Knox E-FOTA On-Premises admin guide

Knox E-FOTA On-Premises

Knox E-FOTA On-Premises allows IT administrators to manage device firmware-over-the-air (FOTA) updates on their organization's network environment. With on-premises features that extend beyond its cloud counterpart, Knox E-FOTA On-Premises is a great FOTA management option for organizations that prioritize security and flexibility in their operations.
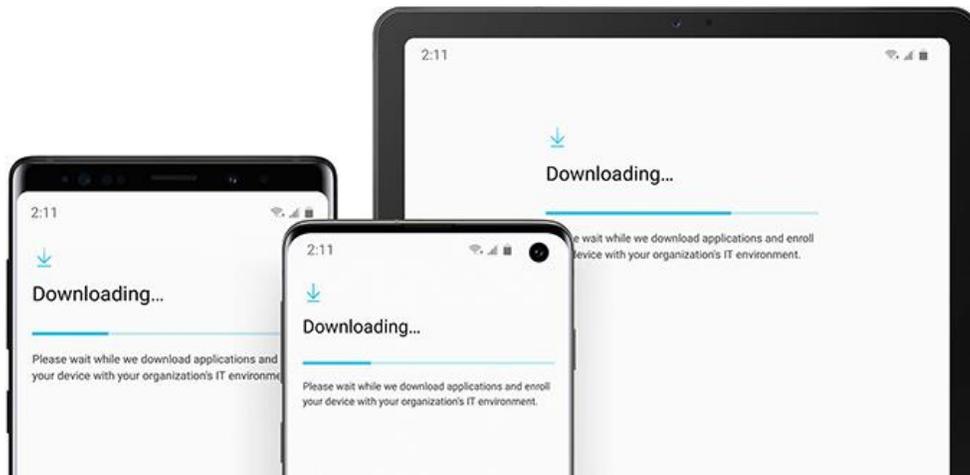
Audience

This document is intended for **IT admins**. Learn how to set up the Knox E-FOTA On-Premises web portal, manage firmware versions, and enroll devices.

Try the solution

This tutorial walks you through how to install the Knox E-FOTA On-Premises agent app, add a license, and add and enroll your devices.

START LEARNING

About Knox E-FOTA On-Premises

This admin guide only discusses features unique to Knox E-FOTA On-Premises. For more information on general Knox E-FOTA features, see the Knox E-FOTA admin guide.

Key features

- **Multi-tenant support** — If your organization has multiple business units, IT admins can work within their respective workspaces to avoid unwanted interactions between units.
- **Firmware testing** — Use the Knox E-FOTA On-Premises console to track firmware versions, mark them as tested, or block them from being installed on devices.

Key benefits

Like Knox E-FOTA, Knox E-FOTA On-Premises provides these key benefits:

- **Schedule updates** — Prevent business interruptions by configuring OS updates to install outside of business hours.
- **Selectively update OS versions** — Choose a specific OS version to roll out to your devices to avoid potential interference with business app functions.
- **Force update target devices** — Ensure devices are always up-to-date with the latest security updates, regardless of user input.
- **No user interactions** — Update device software without requiring user action, streamlining the device management process.

How it works

Knox E-FOTA On-Premises is comprised of three parts:

1. The web portal
2. The client app
3. The organization's network infrastructure

These three components interface to perform FOTA management in a containerized environment, isolated from the cloud. IT admins can sign in to the web portal to enroll devices, create campaigns, update policies, and schedule firmware downloads — all from the safety of an organization's in-house infrastructure.

Step 1 — Access the Knox E-FOTA On-Premises server

Prerequisites

This tutorial assumes that you've already installed Knox E-FOTA On-Premises with the recommended hardware, software, and network configuration. Contact your local Samsung representative for more details about the installation process, or see Installation and upgrade guides.

Access the admin console

Admin console server URL

To access the Knox E-FOTA On-Premises admin console after installation, go to your server URL.

The URL takes the form of ***access_scheme*://*access_address*:*access_port*/admin/**. For example, http://192.168.1.52:6380/admin/.

If you don't know your server URL, contact your Samsung installation engineer.

Account ID and password

The default credentials for the console are:

Property	Value
Account ID	admin
Password	admin12#

Make sure to change your password after you sign in for the first time.

For more details, see *5.1. How to access the admin console page after installing* in the installation guide for your environment.

Step 2 — Add a license

After accessing the admin console, the next step is to add a license. You can generate a license file with your license key and your server's MAC address through the self-service **Knox E-FOTA On-Premises Resources** web page > **Download License Files**.

Once you have your generated license file prepared:

1. On the Knox E-FOTA On-Premises console, click your account icon.
2. In the menu that's shown, click **Settings**.
3. The navigation sidebar pane refreshes with a new set of tabs. Click **License**.
4. Click **UPLOAD LICENSE**.
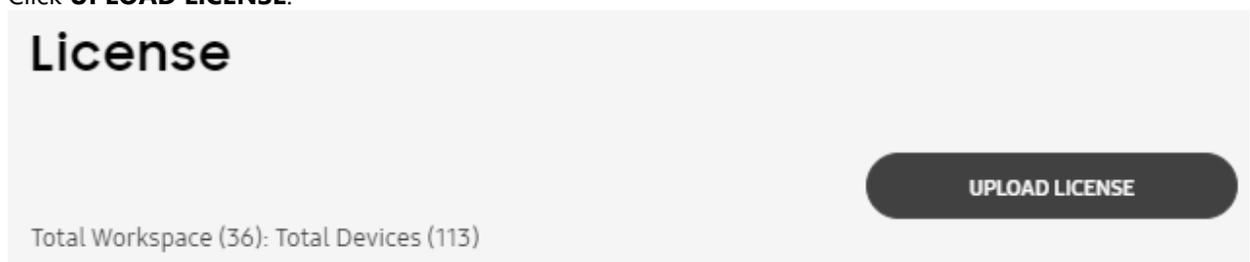
5. In the popup that's shown, click **BROWSER** to launch the file explorer, where you can locate your license file to upload. Select the file, then click **Open**.
6. Click **UPLOAD** to finish uploading the license.

The **License** screen then displays the details of your license.
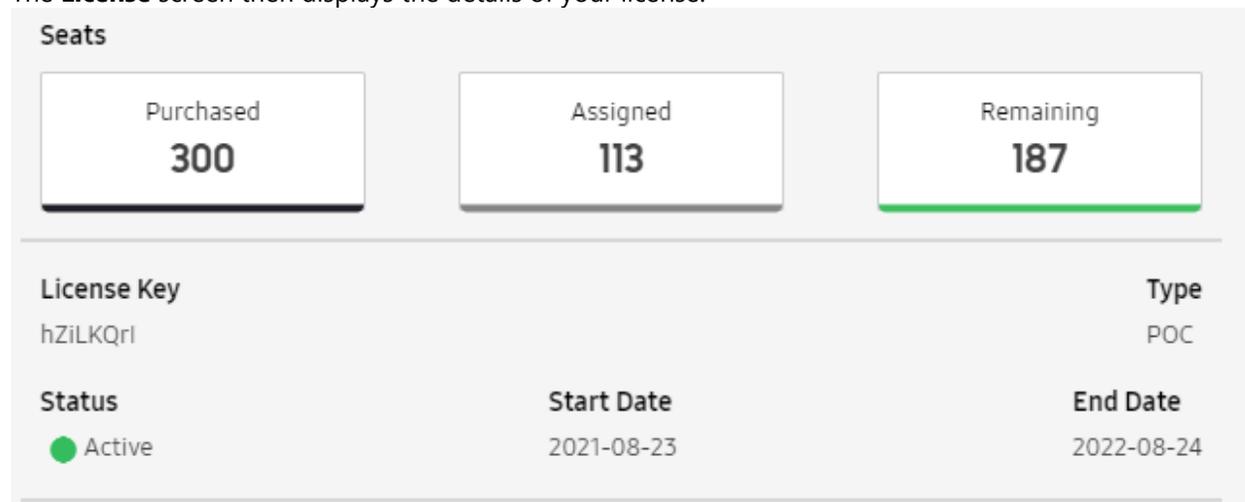
Refer to Manage licenses to learn more.

Step 3 — Add devices

Next, it's time to add devices to the console, which you can do by uploading a CSV file. Adding devices without enrolling them doesn't immediately consume any license assignments.

> **Important**
> Each device you enroll consumes one license seat.

To add devices to the Knox E-FOTA On-Premises console:

1. At the bottom of the navigation sidebar, click **Bulk Actions**.
2. Click **Upload Devices**.

UPLOAD DEVICES

3. Click **Download CSV template** and open the downloaded file.
4. In the first column, enter the IMEI/MEIDs or serial numbers of the devices you want to upload. Enter one IMEI/MEID or serial number per row.

> **Note**
> Don't include a header row, leave rows empty, or duplicate IMEIs, MEIDs, and serial numbers. Otherwise, your devices may not be added properly.

5. Save the file.
6. In the Knox E-FOTA On-Premises console, click **Browse** and select your CSV file.
7. (Optional) Auto-enroll or assign the devices to a campaign. If you skip this step, you can enroll and assign devices at any time.
8. (Optional) Apply tags from the CSV file you uploaded to the devices. You can add a maximum of 10 tags, and tags are case-sensitive.

9. Click **Confirm**.

A message shows and confirms that the CSV file was uploaded. When your devices are verified and added to your inventory, they're added to the **Devices** tab with the status **Not enrolled**.

Step 4 — Enroll devices

If you chose not to enroll devices when adding them in the previous step, you can do that now by selecting specific devices for enrollment through the device list. This action is only available for devices in the **Not enrolled** state.

To enroll your devices:

1. In the sidebar of your Knox E-FOTA On-Premises console, click **Devices**.
2. In the devices list, select the checkboxes next to the devices you want to enroll.
3. Click **ACTIONS**, then **Enroll Devices**.
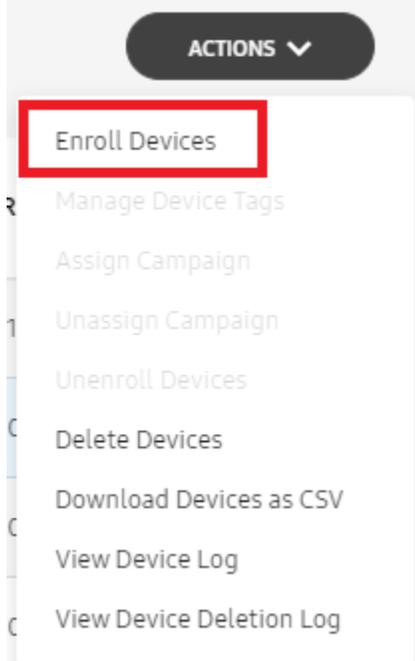
4. In the confirmation popup that appears, click **ENROLL**.

The next time the devices poll the server, they are then enrolled in Knox E-FOTA On-Premises, locking their firmware versions and consuming the corresponding number of license assignments.

Step 5 — Download and install the agent app

Now it's time to install the Knox E-FOTA On-Premises agent app. Contact a Samsung technical support engineer to get new agent app versions.

There are three ways to install the agent app on your devices:

- Update the Knox E-FOTA On-Premises agent app by uploading the package through the console

    Important
    Updating the Knox E-FOTA On-Premises agent app by uploading it to the admin console is only supported if the agent app is already installed and running on your devices.
- Manually install the package
- Install the client through your EMM

Update the Knox E-FOTA On-Premises agent app by uploading the package through the console

If you want to update the existing agent app on your devices:

1. Sign in to the Knox E-FOTA On-Premises admin console. Make sure you're in the correct workspace by verifying its name in the top-right corner of the console.
2. Click your account icon, then click **Settings**.
3. The navigation pane refreshes with a new set of tabs. Click **Agent**.
4. Click **ACTIONS** > **Upload Agent**. A dialog opens and prompts you to upload a package.
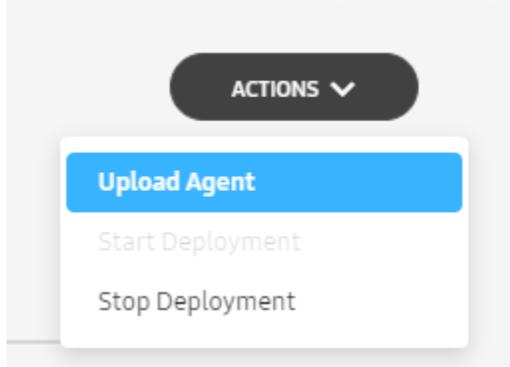
5. Click **BROWSE** and select the package file on your computer. Then, click **UPLOAD**.

Upload Agent ✕

Select an agent file you want to upload

	BROWSER

UPLOAD

The **Agent** screen refreshes with the new agent app information. Click **Actions** > **Start Deployment** to make your devices begin downloading and updating the new agent app.

Manually install the package

Alternatively, you can manually install the package on a device. This method is recommended if you want to test the agent app before deploying it to your full device fleet.

Before you begin, ensure you have the following prepared:

- A device capable of creating and copying a text file to a Samsung Galaxy device. For example, a computer, tablet, or phone.
- Your organization's server, connected to the local network
- A device secured by Samsung Knox, connected locally to the Knox E-FOTA On-Premises server

Create a configuration file

On the device you're using for text editing, you first need to create a file called efota_config. In a text editor of your choice, enter the URL of your on-premises server.

The on-premises server URL is defined by your organization and is used to access the Knox E-FOTA On-Premises admin console. The default server URL defined in the E-FOTA On-Premises agent app is http://192.168.10.10:8080/admin, but this URL can be customized in your efota_config file. If you're not sure what this URL is, contact the Samsung installation engineer who configured your Knox E-FOTA On-Premises server.

Important

If you specify a server URL in efota_config, the declared URL takes precedence over the default URL.

For example, the URL might be in one of the following formats:

- https://example-sec.fota.net:6443/admin/
- http://181.107.61.233:6380/admin/

Then, enter the SSL certificate password — if any — on the line underneath.

Next, save the file. Ensure the file isn't saved with a file extension. Your efota_config file should look like the following:

```
https://example.server.url.com/admin/
password_of_SSL_certificate
```

For example:

```
https://example-sec.fota.net:6443/admin/
mypassword12#
```

Alternatively, you can choose to set the server URL and password through an Android intent. To do so, see Configure your server URL and password through an Android intent.

Copy the configuration file to the device

There are two ways to get the configuration file on your device:

- Use your EMM to push the file to your device's Downloads folder, or
- Copy the file from your computer to the device's Downloads folder

If you're copying the file from your computer, connect the device to your computer through USB. In your computer's file explorer, locate the efota_config file and copy it to your device's Downloads folder. Make sure the agent app APK you received from your local Samsung representative is also present in the Downloads folder.

Install the Knox E-FOTA On-Premises app

On the device, navigate to the Downloads folder and tap the agent app APK to install it. After it's installed, launch the app.

Step 6 — Prepare firmware

Download firmware

Follow Use the Knox E-FOTA firmware downloader to download firmware for Knox E-FOTA On-Premises.

Upload firmware

To upload firmware to the Knox E-FOTA On-Premises server:

1. Click your account icon > **Settings**. The navigation pane refreshes with a new set of entries.
2. Go to **Versions**.
3. Click **Actions** > **Upload Versions**.

4. Under **Select path or directory** in the dialog, browse for the root folder of your downloaded BIN files to upload.
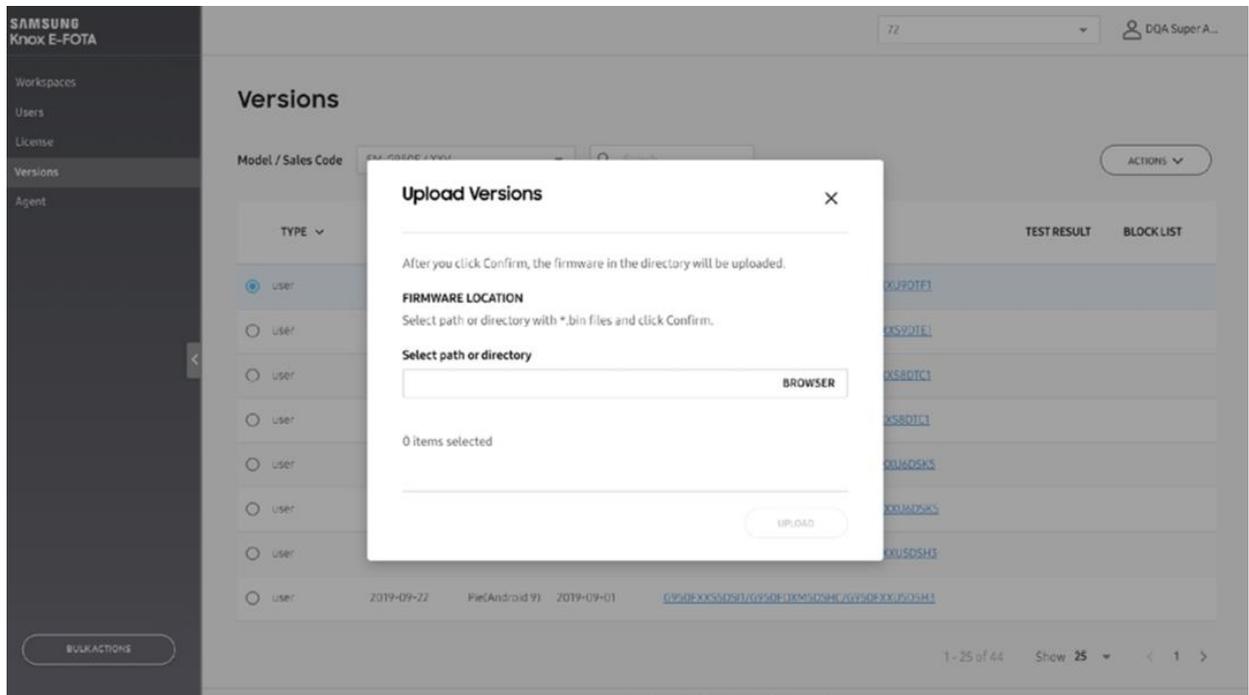
5. Click **Confirm** to select the folder.
6. Click **Upload** to add the firmware to your Knox E-FOTA On-Premises server.

To learn more about how you can better organize and track firmware versions, see Manage firmware versions.

Step 7 — Create and assign a campaign

Now you can create and assign a campaign to target devices.

1. Sign in to your Knox E-FOTA On-Premises server.
2. From the navigation pane, go to **Campaigns** and then click **Create Campaign**.
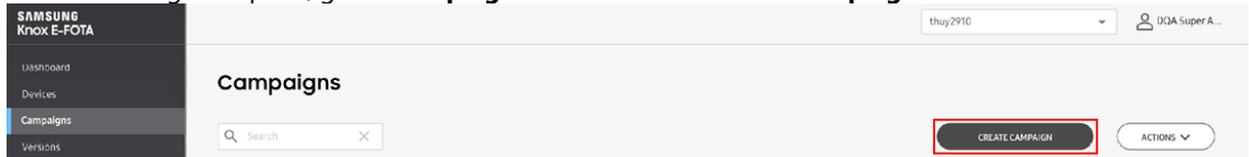
3. Fill in your **Basic info**:
   a. Enter a unique name for the campaign and a description of what the campaign is for.

   b. Click **NEXT**.

4. Fill in your **Target firmware**:

   a. Select the model and sales code corresponding to the target devices. Under **FIRMWARE VERSION**, select one of the following options:

Firmware version	Description
Latest firmware	Automatically push the latest firmware version to the corresponding devices.
Lock current firmware	Keep the current firmware version.
Select from firmware list	Select a firmware version to push to the corresponding devices.

   b. Select the target firmware on the next page and click **SELECT**. The campaign page opens.
   c. Click **ADD ANOTHER ROW** and repeat this step to assign as many firmware versions to the campaign as needed.

TARGET FIRMWARE

MODEL	SALES CODE	FIRMWARE VERSION	OS VERSION	SECURITY PATCH	DEVICES
SM-G950F ▾	XEU ▾	Latest firmware ▴	-	-	0

Latest firmware

Latest firmware (Tested)

Lock current firmware

Select from firmware list

ⓥ ADD ANOTHER ROW

    d. Click **NEXT**.

5. Fill in your **Policy**:

    a. Configure your **Network and speed**:

Field	Description
Download network	Select **Wi-Fi only** or **Any (Wi-Fi or Mobile)** as the network for devices to use for firmware downloads. • For **Any (Wi-Fi or Mobile)**, select **Allow download while roaming** to let firmware versions be downloaded while roaming.

NETWORK AND SPEED

Download network

○ Wi-Fi only

◉ Any (Wi-Fi or Mobile)
    ☐ Allow download while roaming

Max bandwidth	Allocate a maximum bandwidth per device for firmware downloads in MBit/s, where 0 MBit/s represents unlimited bandwidth.

    b. Configure your **Device condition**. Specify how much battery charge a device must have before it can begin installing the update. You can also prevent firmware installation on devices that aren't connected to a charging dock.

DEVICE CONDITION

Battery level for installation

Above 30% ▾

☐ Allow installation only when connected to charging dock

c. Configure **Postpone installation** if you want to allow the device user to postpone the installation. Set the maximum number of times they're allowed to postpone the installation before any pending firmware begins installing.

POSTPONE INSTALLATION

Set postpone policy for end users. Postpone count is reduced each time device checks-in to E-FOTA server. If this option is not selected, installation will be forced

| ☑ | 0 | times |

d. Click **NEXT** once you've configured all the policy settings.

6. Fill in your **Schedule**:

Field	Description
Campaign period	Set the dates when devices in the campaign can start to download and install the update.
Repeat on weekdays	Set the days of the week you want firmware updates to occur.
Installation hours	Set the timeframe within the campaign period when the devices in the campaign can start installing the update. This timeframe is based on the device's timezone. If you want firmware updates to install at any time of the day, set the firmware installation period to identical values: • **From** — 00 • **To** — 00 **Note** Devices will **start** installation during this period, but there's no guarantee that installation will end within this period.
Download hours	Set the timeframe within the campaign period when the devices in the campaign can start downloading the firmware. You can allow downloads to occur at one of the following periods: • **Same as installation hours**: Set the firmware download period to be the same as the firmware installation period. • **Anytime** — Allow firmware downloads at any time. • **Specific hours** — Set the firmware download period to be different from the firmware installation period.

SCHEDULE

Campaign period *

Start date

End date

Repeat on weekdays

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☑	☑	☑	☑	☑	☑	☑

Installation hours *

Firmware installation starts during these hours based on
device timezone. Installation may finish moments
beyond the specified end time.
Select same from/to hours for 24h operation (e.g. 0~0)

From   To

00   ▼   00   ▼

Download hours

◉ Same as installation hours

◯ Anytime

◯ Specific hours

From   To

00   ▼   00   ▼

7.   Click **CREATE**. The admin console creates the campaign and adds it to the **Campaigns** list. A
        notification confirms that the operation completed.

Assign an existing campaign to devices

To assign an existing campaign to devices:

1.   Go to **Devices**.
2.   Select the devices you want to assign.
3.   Click **ACTIONS** > **Assign Campaign**.
4.   Select a running campaign to assign the devices to.
5.   Click **ASSIGN**.

Manage devices

Like Knox E-FOTA, Knox E-FOTA On-Premises lets you manage devices directly from the console.

To view the device list:

1. Sign in to the Knox E-FOTA On-Premises admin console. Ensure you're in the correct workspace by verifying the workspace name in the upper-right corner of the console.
2. Go to **Devices**.

A device list opens with the following information:

Field	Description
DEVICE	The IMEI/MEID or serial number of the device.
ENROLLMENT	The enrollment status of the device, which can be one of the following: • Enrollment pending • Enrolled • Unenrollment pending • Not enrolled
SALES CODE	The country-specific code, or CSC, of the device.
FIRMWARE VERSION	The OS version the device is currently running. Hover over the version to display the full name.
CAMPAIGN	The Knox E-FOTA On-Premises campaign the device is currently assigned to. Hover over the campaign name to display the full name in a tooltip.
UPDATE STATUS	The download and installation status of the new firmware.
MODIFIED	The date the device information was last modified.
SOURCE	The method through which the device was uploaded.

> **Tip**
> See Manage devices in the Knox E-FOTA admin guide for descriptions of device actions and statuses.

Manage campaigns

The campaigns in Knox E-FOTA On-Premises have the same functionality as the campaigns in Knox E-FOTA.

To view your campaigns:

1. Sign in to the Knox E-FOTA On-Premises admin console. Ensure you're in the correct workspace by verifying the workspace name in the upper-right corner of the console.
2. In the left sidebar, click **Campaigns**.

A list of campaigns is displayed with their statuses, assigned devices, repeat frequency, start and end dates, and last modified date. Click a campaign name to view its details or modify it.

If there are no available campaigns, click **CREATE CAMPAIGN** in the upper-right corner to create one.

> **Tip**
> See Step 7 — Create and assign a campaign for detailed instructions on how to create a campaign.

Select a campaign and click the **ACTIONS** menu to access the following features:

Action	Description
Activate Campaign	Activates the campaign if it has been deactivated, and starts the firmware rollout.
Deactivate Campaign	Deactivates the campaign if it's currently active, and stops the firmware rollout.
Modify Campaign	Allows you to change the configured campaign policies, including the target firmware and campaign period.
Delete Campaign	Deletes the selected campaign.

View the activity log

The activity log displays a list of activities that were performed in the admin portal. Use these logged events to troubleshoot issues and track user actions.

To view the activity log:

1. Log in to the Knox E-FOTA On-Premises admin portal. Ensure you're in the correct workspace by verifying the workspace name in the upper-right corner of the console.
2. In the navigation sidebar, click **Activity Log**.
3. Filter the list as needed by doing any of the following:
   - Click **Show all** and select **Last 7 days** or **Last 30 days**.
   - Filter the activity log by **Name** (of the admin), **Category**, **Event**, or a combination of those.
   - Sort the list by **Date**.
   - Enter a keyword in the search bar.
4. To download the full activity log, click **DOWNLOAD AS CSV** in the upper-right corner of the screen.

Update firmware through Ethernet

With Knox E-FOTA On-Premises, you can also update the OS version of a device through a USB Ethernet connection. To do so, ensure you have:

1. A network connection
2. A LAN cable
3. A USB-C Ethernet adapter

First, you need to set up your campaign to support the Ethernet connection:

1. Sign in to the Knox E-FOTA On-Premises admin portal. Ensure you're in the correct workspace by verifying the workspace name in the upper-right corner of the console.
2. Go to **Campaigns** and create a new campaign or modify an existing one.
3. On the **Create campaign** or **Modify campaign** screen, in the **POLICY** tab and under **Download network**, select **Any (Wi-Fi or Mobile)**.
4. If creating a new campaign, click **CREATE,** or if you're modifying an existing one, click **UPDATE**.

After the device receives the new campaign details:

1. Connect the LAN cable to the Wi-Fi access point and the USB-C Ethernet adapter.
2. Plug the USB-C Ethernet adapter in to the device.

A notification appears on the device confirming the Ethernet connection, and it can now download and install the OS update according to the campaign policy.

Use the Knox E-FOTA firmware downloader

To help you manage firmware versions, Knox E-FOTA On-Premises supports a firmware downloader that allows you to select and download firmware versions of your choice.

The Knox E-FOTA firmware downloader uses two JSON files — a scenario JSON file, which contains a list of the firmware versions currently hosted on your Knox E-FOTA On-Premises server, and an input JSON file, which contains a list of target firmware versions you can then import into your server. You need both these files to download select firmware versions.

Prerequisites

Before you can start using the Knox E-FOTA firmware downloader, you first need to:

1. Export a scenario JSON file from the Knox E-FOTA On-Premises console
2. Get the firmware downloader
3. Get an input JSON file from the Knox Admin Portal

If your PC is behind a proxy server, you also need to enter the proxy server host IP and proxy server port later.

Export a scenario JSON file

If you've just installed Knox E-FOTA On-Premises, make sure your devices are successfully enrolled before following these steps. Otherwise, you won't be able to export the proper firmware version information.

To get a scenario JSON file:

1. On the Knox E-FOTA On-Premises console, click **Versions**.
2. On the **Versions** page, click **ACTIONS** > **Download Versions Scenario**.

The scenario JSON file begins downloading to your PC.

Get the firmware downloader

To get the Knox E-FOTA firmware downloader:

1. Sign in to the Knox Admin Portal.
2. On the Knox Admin Portal homepage, under Knox E-FOTA On-Premises, click **Get started**.
3. On the page that opens, click **Download Firmware Files**.
4. Enter your Knox E-FOTA On-Premises license key, then click **CONTINUE**.
5. Next to the firmware downloader tooltip, click **DOWNLOAD HERE**.

← Back to Knox E-FOTA On-Premises Resources   DOWNLOAD FIRMWARE FILES

EFOTA1-UJOOQ4

ⓘ Looking for Knox E-FOTA On-Premises Firmware Downloader? DOWNLOAD HERE ⤓			CHANGE LICENSE KEY	GENERATE REQUEST
REQUEST DATE	**SCENARIO JSON FILE**	**STATUS**	**EXPIRATION**	**FIRMWARE** ⓘ
MM/DD/YYYY	filename3.json	• Complete	MM/DD/YYYY	DOWNLOAD ⤓
MM/DD/YYYY	filename2.json	• Complete	MM/DD/YYYY	DOWNLOAD ⤓
MM/DD/YYYY	filename4.json	• Complete	MM/DD/YYYY	DOWNLOAD ⤓

*Firmware requests expire 14 days after you submit your request.

After the firmware downloader is saved to your PC, open it.

Get an input JSON file

Before following these steps, make sure you exported the scenario JSON file. The input JSON file also requires the scenario JSON file so that the firmware delivery servers can prepare the corresponding firmware versions for your devices.

To download the input JSON file:

1. Sign in to the Knox Admin Portal.
2. On the Knox Admin Portal homepage, under Knox E-FOTA On-Premises, click **Get started**.
3. Click **Download Firmware Files**.
4. Enter your Knox E-FOTA On-Premises license key, then click **CONTINUE**.
5. A page is shown with your license key. Click **GENERATE REQUEST**.

EFOTA1-UJOOQ4

ⓘ Looking for Knox E-FOTA On-Premises Firmware Downloader? **DOWNLOAD HERE** ⬇   (CHANGE LICENSE KEY) (**GENERATE REQUEST**)

REQUEST DATE	SCENARIO JSON FILE	STATUS	EXPIRATION	FIRMWARE ⓘ
MM/DD/YYYY	filename3.json	• Complete	MM/DD/YYYY	DOWNLOAD ⬇
MM/DD/YYYY	filename2.json	• Complete	MM/DD/YYYY	DOWNLOAD ⬇
MM/DD/YYYY	filename4.json	• Complete	MM/DD/YYYY	DOWNLOAD ⬇

*Firmware requests expire 14 days after you submit your request.

6. In the dialog that opens, click **BROWSE** and select the scenario JSON file.
7. Click **GENERATE REQUEST**.

The console notifies you that your request was successfully submitted, and the input JSON file is ready for download after your request is completed.

Download specific firmware versions

The following steps assume the prerequisites outlined previously are met.

To download specific firmware versions using the Knox E-FOTA firmware downloader:

1. Launch the Knox E-FOTA firmware downloader.
2. Under <input.json>, click **Browse** and select the input JSON file you downloaded from the Knox Admin Portal.
3. Under **Target firmware**, click **SELECT FIRMWARE**.
4. A dialog opens with the firmware list specified by the input JSON file. Select the firmware versions you want to host in Knox E-FOTA On-Premises, then click **SELECT**.
5. Under <scenario.json>, click **Browse** and select the scenario JSON file you exported from the Knox E-FOTA On-Premises console.
6. Under **Origin firmware**, click **SELECT FIRMWARE**.
7. A dialog opens with the firmware list specified by the scenario JSON file. Select a firmware version equal to or lower than the lowest firmware version that your devices are running.
8. Under **Save directory**, click **Browse** to choose a location for your firmware download.
9. (Optional) If your PC is behind a proxy server, enter the **Proxy host** and **Proxy port**.
10. Click **DOWNLOAD**.

The target firmware versions are then downloaded to the location you selected, and can be imported to your Knox E-FOTA On-Premises server.

Settings menu overview

While Knox E-FOTA On-Premises has a similar feature set to its cloud counterpart, Knox E-FOTA, certain functionalities are extended to accommodate on-premises setups. These features are located in a separate menu on the Knox E-FOTA On-Premises console.

> **Note**
> Only Super Admins can access the **Settings** menu with the on-premises features.

To navigate to the Knox E-FOTA On-Premises **Settings** menu:

1. Sign in to the Knox E-FOTA On-Premises admin console.
2. Click your account icon.
3. In the menu that's shown, click **Settings**.

The console view updates to show a new sidebar with the following features exclusive to Super Admins:

Feature	Description
Workspaces	Manage separate admin consoles within one Knox E-FOTA On-Premises instance.
Users	View and edit user roles and information.
License	Upload licenses and view their information.
Versions	Upload and view firmware versions.
Agent	Manage Knox E-FOTA On-Premises agent app versions.

To return to the main console view, click the **Knox E-FOTA** logo in the top-left corner of the console.

Manage workspaces

Unique to Knox E-FOTA On-Premises, workspaces allow larger organizations to divide their teams or business units into separate admin consoles. You can easily switch between workspaces using the dropdown menu to the left of your username.

As a Super Admin, you can view and manage a list of your organization's workspaces:

1. Sign in to the Knox E-FOTA On-Premises admin console.
2. Click your account icon.
3. In the menu that's shown, click **Settings**.
4. The left sidebar refreshes with a new set of tabs. Click **Workspaces**.

The following workspace actions are also available to you through the **ACTIONS** menu:

Action	Description
Add Workspace	Select this option to launch a popup where you can enter the name and description for a new workspace. Click **Save** to confirm.
Assign Users	Select the checkbox next to a workspace in the list to enable this option in the menu. A dialog opens with a list of all users in the Knox E-FOTA On-Premises instance, across all workspaces.
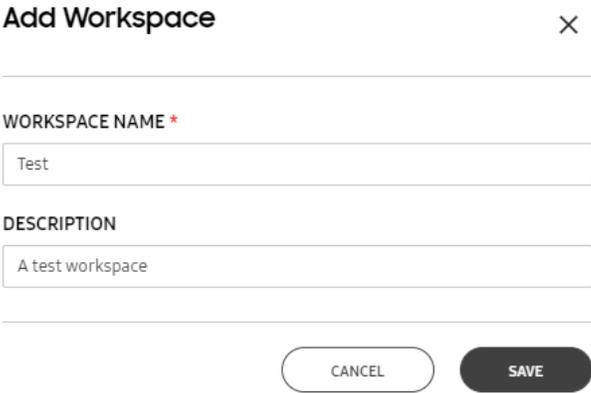
Action	Description

Assign Users

	NAME ↓↑	ID ↓↑	ROLE ⌄ ↓↑	JOIN DATE ↓↑
☑	svmc02@s.com	svmc02@s.com	Super-Admin	2020-08-26
☑	svmc03@s.com	svmc03@s.com	Super-Admin	2020-08-26

Select the checkboxes next to the users you want to assign to the workspace, then click **ASSIGN**.

Modify Workspace	Opens a dialog that allows you to edit the workspace name and description.
Delete Workspace	Select this option and click **Delete** in the confirmation popup to delete a workspace.
Download Workspace as CSV	Downloads a CSV file with the information of the selected workspaces.

Add, edit, and delete users

With Knox E-FOTA On-Premises, Super Admins can manage users and their roles directly from the admin portal.

To access the users list:

1. Sign in to the Knox E-FOTA On-Premises admin console.
2. Click your account icon.
3. In the menu that's shown, click **Settings**.
4. The navigation sidebar pane refreshes with a new set of tabs. Click **Users**.

The users list is then displayed, which includes the name, ID, role, status, and join date of each user.

Add a user

1. On the **Users** screen, click **ACTIONS** > **Add User**.
2. A popup is shown, prompting you to enter the user's details. Fill in the required fields as shown, then click **SAVE**.

After saving, the new user is added to the list. The user's role, assigned password and status can be changed at a later date.

Edit a user

1. On the **Users** screen, select the checkbox next to the user you want to modify.
2. Click **ACTIONS** > **Edit User**.
3. Select one of the available options:

Action	Description
APPROVE	If the user's status is **Pending**, click **APPROVE** to change their status to **Active** and grant them console access.
PASSWORD MODIFY	Set a new password for the user. Depending on how your Knox E-FOTA On-Premises instance is configured, a password length policy may apply. By default, the minimum length for a password is 8 characters, and the maximum length is 12.
EDIT	Change the user's name, role, status, or time zone.

Delete a user

1. On the **Users** screen, select the user you want to delete.
2. Click **ACTIONS** > **Delete User**.
3. In the confirmation popup that appears, click **PROCEED**.

The user is then removed from the list and can no longer access the Knox E-FOTA On-Premises instance.

Manage licenses

Knox E-FOTA On-Premises uses special licenses that can be obtained through the corresponding self-service **Resources** page. For steps on how to generate and add a license, see Step 2 — Add a license in the **Get started** tutorial.

To view your license information:

1. Sign in to the Knox E-FOTA On-Premises admin console.
2. Click your account icon.
3. In the menu that's shown, click **Settings**.
4. The navigation sidebar refreshes with a new set of tabs. Click **License**.

The **License** page is displayed, with a list of the total workspaces and devices. As one license services all the workspaces within your Knox E-FOTA On-Premises instance, you can review this list to see how your license seats are distributed.

Underneath the workspace list, the Knox E-FOTA On-Premises license information is shown:

Field	Description
Purchased	The total number of seats on your license.
Assigned	The number of seats currently consumed by devices.
Remaining	The number of seats available to be consumed by devices.

Your license key, its type, status, start date and expiry date are listed below the seat counts. You can also view your license expiration date in the welcome message on your **Dashboard**.

> **Important**
> To prevent unexpected workflow issues, please renew or extend your license before its expiry date. If your license expires:
>
> • You can still sign in to the console and view or retrieve information, but you won't be able to perform any campaign-related actions.
> • You can still delete and unenroll devices from the console. If you unenroll a device, it reconnects to the B2C FOTA server and continues to receive regular firmware updates.

Manage firmware versions

To better organize and track firmware versions, Knox E-FOTA On-Premises includes a versions list that allows you to record firmware test results and block certain versions.

To view the versions list:

1. Sign in to the Knox E-FOTA On-Premises admin console.
2. Click your account icon.
3. In the menu that's shown, click **Settings**.
4. The navigation pane refreshes with a new set of entries. Click **Versions**.

The version list is then displayed with the following information:

Field	Description
TYPE	Indicates whether the firmware is intended for deployment on devices (**user**), or for testing (**dummy**). See Create a test campaign for more details.
OPEN DATE	The date the firmware version was publicly released.
OS VERSION	The Android version that corresponds to the firmware version.
SECURITY PATCH	The date the security patch was publicly released.
FIRMWARE VERSION	The full name of the firmware version. Click the name to view the firmware details, which includes a description and specific device information.

Above the list, you can filter by device **Model / Sales Code** or search by firmware version ID to quickly identify the firmware versions you need.

Click the **ACTIONS** menu to access more features:

Field	Description
Upload Versions	Select and upload new firmware versions from your PC.
Mark as Tested	Adds an icon to the **TEST RESULT** column to indicate that the firmware version was successfully tested for compatibility with business apps. When creating a campaign, selecting **Latest firmware (Tested)** as the target version allows you to update the latest tested firmware version from the **Versions** menu without modifying the campaign settings.
Unmark from Tested	Removes the icon from the **TEST RESULT** column.
Add to Blocklist	Locks the firmware version, preventing it from being downloaded and installed on devices.

Field	Description
Remove from Blocklist	Unlocks the firmware version and allows it to be downloaded and installed on devices again.
Download Versions Scenario	Downloads a JSON file that contains device version scenario information, including a list of changes between the current firmware version and the target version.

View the agent app version

The **Agent** tab provides an overview of the Knox E-FOTA On-Premises package version, or agent, that is to be or is currently deployed to your devices.

This screen displays the following details:

Field	Description
Deployment	The deployment status of the agent, either **Started** or **Stopped**.
Package Version	The version number of the agent.
Package Name	The full name of the agent.
Release Date	The date the agent version was made publicly available.

Click the **Actions** menu to view more options:

Action	Description
Upload Agent	Opens a popup to upload an agent file. Click **BROWSER** to launch your PC's file explorer and select the file. Then, click **UPLOAD**.
	The **Agent** screen is then refreshed with the new agent information.
Start Deployment	Prompts the devices to start downloading and installing the agent the next time they poll for updates.
Stop Deployment	Stops the devices from downloading and installing the current agent version.

Configure your server URL and password through an Android intent

When you download and install the Knox E-FOTA On-Premises agent app, you can choose to set the server URL and password through an Android intent. To do so, refer to the following sample code:

```java
// package name, action
final String PACKAGE_NAME   = "com.samsung.android.efotaagent";
final String ACTION_CONFIG_MODE = PACKAGE_NAME + ".CONFIG_MODE";
final String ACTION_SERVER_URL = PACKAGE_NAME + ".SERVER_URL";
final String ACTION_BKS_PASSWORD = PACKAGE_NAME+".BKS_INFO";

// set Config mode
final String CONFIG_MODE_EXTRA = "MODE";
final String CONFIG_MODE_FILE = "file";
final String CONFIG_MODE_INTENT = "intent";
// set server URL
final String SERVER_URL_EXTRA = "URL";
final String SERVER_URL = "https://example.server.url.com/admin/";
// set server password
final String BKS_INFO_EXTRA = "BKS";
final String BKS_PASSWORD = "password_of_server";
// set config mode to intent
sendBroadcast(new Intent()
        .setAction(ACTION_CONFIG_MODE)
        .putExtra(CONFIG_MODE_EXTRA, CONFIG_MODE_INTENT)
        .setPackage(PACKAGE_NAME)
        );
// set URL by intent
sendBroadcast(new Intent()
        .setAction(ACTION_SERVER_URL)
        .putExtra(SERVER_URL_EXTRA, SERVER_URL)
        .setPackage(PACKAGE_NAME)
        );
// set password by intent
sendBroadcast(new Intent()
        .setAction(ACTION_BKS_PASSWORD)
        .putExtra(BKS_INFO_EXTRA, BKS_PASSWORD)
        .setPackage(PACKAGE_NAME)
        );
// set config mode to file (efota_config)
sendBroadcast(new Intent()
        .setAction(ACTION_CONFIG_MODE)
        .putExtra(CONFIG_MODE_EXTRA, CONFIG_MODE_FILE)
```

```
    .setPackage(PACKAGE_NAME)
    );
```

To learn more about how to download and install the Knox E-FOTA On-Premises agent app, see Step 5 — Download and install the agent app.

Knox E-FOTA On-Premises 23.12 release notes

Support for Red Hat Enterprise Linux 9.2

Starting with the 23.12 release, Knox E-FOTA On-Premises now supports Red Hat Enterprise Linux 9.2 in addition to 8.4.

Support for Red Hat Enterprise Linux High Availability Add-on

Knox E-FOTA On-Premises previously only supported high availability technologies on Ubuntu. Additionally, high availability technologies were only supported with an application layer through dfm-core and dfm-console.

Starting with the 23.12 release, Red Hat Enterprise Linux High Availability Add-on is now fully supported with HAProxy, DB, and minIO storage servers. The full-stack High Availability Add-on is also supported.

Improvements to polling cycles of firmware versions

Before the 23.12 release, you had to wait for the next polling cycle — configured to either every hour or every 24 hours — before the device could proceed to the next step in a campaign.

To help you deploy firmware at a shorter cadence, the waiting time between steps can now be configured. Updates now shorten previously established polling cycles and instead update whenever available.

During sequential updates, devices also reboot and update accordingly. For the first installation of a sequential update, a firmware installation notice displays for 30 seconds by default. The waiting time can be adjusted to any value from 1 to 7200 seconds in the dfm_conf.json file.

Tooltip for invalid firmware

Previously, there was no way to verify whether enrolled devices had official Samsung firmware installed.

Knox E-FOTA On-Premises 23.12 can now detect unofficial firmware versions. If the admin console detects unofficial firmware, a warning icon displays beside the firmware version, and a tooltip shows when you hover over the corresponding firmware version on the **Devices** page.

Default server URL in the client app

From Knox E-FOTA On-Premises 23.12 onward, the client app can now work with a predefined server URL. If there's no efota_config file configured after installation, the Knox E-FOTA On-Premises agent app sets a default server URL — http://192.168.10.10:8080/admin.

If you uninstall the agent app from a device and reinstall it afterward, any custom server URLs aren't kept. However, the agent app will still work with the default server URL.

If you've configured an efota_config file, the server URL specified takes precedence over the default server URL.

See Create a configuration file for more information.

Knox E-FOTA On-Premises 23.04 release notes

Improvements to the Knox E-FOTA firmware downloader

To reduce the number of firmware versions you need to download for your on-premises server, the Knox E-FOTA firmware downloader now allows you to select target firmware versions to download for your on-premises server.

The latest list of available firmware versions can be obtained as a input.json file from the Knox Admin Portal homepage. You can browse for this file in the firmware downloader, as well as a scenario.json file containing the current firmware versions of your enrolled devices.

After uploading these two files, you can then select specific firmware versions for download. Note that if your PC is behind a proxy server, you also need to enter your proxy server host IP and port before you can download the firmware.

Support for a certificate password field in configuration file

The Knox E-FOTA On-Premises agent now allows you to input required passwords through an additional field in the efota_config file. If you're familiar with the Android API, you can also add an Android intent listener to define the password.

See Step 5 — Download and install the agent app for more details.

Improvements to service performance

Starting with the 23.04 release, Knox E-FOTA On-Premises now automatically evenly polls device groups for updates. If you allocated a maximum bandwidth per device in the campaign policy, the agent ensures it meets the download speed limit by stopping and starting the firmware download as needed.

Enhancements to bulk device deletion

Previously, Knox E-FOTA On-Premises didn't require additional confirmation from you when bulk deleting devices.

With the 23.04 release, when you delete devices in bulk, a dialog asks you to confirm before the operation begins.

Enhancements to device tags

Prior to the 23.04 release, Knox E-FOTA On-Premises only supported device tags up to 10 characters long. When the maximum device tag length was reached, no error message would display in the console.

To allow for easier differentiation between devices, device tags up to 45 characters long are now supported. Tag limitations are also dynamically shown as you enter the device tag — for example, an error message notifies you when you enter a tag 46 characters long.

Knox E-FOTA On-Premises 22.09 release notes

Support for high-availability clusters on Ubuntu OS

With the 3Q 2022 release, Knox E-FOTA On-Premises for the Ubuntu platform now supports high-availability (HA) clusters. Current Ubuntu installations of Knox E-FOTA On-Premises can be upgraded to enable HA support.

> **Important**
> Only the Ubuntu installation package supports HA.

For the latest installation and upgrade guides, refer to Knox E-FOTA On-Premises installation and upgrade guides.

Knox E-FOTA On-Premises 22.06 release notes

Support for Redhat Enterprise Linux (RHEL) 8.4

Previously, the Knox E-FOTA On-Premises installation package only supported RHEL 8.3. The RHEL 8.3 installation ISO image has since been removed from the project's official download center.

With this release, the Knox E-FOTA On-Premises installation package now supports RHEL 8.4.

Knox E-FOTA On-Premises 22.04 release notes

Updates to password hash algorithm

Previously, Knox E-FOTA On-Premises used the bcrypt password hash algorithm.

Starting with this release, passwords are now hashed with the PBKDF2 algorithm to offer more flexible password security measures for high-security enterprises.

Benefits of the PBKDF2 algorithm include:

- Longer salt length and key length — 128 bits or higher
- Higher key iteration count — 10,000 or higher
- Lightweight pseudorandom function (PRF) — HMAC-SHA256 or HMAC-SHA512

Password length configuration

To comply with enterprise security regulations, Samsung installation engineers can now set a minimum and maximum length for user passwords. By default, the minimum password length is set to 8 characters, and the maximum is set to 12. The minimum password length that an installation engineer can set is 8-20 characters. The maximum length can be 12-30 characters.

> **Important**
> Existing user passwords are not affected by this change. However, when an old password is updated, the new password must conform to the current policy.

Knox E-FOTA On-Premises 21.09 release notes

Support for Redhat Enterprise Linux 8

This Knox E-FOTA On-Premises release adds support for Redhat Enterprise Linux (RHEL) 8. This allows a wider range of support for RHEL from version 8 onwards. RHEL 8 offers container tools to support containerized applications, and also provides compatibility across new hardware architectures and environments.

Knox E-FOTA On-Premises 21.06 release notes

Support for firmware updates through Ethernet connection

This Knox E-FOTA On-Premises release adds a new feature that allows IT admins to update the firmware of devices through a USB Ethernet connection. This feature requires the use of a LAN cable and a USB-C Ethernet adapter.

See Update firmware through Ethernet for more details.