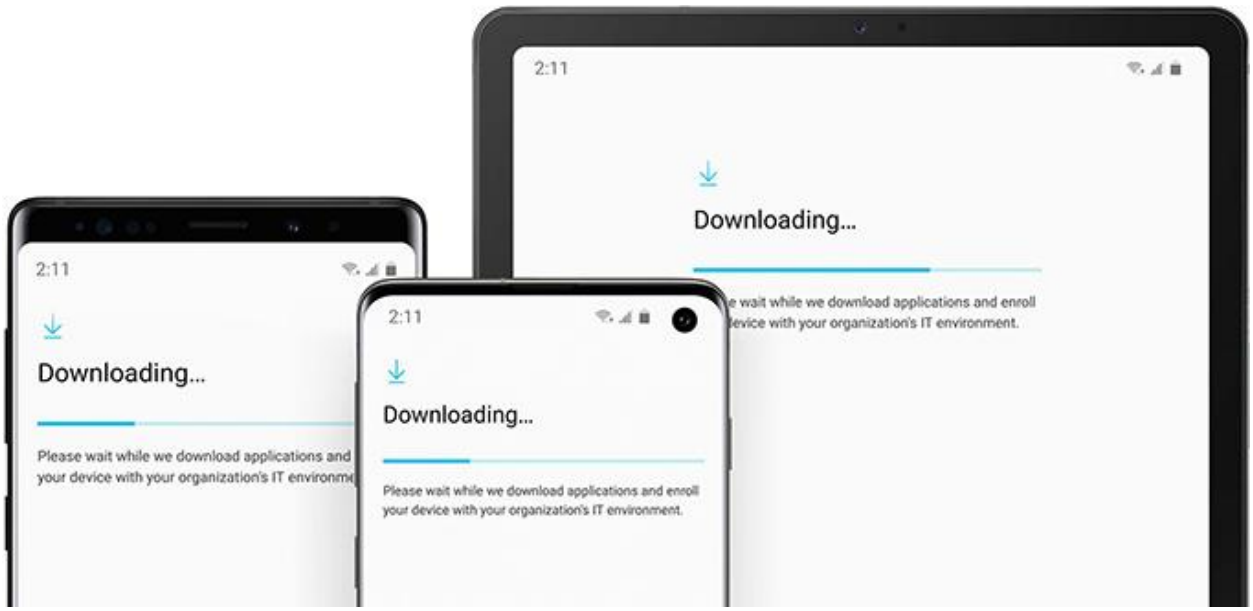
Knox E-FOTA On-Premises admin guide

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.
- **Knox E-FOTA On-Premises portable** — Use Knox E-FOTA On-Premises on a portable device such as a laptop and bring it to your business sites. With this feature, you don't have to manage individual Knox E-FOTA On-Premises servers at each site.

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 console

Console server URL

To access the Knox E-FOTA On-Premises 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/.

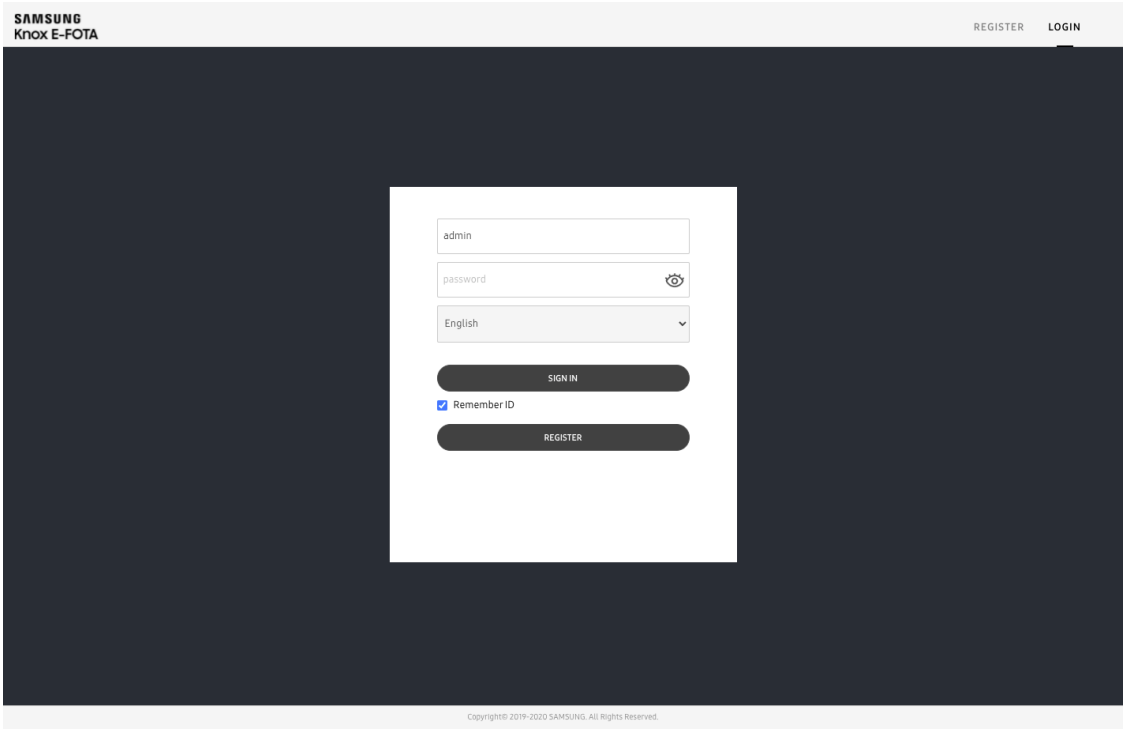
If you don't know your server URL, contact your Samsung installation engineer.

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.

Tutorial progress

You've completed 1 of 7 steps!

Step 2 — Add a license

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

> **Important**
> License keys can't be reused once they've been used to generate a license file.

Use these commands to get the hardware serial number of your server machine:

On Windows Powershell:

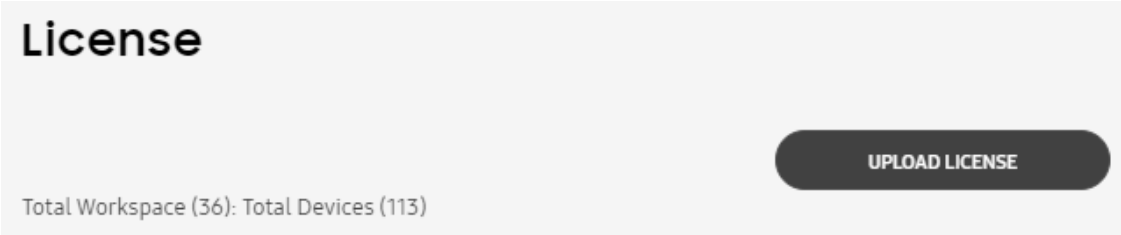
```
Get-WmiObject -class Win32_Bios | Out-String -stream | Select-String -Pat
tern Serial
```

On Linux:

```
sudo dmidecode -t2 | grep Serial
```

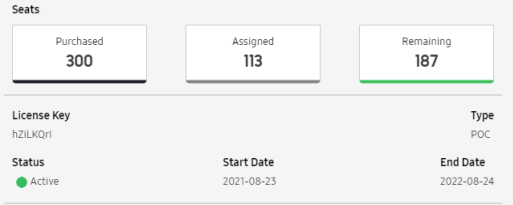
Once you've prepared your generated license file, you can add the license:

1. In 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.

Tutorial progress

You've completed 2 of 7 steps!

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 assignment.

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**.

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**.

Tutorial progress

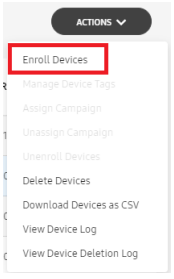
You've completed 3 of 7 steps!

Step 4 — Enroll devices

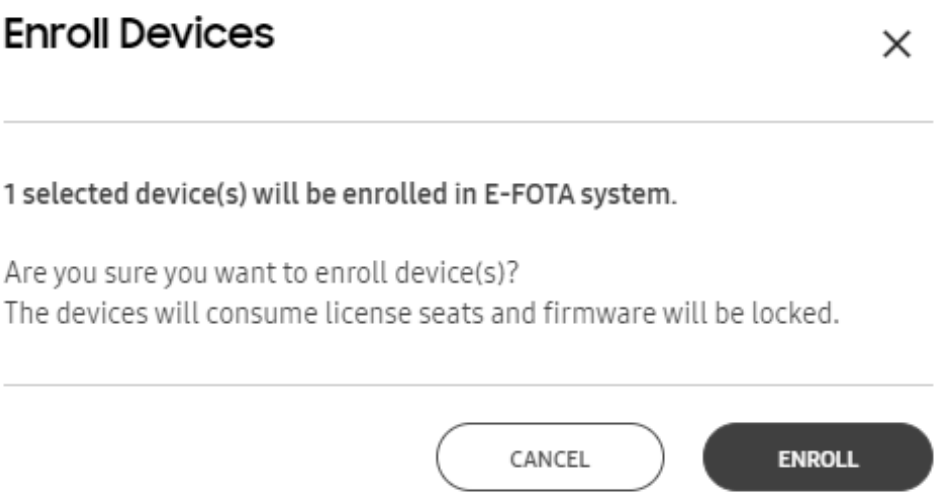
If you chose not to enroll devices when adding them in the previous step, you can do that now by selecting specific devices for enrollment through the device list. This action is only available for devices in the **Not enrolled** state.

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.

Tutorial progress

You've completed 4 of 7 steps!

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 four ways to install the agent app on your devices:

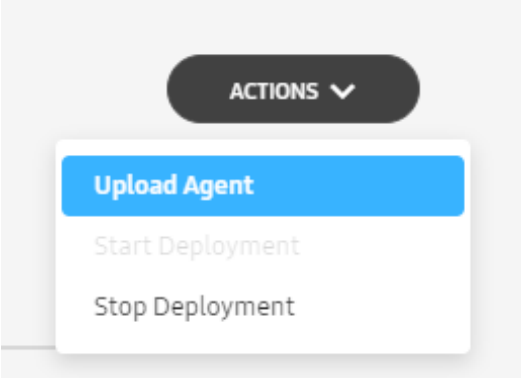
- Update the Knox E-FOTA On-Premises agent app by uploading the package through the console
- Manually install the package
- Install the client through your EMM
- Download the client through a QR code

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

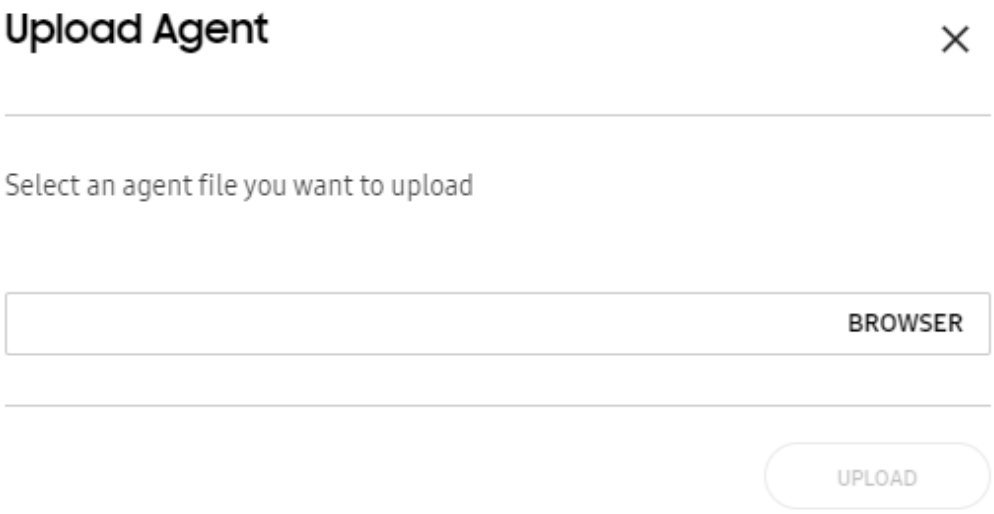
> **Important**
> Updating the Knox E-FOTA On-Premises agent app by uploading it to the console is only supported if the agent app is already installed and running on your devices.

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

1. Sign in to the Knox E-FOTA On-Premises 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**.



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

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 entire 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 Knox E-FOTA On-Premises server, connected to your local network.
- The TLS certificate `efota.pem` file used to connect to your Knox E-FOTA On-Premises server.
- If you're using mutual TLS, follow the steps in Use mutual TLS to generate your `efota_client.pem` file.
- A device secured by Samsung Knox, connected to your local network.

Create a configuration file

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

The on-premises server URL is defined by your organization and is used to access the Knox E-FOTA On-Premises 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/

If you're using mutual TLS, provide the password for the encrypted private key in the `efota_config` file, on the line after the server URL.

Next, save the file. Ensure the file isn't saved with a file extension. Your `efota_config` file should look similar to this:

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

Transfer the files to the device

Transfer the `efota_config` file and the TLS certificate `efota.pem` file to your device.

There are two ways to get these files on your device:

- Use your EMM to push the files to your device's Downloads folder, or
- Copy the files 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 the TLS certificate file and copy it to your device's Downloads folder. If you're using mutual TLS, copy your `efota_client.pem` file to the Downloads folder as well. 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. The Knox E-FOTA On-Premises app loads the server URL from `efota_config` and the TLS certificate `efota.pem` file to connect to your on-premises server.

Install the client through your EMM

If you're using Knox E-FOTA On-Premises alongside an EMM, you can use your EMM to push the Knox E-FOTA On-Premises app to your devices.

Your local Samsung representative provides you with the APK for the Knox E-FOTA On-Premises app. Follow your EMM's documentation to add an internal app and push it to your fleet of devices.

The Knox E-FOTA On-Premises app supports a managed configuration, which lets you configure connection and authentication details needed for the app to communicate with your Knox E-FOTA On-Premises server. Follow your EMM's documentation on how to configure an app's managed configuration.

The managed configuration has the following fields:

- `server_url` — The URL of your Knox E-FOTA On-Premises server.
- `pem` — Your server's TLS certificate.
- `client_cert_pem` — (Only used for mutual TLS) Client certificate used by clients to authenticate themselves to your server.
- `client_key_pem` — (Only used for mutual TLS) Encrypted private key used by clients for signing.
- `client_pem_password` — (Only used for mutual TLS) Password for the encrypted private key.

For details on mutual TLS, see how to Set up mutual TLS.

Test the managed configuration

You may want to test the Knox E-FOTA On-Premises app's managed configuration on individual devices before deploying it to your device fleet with your EMM. You can do this

with Google's TestDPC to update managed configurations for apps on the device. Here is an example showing how to set an app's managed configuration with TestDPC.

1. Deploy and setup TestDPC on the device.
2. Open TestDPC, and tap on **Managed configurations**.
3. On the dropdown, select the Knox E-FOTA On-Premises app, and tap **LOAD MANIFEST RESTRICTIONS**. The app's managed configuration opens with fields to set the server URL and TLS certificate.
4. Tap on `server_url` and enter the URL of your Knox E-FOTA On-Premises server.
5. Tap on `pem` and paste the contents of your pem file with your TLS certificate information.
6. Tap **SAVE**.
7. Open the Knox E-FOTA On-Premises app and verify that the server URL is correct and the app is able to connect to your server.

For more information, please see Google's Android Managed Configuration Sample.

Download the agent app through a QR code

> **Important**
> Before you can download the agent app from Knox E-FOTA On-Premises to your devices, you must first upload the agent app to your Knox E-FOTA On-Premises server. You can do this on the agent page through the settings menu.

You can download the agent app onto your devices using a QR code:

1. From the settings menu, click **Agent**.
2. Click the package version to show the QR code.
3. Scan the QR code with your device to download the agent app.
4. On the device, navigate to the **Downloads** folder and tap the agent app APK to install it. If you encounter a warning, tap **OK** to install the app anyway.

The QR code is valid for 7 days. You can generate another QR code by refreshing the **Agent** page and clicking the package version again.

Tutorial progress

You've completed 5 of 7 steps!

Step 6 — Prepare firmware

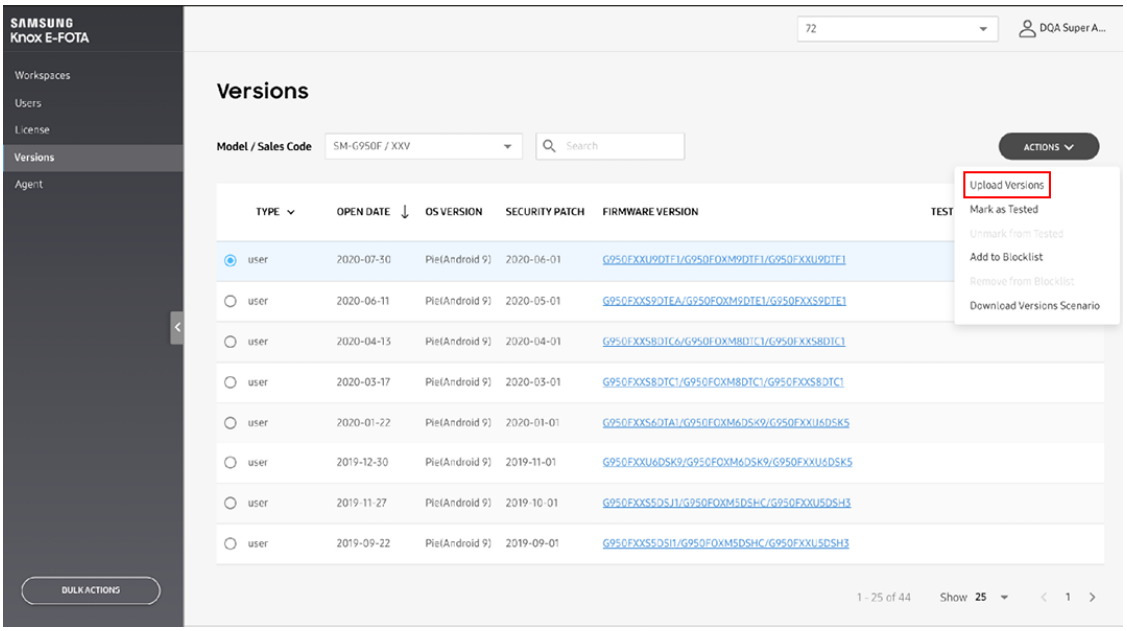
Download firmware

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

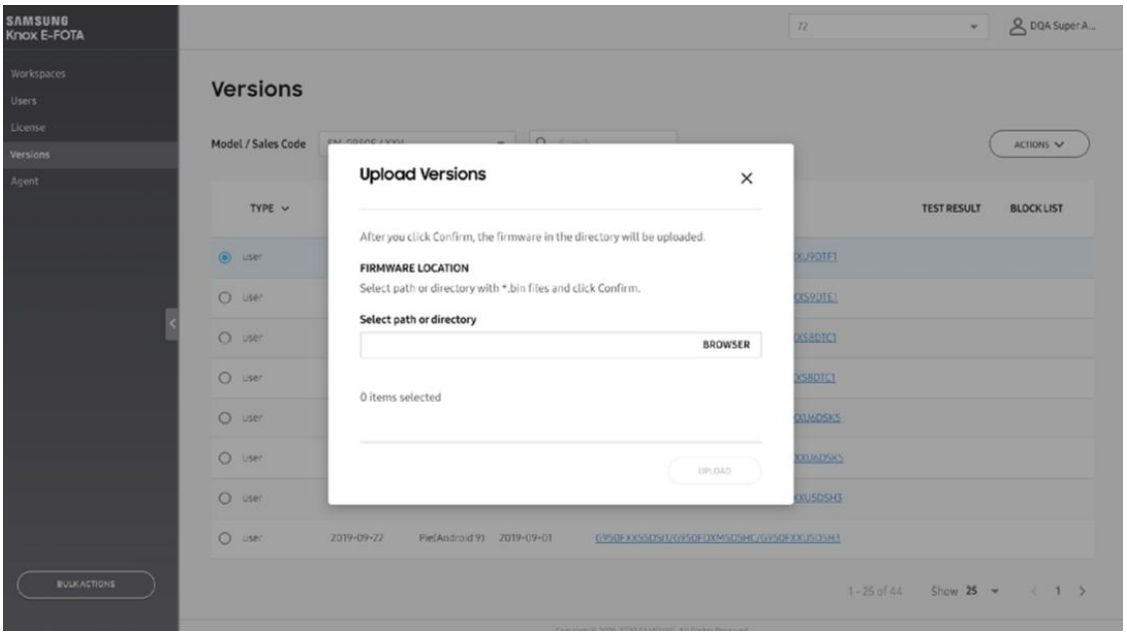
Upload firmware

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.

Tutorial progress

You've completed 6 of 7 steps!

Step 7 — Create and assign a campaign

To apply a firmware update to devices, you must create a campaign and specify which firmware version is pushed to your devices, and configure policies that control firmware download and installation.

1. Sign in to your Knox E-FOTA On-Premises server.
2. Go to **Campaigns** and then click **Create Campaign**.

Fill in the following campaign information.

Basic info

Enter a unique name for the campaign and a description of what the campaign is for.

Target firmware

Each row of the **Target firmware** table represents a target device group and the firmware version policy applied to those devices.

1. Select the model and sales code combination that specifies your target devices. Under **FIRMWARE VERSION**, select one of the following options:
    - **Latest firmware** — Automatically push the latest firmware version to your target devices.
    - **Lock current firmware** — Keep the current firmware version.
    - **Select from firmware list** — Select a specific firmware version to push to your target devices. Only the firmware versions that are compatible with your selected combination of model and sales code are available.

- Click **ADD ANOTHER ROW** to target another set of devices and assign them to a firmware version policy.

Policy

You can define policies that govern firmware download and installation.

Network and speed

- **Download network** — Select which networks devices can use to download firmware.
    - **Wi-Fi only** — Only download firmware over Wi-Fi.
    - **Any (Wi-Fi or Mobile)** — Allow firmware downloads over Wi-Fi and mobile networks. This option also allows downloads over VPNs and private networks. To allow firmware downloads while roaming, select **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.

Device condition

You can specify conditions required for firmware installation.

- Specify how much battery charge a device must have before it can begin installing the update.
- Only install firmware if the device is connected to a charging dock.

Postpone installation

Enable this option to allow devices users to postpone firmware installation. You can set the maximum number of times they're allowed to postpone the installation before any pending firmware begin to install.

Schedule

You can define a schedule for firmware download and installation.

- **Campaign period** — Set the date range when devices in the campaign can start to download and install the update.
- **Repeat on selected days** — Set the days of the week you want firmware updates to occur.
- **Installation hours** — Set a time window that determines when during the day devices can begin installing firmware. 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 a time window that determines when during the day devices can start downloading 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 a firmware download period that's different from the firmware installation period. - **Gradual campaign rollout** — Configure a gradual campaign rollout that deploys in randomized daily batches instead of all devices at once. You can control the rollout rate as a percentage of total devices. This feature allows you to monitor device updates progressively, so you can discover and troubleshoot firmware

issues before they spread to all devices. - Changes to either the rollout rate, target firmware version, or campaign status during gradual rollout will reset the rollout start date of all assigned devices. - Rolling out a campaign to devices newly assigned during the gradual rollout doesn't reset the rollout start date of devices that were already assigned the campaign, preventing any delay in pushing firmware updates.

Activate your campaign

Once you've finished entering your campaign information, click **CREATE**. You new campaign appears on the **Campaigns** list.

To assign the campaign to your devices:

1. Go to the **Devices** page.
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**.

Tutorial progress

Congratulations, you've completed the tutorial! You're now set up to use Knox E-FOTA On-Premises.

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 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:

- **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
- **Model** — The device's model.
- **Sales Code** — The country-specific code (CSC) of the device.
- **Firmware Version** — The firmware version currently running on the device. Hover over the version to display the full name.
- **Tags** — Any tags assigned to this device.
- **Campaign** — The Knox E-FOTA On-Premises campaign the device is currently assigned to. Hover over the campaign name to display the full name.
- **Update Status** — The download and installation status of the new firmware.
- **OS version** — The Android OS version currently running on the device.
- **Source** — The method through which the device was uploaded to Knox E-FOTA On-Premises.

Perform device actions

Click the **Actions** dropdown to perform the following actions:

- **Enroll devices** — Enroll the selected devices to Knox E-FOTA On-Premises.
- **Manage device tags** — Add and remove tags for this device.
- **Assign campaign** — Assign the selected devices to a campaign.
- **Unassign campaign** — Unassign the selected devices from their campaigns.
- **Unenroll devices** — Unenroll devices from Knox E-FOTA firmware management. These devices now receive B2C FOTA updates, and no longer consume a license seat.
- **Delete devices** — Delete the selected devices from Knox E-FOTA On-Premises.
- **Download devices as csv** — Exports a list of devices in CSV format for external analysis or record-keeping.
- **View device log** — View device event logs for status updates and errors.
- **View the device deletion log** — Displays logs related to deleted devices, including timestamps and reasons for deletion.

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 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. For details, see Create and assign a campaign.

Click the **Actions** dropdown to perform the following actions:

- **Activate** — Activates the campaign if it has been deactivated, and starts the firmware rollout.
- **Deactivate** — Deactivates the campaign if it's currently active, and stops the firmware rollout.
- **Modify** — Allows you to change the configured campaign policies, including the target firmware and campaign period.
- **Duplicate** — Creates a copy of the selected campaign. All settings are replicated except for unique identifiers, and the new campaign is created in an inactive state, so you can modify settings before activation.
- **Delete** — 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.

- 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, do as follows:

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 import into your server. You need both these files to download 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

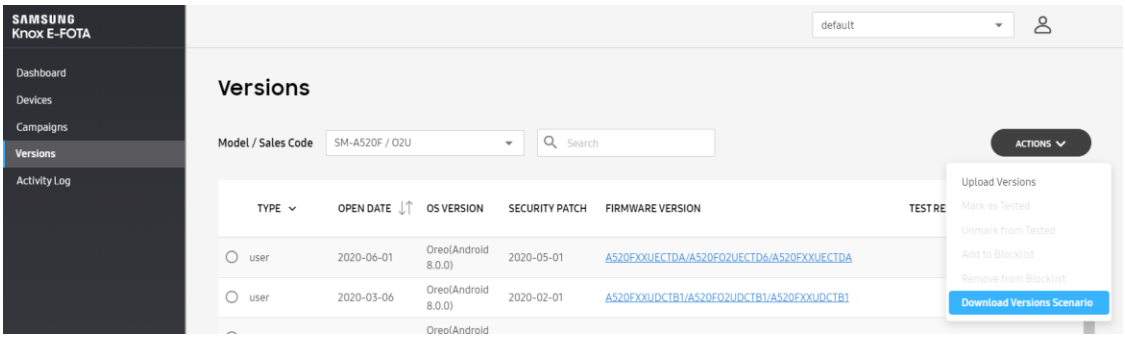
If your PC is behind a proxy server, you also need to enter the proxy server host IP and proxy server port later.

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**.



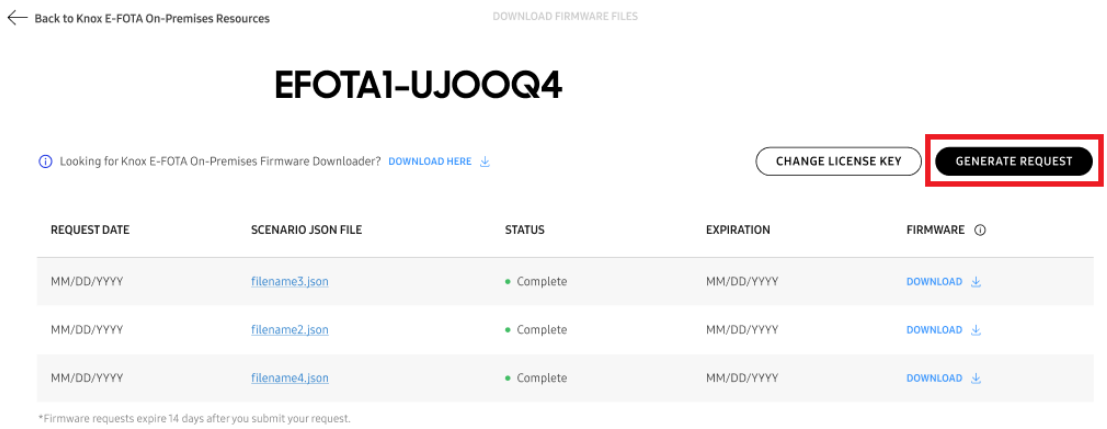
The scenario JSON file begins downloading to your PC.

Get an input JSON file

Before following these steps, make sure you've already exported the scenario JSON file. The input JSON file 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**.



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

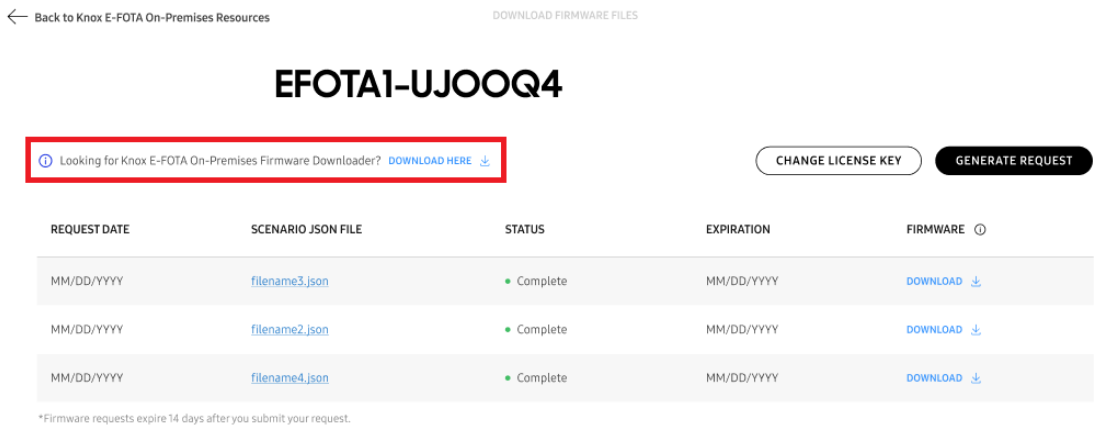
7. Click **GENERATE REQUEST**.

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

Get the firmware downloader

Before following these steps, make sure you've already uploaded a scenario JSON file. The firmware downloader link only appears after you upload your first scenario 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. 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**.



The firmware downloader is saved to your PC.

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. You can select multiple origin firmware versions.
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. (Optional) Check **Encrypt firmware files with password** to encrypt downloaded firmware files with AES-256 encryption. Set a password for the encrypted files, which is used to decrypt them when you're ready to import them to your Knox E-FOTA On-Premises server.
11. 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.

Decrypt firmware files

If you previously encrypted your firmware files when downloading them, you must decrypt them before you can import them to your Knox E-FOTA On-Premises server.

1. Launch the Knox E-FOTA firmware downloader.

2. At the bottom of the page, click **Decrypt Files**.

3. In the **Input files** field, click **Browse** and select a folder of firmware files to decrypt.

4. Enter the password you previously set when encrypting these files.

5. Click **Start Decryption** to decrypt all firmware files in the selected folder.

Decrypted firmware files can now be imported to your Knox E-FOTA On-Premises server.

Check for firmware updates using app intent

You can now send intents from your app to trigger the Knox E-FOTA agent to check for firmware updates. If an update is available, and firmware download and installation conditions are met, the device performs the firmware update.

See the following example to implement this on your app:

```
Intent intent = new Intent()
        .setAction("com.samsung.android.efotaagent.POLLING")
        .setComponent(new ComponentName("com.samsung.android.efotaagent","com
.samsung.android.efotaagent.receiver.ThirdPartyReceiver"));
sendBroadcast(intent);
```

Settings 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 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 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 consoles. You can easily switch between workspaces using the dropdown menu to the left of your username.

As a super admin, you can set the workspace to **All workspaces** to view information across all workspaces on the **Devices**, **Campaigns**, and **Activity log** pages. Downloading devices and activity logs while **All workspaces** is selected downloads information across all workspaces as a single CSV.

> **Note**
> While All workspaces is selected, you can only view and export information. You can't perform actions to manage Knox E-FOTA settings and features across all workspaces.

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 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 entries. Click **Workspaces**.

Click the **Actions** dropdown to perform the following actions:

- **Add Workspace** — Create a new workspace with a name and description.

- **Assign Users** — Select a workspace from the list, and assign users to that workspace. You can select users from a list of all users on Knox E-FOTA On-Premises across all workspaces.
- **Modify Workspace** — Edit the workspace name and description.
- **Delete Workspace** — 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 admin can manage users and their roles directly from the admin portal.

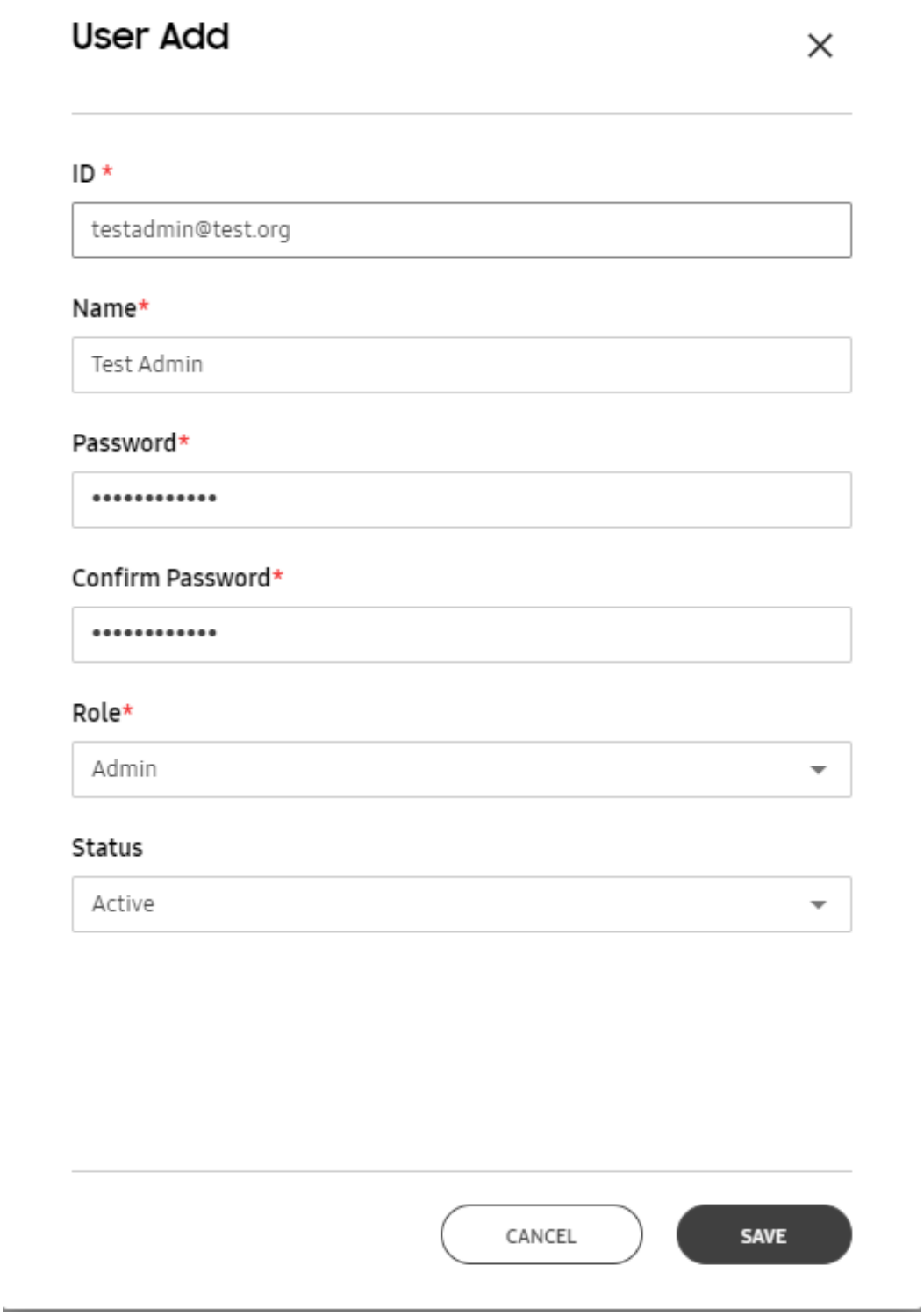
To access the users list:

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

The version list displays, and you can filter by device **Model / Sales Code** or search by firmware version ID to quickly identify the firmware versions you need. The list shows the following information for each firmware version:

- **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.

Click the **Actions** dropdown to perform the following actions:

- **Upload firmware versions** — Select and upload new firmware versions from your PC. You can upload firmware to Knox E-FOTA On-Premises even if it's not compatible with any devices enrolled on your server.
- **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 tested icon from the **Test result** column.
- **Add to Blocklist** — Locks the firmware version, preventing it from being downloaded and installed on devices.
- **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.
- **Delete all** — Deletes all firmware files from your Knox E-FOTA On-Premises server.

View the agent app version

The **Agent** tab provides an overview of the Knox E-FOTA On-Premises agent app on your Knox E-FOTA On-Premises server. The Knox E-FOTA On-Premises agent app manages the firmware on your devices, see how to Download and install the agent app.

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:

- **Upload Agent** — Upload a new agent version to your Knox E-FOTA On-Premises server. Click **BROWSER** to launch your PC's file explorer and select the file. Then, click **UPLOAD**.
- **Start Deployment** — Prompts your devices to start downloading and installing the agent the next time they poll for updates.
- **Stop Deployment** — Stops your devices from downloading and installing the current agent version.

Knox E-FOTA On-Premises portable

Knox E-FOTA On-Premises provides a portable solution, which allows you to install Knox E-FOTA On-Premises on a laptop and bring it to your business sites. With this solution, you don't have to install and maintain Knox E-FOTA On-Premises servers at each site. You can use one server to manage firmware for your entire device fleet, which may span across multiple business sites.

Currently, Knox E-FOTA On-Premises portable is only available as a Windows Hyper-V virtual machine package.

Prerequisites

- Enable Hyper-V
  - Windows 10
  - Windows 11
- Set up a network interface with IP address `192.168.10.10` on your laptop. This address should be accessible to your fleet of devices to download firmware updates.

Install and run Knox E-FOTA On-Premises portable

1. Download the compressed Knox E-FOTA On-Premises portable Hyper-V image and the support files.
2. From the support files, decompress the `Knox E-FOTA licenseApp_pkg_win.zip` file and run the `Knox E-FOTA licenseApp reg.bat` file as an administrator to install the license service.
3. From the support files, run the `Knox E-FOTA Portable NW reg.bat` file as an administrator to configure network settings.
4. Decompress the Hyper-V virtual machine image.
5. Import the virtual machine using Hyper-V Manager.
6. Run the virtual machine.
7. From the support files, ensure that `cert.crt` and `add_cert.bat` are in the same folder, then run `add_cert.bat` as an administrator.

You can now access your Knox E-FOTA On-Premises portable server through its URL:

`https://192.168.10.10:8080/admin/`

This URL is configured in `Knox E-FOTA Portable NW reg.bat`.

Set up mutual TLS

To use mutual TLS, you must create the client certificate and its private key. Enter the following commands to set up your certificate for mutual TLS:

1. Create your private key:

   ```
   openssl genrsa -out key.pem 4096
   ```

2. Create your certificate:

   ```
   openssl req -x509 -new -key key.pem -out cert.pem -days 365
   ```

3. Encrypt your private key:

   ```
   openssl pkcs8 -topk8 -in key.pem -out key.pem -v2 aes-128-cbc
   ```

4. If you're going to manually transfer the certificates to your devices, combine the two files to create `efota_client.pem`. If you're going to use the Knox E-FOTA On-Premises agent's managed configuration, skip this step.

   ```
   cat key.pem cert.pem > efota_client.pem
   ```

5. Create a copy of `cert.pem` named `client.pem` for HAProxy:

   ```
   copy cert.pem client.pem
   ```

6. Add the settings below to your HAProxy config file `haproxy.cfg` to install the client certificate and only allow authenticated clients:

```
frontend fe_web
  bind :80
  bind :443 ssl crt /usr/local/etc/haproxy/example-sec-
fota.net.pem ca-   file /usr/local/etc/haproxy/client.pem
verity optional

  # monitoring uri
  monitor-uri /health

  http-request capture req.hdr(Host) len 100

  acl acl_dfm_device path_reg ^/dfm/device/v1/*
  acl has_client_cert ssl_fc_has_crt eq 1
  http-request deny if acl_dfm_device !has_client_cert
  use_backend dfmCoreBackend if acl_dfm_device
```

7. To apply the client certificate to your devices, you can either manually transfer the certificate file or push the certificate information through the Knox E-FOTA On-Premises agent's managed configuration.

   a. If you're manually transferring the certificate file, enter the password used to encrypt the private key in the `efota_config` file on the line after the server URL, then push the `efota.pem`, `efota_client.pem`, and `efota_config` files to the **Download** folder on your devices. Ensure that the agent app apk is also in the **Downloads** folder when you run it to install the app. For details about installing the agent app, see Download and install the app.

   b. If you're using the Knox E-FOTA On-Premises agent's managed configuration, fill in the following configuration fields:

      - `client_cert_pem` — Paste the contents of `cert.pem` to push the client certificate to your devices.
      - `client_key_pem` — Paste the contents of `key.pem` to push the encrypted private key to your devices.

- `client_pem_password` — Enter the password used to encrypt your private key in step 3.

For details about the managed configuration, see how to Install the client through your EMM.

Knox E-FOTA On-Premises 26.06 release notes

Version	Release date
1.0.1.12	June 9th, 2026

New

Encrypt downloaded firmware files

You can now encrypt firmware files when using the Knox E-FOTA firmware downloader. Check **Encrypt firmware files with password** and enter a passcode to encrypt downloaded firmware binaries with AES-256 encryption, protecting them during transfer to your on-premises server. When you're ready to import the firmware, use the Knox E-FOTA firmware downloader to decrypt the files by entering the passcode.

For details, see Use the Knox E-FOTA firmware downloader.

Knox E-FOTA On-Premises 25.12 release notes

Version	Release date
1.0.1.11	December 29, 2025

New

Gradual campaign rollout

You can now configure gradual campaign rollouts that deploy to randomized daily batches instead of all devices at once. You can control the rollout rate and monitor device updates

progressively, allowing you to discover and troubleshoot firmware issues before they spread to all devices.

For details, see Create and assign a campaign.

Duplicate existing campaigns

You can now duplicate active or completed Knox E-FOTA campaigns, saving you time on repetitive configurations. When copying a campaign, all settings are replicated except for unique identifiers, and the new campaign is created in an inactive state, allowing you to modify settings before activation.

For details, see Manage campaigns.

Enhanced polling interval configuration

You can now configure the default polling interval for campaigns on Knox E-FOTA On-Premises. This gives you greater control over how frequently the system performs various checks and updates.

For details, see our Installation and upgrade guides.

Delete firmware files

You can now remove outdated or unnecessary firmware files from the Knox E-FOTA On-Premises console. This feature allows you to easily clean up server storage, without needing to do it on the command line which may require root-level permissions.

For details, see Manage firmware versions.

Update

Support for RHEL 9.6

Knox E-FOTA On-Premises now supports Red Hat Enterprise Linux (RHEL) version 9.6. This includes both standalone and high availability (H/A) deployment configurations.

UI enhancements for on-premises agent

The Knox E-FOTA On-Premises agent can now display in landscape mode, which provides enhanced usability especially for tablet devices. The agent also supports dark mode, offering additional personalization options for device users.

Enhanced firmware update tracking

The Knox E-FOTA On-Premises agent now shows the current number of completed updates and total number of updates required to complete the firmware update, along with the estimated time remaining for each step in the firmware update process. This information is available on the installation reminder screen and the progress notification bar.

Additional information on Devices page

The **Devices** page now shows ten columns, so you can review more device information at once. Additionally, you can now sort devices by **Security Patch** dates and organize **Workspace** names for better data management.

For details, see Manage devices.

Enhanced certificate management

The Knox E-FOTA On-Premises agent no longer generates a default `efota.pem` file in the device's **Download** folder when no URL is configured. This update resolves potential conflicts between self-signed certificates and the default `efota.pem` certificates.

Support for mutual TLS

Knox E-FOTA On-Premises now supports mutual TLS (mTLS), ensuring that client-server connections are authenticated both ways. You can push the client certificate and encrypted private key manually, or through the Knox E-FOTA On-Premises agent's managed configuration.

For details, see Install the agent app, and how to Set up mutual TLS.

Knox E-FOTA On-Premises 25.05 release notes

Version	Release date
1.0.1.10	May 27, 2025

New

View information across all workspaces

Super admins can now set the workspace to **All workspaces**, which displays device, campaigns, and activity log information across all workspaces. Downloading devices and activity logs while **All workspaces** is selected downloads information across all workspaces as a single CSV.

> **Note**
> When **All workspaces** is selected, you can only view and export information. You can't perform actions to manage Knox E-FOTA settings and features across all workspaces.

For details, see how to Manage devices and workspaces.

Check for firmware updates using app intent

You can now trigger your device to check for firmware updates using app intents. When your app emits the intent, the Knox E-FOTA agent polls your Knox E-FOTA On-Premises server for any pending firmware updates. App triggered update checks can only be performed once every 30 seconds.

For details, see how to Check for firmware updates using app intent.

Improvements to the firmware downloader

You can now select multiple origin firmware versions from your scenario JSON file on the Knox E-FOTA firmware downloader. You can also upload firmware to Knox E-FOTA On-Premises even if it's not compatible with any device enrolled on your server.

For details, see how to Use the Knox E-FOTA firmware downloader.

Updates

Support for HTTPS on Knox E-FOTA On-Premises portable

Knox E-FOTA On-Premises portable now supports HTTPS for network communication. You can install self-signed TLS certificates on your server, and push TLS certificates in the Knox E-FOTA agent's managed configuration, so your devices can securely communicate with your server.

Support for Ubuntu 24.04 LTS

Knox E-FOTA On-Premises now supports Ubuntu 24.04 LTS.

Knox E-FOTA On-Premises 24.12 release notes

Version	Release date
1.0.1.9	December 26, 2024

New

Enhancement to the Knox E-FOTA On-Premises app

Previously, the URL and TLS certificate needed for the app to connect to your Knox E-FOTA On-Premises server could only be configured with a config file.

With this release, the Knox E-FOTA On-Premises app now supports a managed configuration, which allows you to configure the URL and TLS certificate when you push the app to your devices with your EMM. This feature means that you no longer need a separate config file for your devices to connect to your Knox E-FOTA On-Premises server.

For more information, see how to Install the client through your EMM.

Updates

Updated Java version for Knox E-FOTA On-Premises

With this release, we are updating the Java version used in Knox E-FOTA On-Premises to ensure optimum security for your assets.

Knox E-FOTA On-Premises 24.07 release notes

Version	Release date
1.0.1.8	June 28, 2024

New

Knox E-FOTA On-Premises portable

The 24.07 release introduces a portable solution for Knox E-FOTA On-Premises. This solution allows you to install Knox E-FOTA On-Premises on a laptop with a Hyper-V virtual machine and bring it to your business sites, so you don't have to install and maintain Knox E-FOTA On-Premises servers at each site.

For more information, see Knox E-FOTA On-Premises portable.

Download the Knox E-FOTA client through a QR code

With this release, you can download the Knox E-FOTA On-Premises client on your devices through a QR code in the Knox E-FOTA On-Premise console. This feature allows you to quickly set up Samsung devices with Knox E-FOTA On-Premises, streamlining the initial setup for your fleet of devices.

For more information, see Download and install the agent app.

Updates

Improvements to license installation

The 24.07 release introduces improvements to license installation.

- License keys can't be reused once the license file is generated.
- Licenses are now activated with the hardware serial number of the motherboard instead of the MAC address of the device.

Support for Virtual A/B updates

With this release of Knox E-FOTA On-Premises, you can now deploy virtual A/B firmware updates to Samsung Galaxy A55 5G devices running Android 14 or higher. With Virtual A/B, the device seamlessly rolls back a firmware update if it fails to boot. Furthermore, firmware can be installed in separate dynamic partitions to allow both download and installation to occur in the background, and to ensure faster reboot speeds. Support for other device models will be available in future releases.

You can configure when the installation occurs. Once the installation is complete, the device reboots automatically.

See the Android Virtual A/B overview documentation to learn more about virtual A/B updates.

Download firmware over VPNs or private networks

With this release of Knox E-FOTA On-Premises, you can download firmware on your fleet of devices over VPNs and private networks if the **Download network** campaign setting is set to **Any**.

You can configure this when you create a campaign.

Knox E-FOTA On-Premises 24.03 release notes

Hotfixes

Hotfix for firmware updates through VPN

You can now bypass the network restrictions that block devices from downloading firmware when connected to a VPN. To remove the restrictions in your campaign, set **Download network** to **Any (Wi-Fi or Mobile)**.

For more information on configuring campaigns, see Step 7 — Create and assign a campaign.

Knox E-FOTA On-Premises 23.12 release notes

Version	Release date
1.0.1.7	December 14, 2023

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 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

Version	Release date
1.0.1.6	April 28, 2023

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 highe
- Higher key iteration count — 10,000 or highe
- 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.