

The deployed configuration which has only one value specified per category, such as VPN and Email settings, is installed automatically on the device. Wi-Fi is installed automatically even if one more values are registered. For more information about auto-installation, see Auto-installing configuration.

Users can only view the items that have been specified in advance by administrators, depending on the settings installed in the user device, to distinguish the scope of view.

Note:
- When deleting installed VPN, reboot the device to delete the profile completely.
- Only one Generic VPN is allowed per device, regardless of whether it would be general container or Knox Workspace.
- Android Enterprise users can install the Wi-Fi and Bookmark settings on their managed devices.

Installing and deleting corporate configuration

To add or remove security settings on the Android devices, follow the steps below:

1. On the right-top of Knox Manage Home screen, tap  or tap **Download Configuration** in draw menu.
2. Tap **Install** to the right of the item you want to install.
3. To uninstall installed items, tap **Delete** to the right of the item you want to remove. However, you cannot remove items that the administrator has prevented from being removing.

Configuring services

Settings on the side menu consists of notification settings for event policies, screen lock password settings, and service deactivation. The screen lock is shown according to the policy setting of the Admin Portal.

- **Event Notification**: You can receive notifications for the events that you have selected to receive notifications for **Show noti when event is on** and **Show noti when event is off** and you will not receive notifications for events that you have not selected to be notified about. If you tap **On** for **Restrict dismissing noti**, on the Android device, it is fixed on the notification bar and you cannot swipe any event-related notifications to delete. For iOS devices, notifications are displayed on the top of the app screen for 5 seconds.
- **Screen lock**: Set a new screen lock password.
- **Unenrollment**: There are two ways to unenroll Knox Manage.

- If your device is unable to connect to a network, then enter an offline unenrollment code to disable Knox Manage. The code is provided by administrators. If the code is not valid and an error message appears, you must contact the administrator again.
- If your device is able to connect to a network, then you can make a request to disable Knox Manage. This option is only available if the administrator has allowed users to request disabling of Knox Manage from the Admin Portal.

Note: When the Knox Manage service is deactivated, depending on the administrator settings, the apps managed by the Knox Manage may be automatically deleted from the user's device.

- **Knox Workspace**: If you are using a Knox Workspace on your device and forget your password, then you can reset the password through the Knox Manage user verification process.
  - Devices running Android 8.0 Oreo or later: After entering the Knox Manage log-in password and successfully completing the verification process, enter the temporary password appearing in the notification bar at the top of your device, and then change the Knox Workspace password.
  - Devices running versions before Android 8.0 Oreo: After entering the Knox Manage log-in password and successfully completing the verification process, change the Knox Workspace password.

4 Using applications

Applications registered in the Knox Manage Admin Portal can be deployed to users. Some applications registered as automatic or mandatory installation type in Admin Portal are automatically installed on devices without user intervention. Applications can be installed on devices as follows:

- Installing Google Managed apps: For Android Enterprise devices, you can download the public applications approved by the administrator from Google Play Store. The Google Managed apps can be installed automatically or manually depending on the app policies.
- Installing VPP applications: For DEP devices running on iOS, you can download VPP applications from Apple's App Store.
- Using App Store: For manual installation apps, you can download applications from the Knox Manage App Store.

To deploy applications using Volume Purchase Program (VPP) on iOS devices, see Installing VPP applications.

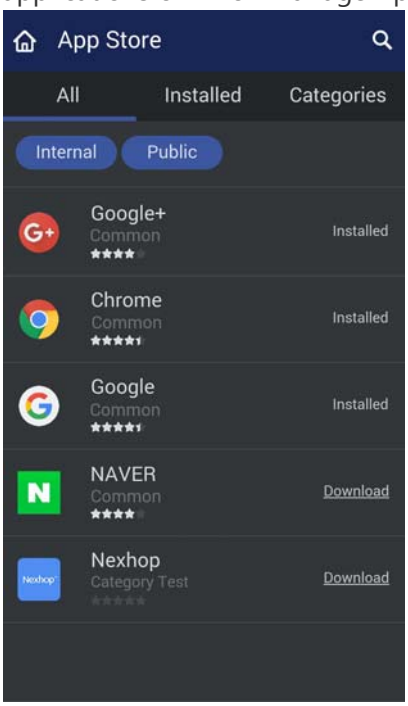
Note: If you are using Knox, you can view and run applications that you have downloaded and installed via the Knox Manage App Store in the Knox Workspace.

Using App Store

Using App Store of the Knox Manage, users can browse and download both internal apps provided by administrator and public apps permitted.

Viewing application list

To view the complete list or installed list of internal applications and public applications on Knox Manage Application Store, follow the steps below:



1. Tap **All** to view all applications registered on Knox Manage Application Store. The category name and app's rating with the number of starts appear on the list.
2. Tap **Installed** to view only device-installed applications.
3. Tap on the top right corner of the screen and enter the application name, and then tap to search for the application you want.
4. Tap **Download** to download and install the selected application. Depending on the policy settings, you can check the download progress.

Using internal/public apps

You can view internal/public apps with using filter on **all**, **installed**, **categories**. An internal application is a corporate's own mobile business application developed using Knox Manage SDK. A public application means an application registered on a public app store such as Google Play Store or iOS App Store. In public application list, applications that are allowed to be shown by an administrator appear.

To download and install internal or public applications using application filter, follow the steps below:

1. To view only internal application in app store, tap **Public** to deselect.
   - An application filter switches on/off by clicking. In default, **Internal** and **Public** are on.

2. To view only public applications, tap **Public** and tap **Internal** to deselect internal applications.
3. Enter the application name on the top right corner of the screen and tap  to search the application.
4. Tap **Download** to download and install the selected application.

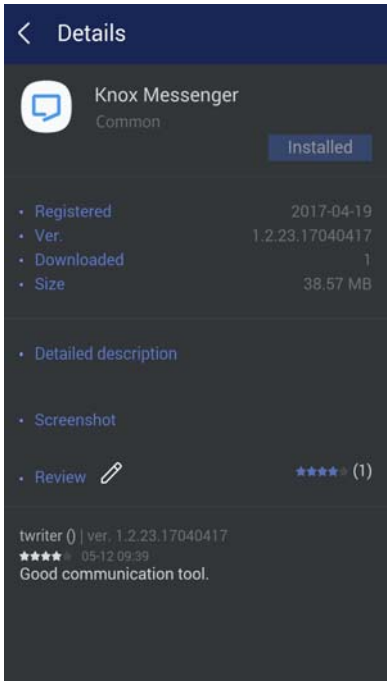
Viewing detailed app information

To view detailed app information, follow the steps below:

1. Tap the app you want on the list to see the detailed information, such as the app introduction and the app screenshot.
   - You can install the application by tapping **Download** on the **Details** page.
   - Applications installed on a user device are shown as **Installed**. Applications needed to update are shown as **Update**.
   - Tap the application **Screenshot** at the bottom of the detail page, and then the larger image pops up.
   - You can check app's rating with the number of starts and individual user reviews on the Detailed app information page.
2. Tap on the top left corner of the screen to go back to the previous page.
3. Tap  on the upper of the application list to quit the App Store and return to Knox Manage home.

Using application reviews

Users can see individual user reviews of applications or rate the applications with a star rating and review. They can only rate internal applications. To use application reviews, follow the steps below:



1. Select an internal application filter on upper side of app store and tap an application.
2. See ratings and review of applications in the App details page.
3. Tap on the right of **Review** on the **Details** page to rate the apps and post your review. When you finish with your review, tap to save it.
4. If you want to cancel the review and go to the previous page, tap on the top left in Update your review page.

Using app categories

You can define categories to group the applications on the App store. The applications are sorted by category. To use app categories, follow the steps below:

1. Tap **Categories** on the bottom of the screen to view the category list.
2. Each category displays the number of applications that you can download and install. If you want to check the applications of a specific category, just tap the category you want.
3. Enter the name of the application on the upper side of a screen to search an application sorted into a specific category.
4. Tap **Download** to download and install the selected application.
   Once downloaded, you can install the application.

Updating applications

If user-installed applications need to be updated, a **Update** button is shown in right side of an application list. Tap **Update**, and then run the update. To update applications, follow the steps below:

1. Tap **Installed** on the top right corner of Knox Manage App store. The installed list of application appears.
2. Tap **Update** to update each application, or tap **Update all** to update all applications.
   - You can update applications in **All** or **Categories**.

Note: When an application is deleted from a device, all related data is also deleted.

Installing Google Managed apps

You can install Google Managed apps approved by the administrator on Android Enterprise devices from Google's Play Store. They are managed using a Work account at your workplace without requiring you to enter your personal Google account's credentials.

To install Google Managed apps on an Android Enterprise device, follow the steps below:

1. Run Google's Play Store app on your device.
   - For devices that are activated in Work Profile type or Fully Managed with Work Profile type, you need to open the Play Store app that has a briefcase badge on it. This Play Store app manages the applications within the work area.
   - You can also be redirected to Google Managed Play Store by tapping App Store in Knox Manage app.
2. A list of applications approved by the administrator is displayed. Select the desired applications, and tap **Install**. Then, the Google managed apps are installed on your device.

Installing VPP applications

To deploy applications using VPP on iOS user devices, follow the steps below:

1. Accept the app assignment message that is sent when administrators invites the VPP users.
   If the user cancel the VPP invitation message, click the link sent to the user's email.
2. Check the terms and conditions of Apple and click **Agree**.
3. Check the assigned apps to VPP users under **Account > Purchased** in App Store.
4. Tap **install** of the assigned app to be installed on the device.
5. To install the apps purchased by the Redeem code, click on the link in the email sent by administrators when assigning the apps. Users can see the installed apps in your account on the App Store.

5 Remote Support

You can share your device screen and receive technical support remotely. Remote Support service (hereinafter called “RS”) can only be supported under enterprise security licenses. Support agents can view your device screen remotely so that they can respond to your inquiries more quickly and accurately.

Installing Remote Support

For remote support, the RS Viewer should be installed on the administrator's computer, and the RS app should be installed on the user's device.

Supporting device platform

The following device platform is supported. For non-Samsung Android devices, use of some features may be restricted.

- Samsung Galaxy or other devices with Android 5.0 (Lollipop) or later
  - If you want to use Remote Support from Knox Workspace, please install the Remote Support app in general area.
  - Supporting devices of Android platform for remote service as following:

Android Legacy Device	Android Legacy Knox	Android Enterprise Fully Managed	Android Enterprise Work Profile	Android Enterprise Fully Managed with Work Profile
O	O	O	X	X

Note: For Android Enterprise Work Profile or Fully Managed with Work Profile devices, Knox Manage can support remote service for perosnal area of device except the Work Profile area. The RS app should be installed in personal area.

Installing mobile application

To install the Remote Support app on your device, follow the steps below:

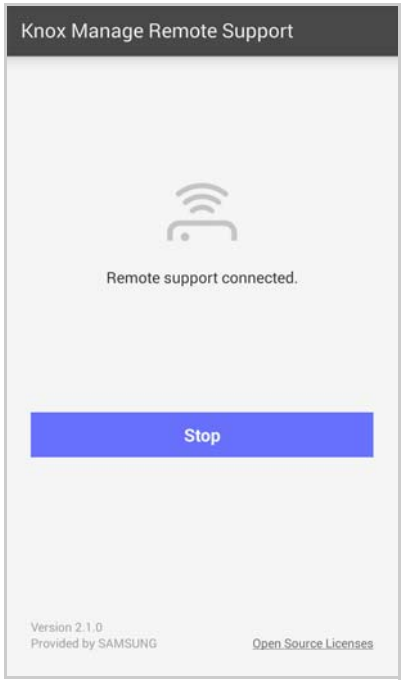
1. Search for **Knox Manage Remote Support** in Google Play and install it.
   - Or, tap **Download Remote Support App** in **Service Desk** in the Knox Manage app, or install the application sent by an administrator.
   - Install the latest version of Remote Support app to use Remote Service without issues.

2. Launch the application upon installation, and the Knox License confirmation process will proceed automatically.
3. The passcode for remote support will be automatically entered, and the RS app will be launched without any user intervention.

Receiving remote support

To receive remote support, follow the steps below:

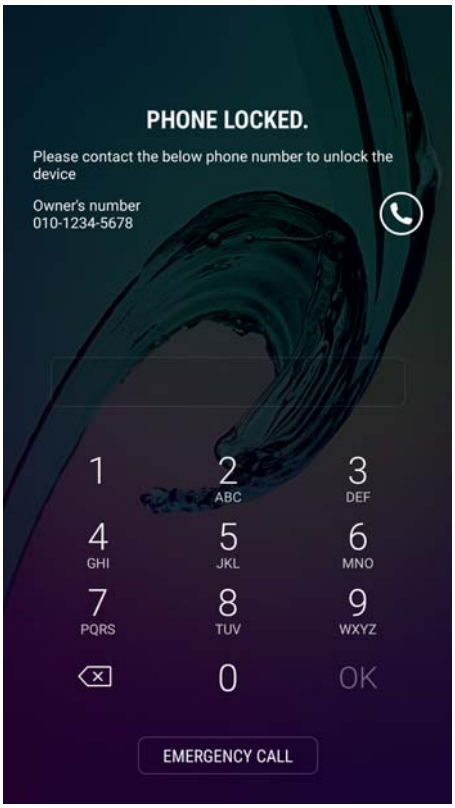
1. Tap the **Knox Manage Remote Support** icon on your device to launch the app.
   - Or, tap **Run Remote Support App** in Service Desk in the Knox Manage app.
2. The remote support service starts from the device home screen.
   - In normal case, users do not have to enter the access code, and the app will start automatically.
3. To close the Remote Support app, tap **End** on the Remote Support screen, or when the support agent ends the support session.



Appendix A Resolving issues

A.1 Fixing the device lock issue

The Knox Manage administrator can send device command to lock user devices or distribute a policy to lock the device.



To unlock your device if it is locked by Knox Manage policy, follow the steps below:

1. If you ask for administrator about your device lock by using your user ID and device ID, the administrator will check whether your device can communicate with the Knox Manage server.
2. If the communication between the device and the Knox Manage server is available, the administrator will send the device command to unlock the device immediately.
3. If communication between the device and the Knox Manage server is not available, the administrator will tell you the device unlock code. Enter the unlock code on your device to unlock it.

Note: If your device is locked due to other reasons, you cannot resolve this issue using the steps above. You must contact a service center to perform a factory reset of the device.

A.2 Addressing password issues

The user device has the following four types of passwords:

- The login password you enter with your user ID when logging in to the Knox Manage server.
- The screen lock password for Knox Manage app that can unlock the screen after logging in to the Knox Manage.
- The screen lock password for the device itself to access the device features.
- The screen lock password for Knox container or Work Profile area to access the device's container area.

To retrieve the password if you forget your password, follow the steps below:

- If you forget your login password:
  a. Request a password reset from the administrator.
  b. Receive a temporary password by email.
  c. Reset your password after logging in to the Knox Manage server with a temporary password.
- If you forget your screen lock password for Knox Manage app:
  a. Request that the administrator use a "Reset screen password" device command.
  b. Your device will be logged out of the Knox Manage, and then you can log in again.
  c. Set a new screen lock password on the login page.
- If you forget your device lock password:
  a. Request that the administrator use a "Reset screen password" device command.
  b. The existing Device Lock password set to the user device will disabled and the password setup screen will appear.
  c. Set a new device lock password.
- If you forget your container screen lock password:
  a. Request to Administrator
  For Knox container lock password, request the administrator to send the "Reset container password" from Container Management device command. For Work Profile lock password, request the administrator to send the "Reset screen password" from Work Profile device command.
  a. Reset by User
  Open Knox Manage app in general area, and tab the  at top left corner and go to Settings> Reset container password. And then validate with Knox Manage login password.

b. For devices with Android 8.0(Oreo) or higher version, the temporary password will be sent and can be found from notification bar. Enter the temporary password and set the new lock password for container.
For devices with lower version than Android 8.0(Oreo), users can directly set the new lock password for container without temporary password.

www.samsungknox.com
Provided by SAMSUNG