Knox Cloud Services Overview for managed devices

Samsung Knox offers a variety of cloud solutions to assist with enterprise device management. Our cloud solutions are complimentary to IT asset management solutions and have native integrations with leading MDM, UEM, and SIEM solutions.

Samsung Knox products include:

Samsung Knox Product	**Use Cases**	**Device Management Type**
Knox Mobile Enrollment	Device set up and EMM enrollment	Corporate owned managed devices
Knox Mobile Enrollment Advanced	Device set up and EMM enrollment with loss prevention	Corporate owned managed devices
Knox E-FOTA	Firmware management	Corporate owned managed devices
Knox Asset Intelligence	Enterprise device productivity, Security telemetry	Corporate owned managed device
Knox Manage	Unified device management	Managed devices (iOS, MacOS, Windows, Android)
Knox Remote Support	Remote access to a single device for troubleshooting	Corporate owned managed devices

All Samsung Knox cloud solutions are SOC2 certified and have supplementary controls for enterprises requiring additional compliance support (e.g., General Data Protection Regulation (GDPR) requirements). For more information, see Knox security certifications and guidance.

Managed software updates

It's important for enterprise customers to have a strategic software rollout plan and the controls to execute their plans. To assist with this process, Android Enterprise and Samsung Knox offer various tools to help understand the security risks associated with an out-of-date device, when software updates are available, and controls to manage firmware over the air (FOTA).

Controlling the rollout of software updates allows IT admins to:

- Homogenize the firmware versions and capabilities of deployed device models.
- Carry out interoperability or compatibility testing with in-house or proprietary servers, apps, and endpoint settings.
- Ensure that known issues are patched before the deployment of major firmware version updates.
- Perform field tests of new firmware and software on a subset of devices before mass deployment.
- Force the use of firmware versions that have been validated to meet industry certification or regulation requirements.

Android Enterprise's managed system updates feature offers foundational controls for firmware management. Using these controls, many enterprises can achieve a robust firmware management plan without sacrificing productivity. Through Android Management APIs (AMAPIs), EMM solutions can:

- Enforce software updates and allow the user to temporarily delay an update and schedule it for a later time.
- Delay operating system (OS) upgrades and maintenance releases for up to 60 days.
- Allow firmware download over Wi-Fi only.

Beyond Android Enterprise controls, a wide range of EMM partners support Samsung's firmware management features by integrating firmware management with other asset management activities. IT admins can use these tools to test and deploy software updates in a consistent and low-risk manner. By using EMM solutions, enterprises can restrict users from loading unauthorized firmware through their devices or USB-connected computers.

Through the Knox platform, enterprises can also:

- **Disable automatic firmware updates**: IT admins can prevent users from using Android settings to enable or disable automatic firmware updates.

- **Disable all OTA updates**: IT admins can prevent users from using Android settings to enable or disable all software updates. This includes updates for firmware, security patches, bug fixes, and apps.
- **Disable USB-connected updates**: IT admins can prevent users from booting into **Download Mode** and manually installing a software update. This includes updates through the Odin, Kies, and Smart Switch update tools.

Samsung Knox firmware controls are complimentary to Android Enterprise managed system updates. While effectively managing firmware on Samsung devices doesn't require Knox cloud software or controls, there are numerous benefits for leveraging the Knox platform's added capabilities.

Knox E-FOTA

Samsung developed Knox Enterprise Firmware Over-the-Air (E-FOTA) to enable enterprises to efficiently manage mobile infrastructure, reduce support costs, and save time. With Knox E-FOTA, IT admins can ensure that device users can't independently update to unsupported firmware versions, preventing issues that could negatively impact employee productivity, support costs, and data security.

With Knox E-FOTA, enterprises can control device software updates in the following ways:

- **Select the target firmware version**: Knox E-FOTA provides a list of firmware options and their corresponding details based on your device model. You can set the target Android OS version or update to the latest version.
- **Force target firmware version update onto select devices**: Enterprises can push new firmware to specific devices to ensure interoperability and compatibility with proprietary systems and apps. This prevents any operational or performance issues that may arise due to incompatibility.
- **Schedule updates during non-peak work times and granular network resource management**: Knox E-FOTA offers setting granular control over when to download the update, and how. This ensures update scheduling prevents any interruptions to employee productivity. Additionally, Knox E-FOTA enables enterprises to manage network bandwidth restrictions through a set of configuration options and deploy the updates entirely on-premises.
- **Mass deploy the target firmware version**: Mass deployment eliminates the issue of software version fragmentation, and there's no need to support multiple legacy firmware versions for every deployed device. You can ensure that all devices are updated to the desired firmware version, regardless of their current firmware version.

Recommended update cadence for users & enterprises

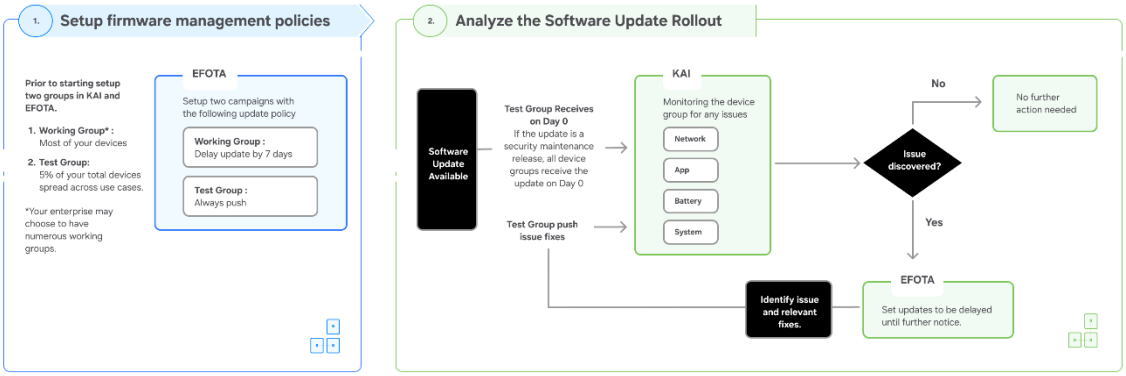
Choosing the best update cadence for your enterprise requires alignment with your cybersecurity strategy. It's important to have a clear understanding of your goals and compliance requirements ahead of deciding the update cadence for your devices.

To effectively manage Samsung mobile devices, it's important to keep the following objectives in mind:

- Patching as soon as possible is a priority to reduce security risk.
- Maintain a control group and a test group for rolling out device updates (non-security).
- Ensuring device stability after a patch requires a feedback loop.

As described in Security patch vs maintenance patch, there are numerous types of software updates released. Maintenance releases and operating system upgrades can potentially impact dependent software and systems that interface with the device. However, security updates don't carry this risk and are purely beneficial. It's important to not delay these types of updates and roll them out as soon as possible.

For handling non-SMR related updates, we encourage our users to leverage Knox Asset Intelligence and Knox E-FOTA.



For OS upgrades and One UI updates, enterprises can enroll in the OS beta program and get a head start on the integration process. This can help you make necessary changes to in-house applications and configurations prior to deploying to a large-scale software update.

When participating in the OS beta program, Knox E-FOTA and Knox Asset Intelligence will not be available for use.

For more information, please contact your Samsung Sales Representative.

Knox Asset Intelligence Security Center

To help Samsung Knox customers better manage their security risks, SecOps Teams can easily track the security posture of every device in their fleet with powerful insights like the total number of devices with vulnerabilities detected, which devices have outdated security patches, and which devices pose the highest security risk to the organization.

The Knox Asset Intelligence Security Center provides clear, granular mapping of device vulnerabilities, as well as routine attestation to track the health of enrolled Samsung Knox endpoints. SecOps Teams, in collaboration with IT admins, can prioritize security patching efforts based on security risks reported by the Knox Asset Intelligence Security Center.

For example, if an organization has a mixed device fleet consisting of XCover Pro and Galaxy S22 models, the Security Center can report the total number of vulnerabilities affecting each *specific* device model and *omit* any devices that already have the latest security patches deployed, thus making it easier for SecOps and IT admins to identify only the devices that are at risk. IT admins can then launch Knox E-FOTA to deploy the correct security patch for each model, ensuring that devices are updated in the most effective way, with the least amount of business disruption.

The Security Center provides 3 benefits for enterprises:

- Granular mapping of vulnerabilities to individual device models
- Daily health attestation through Knox Device Health Attestation
- Knox Security Events & Log for Security Operations Centers

Vulnerability management

As many purpose-fit devices are deployed across the enterprise, the ability to manage security risks becomes increasingly complex due to differences in device vulnerabilities and patch cadence. Without an understanding of each device's hardware and drivers, enterprises have no way to accurately assess the risks posed by certain chipset vulnerabilities, or know which devices were—or could have been—exploited.

Security Center leverages Samsung's software and hardware supply chain to directly map vulnerabilities to devices. By hooking directly into our software supply chain, we can granularly track which vulnerabilities have an impact on each specific binaries, and specify which builds patch each vulnerability. This becomes especially important for devices impacted by Samsung Vulnerabilities and Exposures (SVEs) not bound to the Android Security Patch Level (ASPL).

Given the diverse set of Samsung devices across the globe, many device families often have differing hardware depending on the region. For example, a Galaxy S24 in the US has a Qualcomm chipset, while EU models have the Exynos chipset. This difference in

chipset can have a significant impact on how vulnerabilities get patched, as one vulnerability reported in one chipset may not be reported in the other, despite being the same device model. In other words, a Galaxy S24 with a Qualcomm chipset will have different vulnerabilities than a Galaxy S24 with an Exynos chipset. With the Knox Asset Intelligence Security Center, you can trust that the vulnerabilities reported are the actual vulnerabilities that impact the models in your fleet, right down to the root hardware and software level.

Daily attestation

Each device enrolled in the Security Center gets attested on a daily basis to verify its security posture. If devices are offline (no internet connection) or powered off during the attestation request, these devices are categorized as **Unknown** in the Security Center dashboard. If attestation is successfully carried out, devices are categorized as either **Good** or **Bad**. Devices with a **Bad** attestation result should be investigated immediately, as this is a strong indicator of compromise.

Connecting Security Center to your SOC

To allow security telemetry to be gathered from your devices, a **Security Information & Events Management** (SIEM) solution must be connected to the Security Center. The Security Center itself does not store any data related to security events or logs, as it purely provides a passthrough architecture. For this reason, IT Admins and SecOps teams must connect Security Center to a third-party service for events & log reporting.

For more information on how to connect Knox Asset Intelligence with your SIEM solution, please contact a Samsung Knox sales representative.