Samsung KNOX

Samsung KNOX™ User Guide

Enterprise Edition

October 2013
Version: 1.0

SAMSUNG

Document Information

This document was last modified on October 21, 2013.

Contact Information

Samsung Enterprise Mobility Solutions – Santa Clara
Samsung Telecommunications America, Ltd
3920 Freedom Circle; Suite 101
Santa Clara, CA 95054
United States of America

Contents

Preface 1

About This Guide 1
Audience 1
Notational Conventions 1
Notice Icons 1

1 About Samsung KNOX 2

The KNOX Container 3
Isolate Your Private and Corporate Data 3
Restrictions 4
Device Support 4

2 How to Use Samsung KNOX 5

Setting up a KNOX Container 5
Logging into the KNOX Container 6
KNOX Menu Options 7
Exiting the KNOX Container 7
Managing KNOX Security 7
Changing the KNOX Container Password 7
Resetting a Forgotten Password 8
Changing the KNOX Session Timeout 8
Setting the SE for Android Level 8
Uninstalling, Backing Up, and Restoring KNOX 9

3 How to Use Single Sign-On Service 10

About SSO Service 10
Log in Via SSO Service 11

4 How to Use Samsung KNOX Apps 12

Samsung KNOX Apps 12
Camera and Gallery 13
Contacts 13
E-mail 14
My Files 14
Phone 15
S Planner 15

5 How to Use Samsung KNOX Tools 16

About Device 16
App Information 17
Common Access Card (CAC) 17
CAC Screen Lock 18
Device Status 19
KNOX Settings 19
Notifications Bar 20

Settings 21
Task Manager 21
VPN 22
Wi-Fi Status 23

6 How to Troubleshoot Issues 24

Device Activation Issues 24
Cannot Activate KNOX 24
Message Displays: "Device Activation has failed" 24
Password Issues 25
Cannot Create Password 25
Locked Out of KNOX Container 25
Business E-mail not Synced 25
Cannot Download from Samsung KNOX Apps 26
VPN Issues 26
No VPN Connection 26
VPN Observed Timeout / Host Not Found 26
Error Messages 27
System Has Been Compromised 27
SE for Android Denial 27
Your Device is Not Authorized to Enter KNOX Mode 27
To Check the Warranty Bit 28
CAC Issues (DoD) 29
Absolute Theft Recovery 29
Report a Missing or Stolen Device 30

7 How to Get Support 31

Where to Get More Information 31
Who to Contact 31
What to Provide 31

List of Figures

Figure 1. Samsung KNOX Enterprise 2
Figure 2. Samsung KNOX Container 3
Figure 3. Samsung KNOX App Isolation 4
Figure 4. Samsung KNOX Installation 5
Figure 5. How to Log into the Container 6
Figure 6. KNOX Home, Apps, and Widgets Menus 7
Figure 7. Single Sign-On Service 10
Figure 8. Samsung KNOX Apps store 12
Figure 9. KNOX Container Camera App 13
Figure 10. KNOX Contacts App 13
Figure 11. Personal and KNOX My Files 14
Figure 12. KNOX Phone App 15
Figure 13. S Planner 15
Figure 14. About Device 16

Figure 15. Common Access Card 17
Figure 16. Common Access Card PIN 18
Figure 17. Device Status 19
Figure 18. Notifications Bar 20
Figure 19. KNOX Task Switcher 21
Figure 20. KNOX Using Per-App VPN with KNOX Containers 22
Figure 21. Checking Device Warranty Bit 28
Figure 22. Warranty Bit Status 28
Figure 23. QR Code for Samsung Support Web Portal 31

List of Tables

Table 1. Device Support 4

Preface

About This Guide

This guide describes how to activate and use the enterprise version of Samsung KNOX™. The guide describes KNOX, its secured container, apps within the container, and troubleshooting tools.

Use the links below to jump to a specific location of your interest in this document:

- Chapter 1, About Samsung KNOX
- Chapter 2, How to Use Samsung KNOX
- Chapter 3, How to Use Single Sign-On Service
- Chapter 4, How to Use Samsung KNOX Apps
- Chapter 5, How to Use Samsung KNOX Tools
- Chapter 6, How to Troubleshoot Issues
- Chapter 7, How to Get Support

Audience

This guide is for users of Samsung KNOX Enterprise. The content is based on the assumption that you are knowledgeable in the Android operating system.

Notational Conventions

This guide uses the following notation conventions.

- **Boldface** emphasizes words in text such as screen or window names.
- *Italic* identifies new words, emphasizes phrases, or identifies document names.
- `Monospace` represents information as it appears on a display or in command syntax.

Notice Icons

This guide uses the following notice icons:

Icon	Alerts you to...
 Note	Important features, instructions, or additional relevant information.
 Caution!	Information on conditions that can cause unintended or adverse consequences.

1 About Samsung KNOX

Samsung KNOX protects private and confidential information on Android devices. KNOX is designed to overcome the shortcomings of the current open-source Android operating system. It bases its solution in the tamper-proof device hardware and provides protection to the Linux kernel, Android operating system, and apps and personal data. It is the perfect choice for employees and businesses.

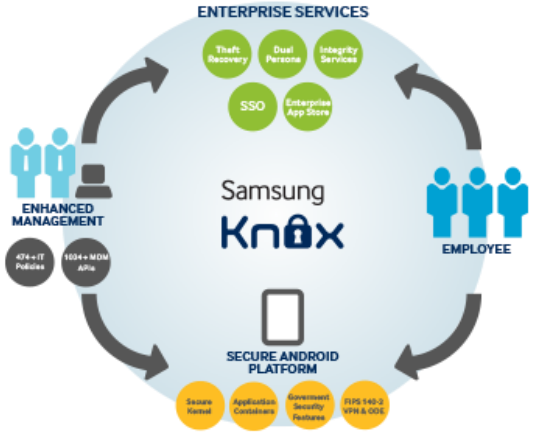

Figure 1. Samsung KNOX Enterprise

Samsung KNOX provides a layered security solution. It includes the following features:

- *Trusted Boot*—Ensures that the device boots only from an authorized kernel, and not from a hacked or rooted kernel
- *TrustZone-based Integrity Measurement Architecture (TIMA)*—Verifies the integrity of the kernel on a continuous basis
- *Security Enhancements for Android*—Uses Mandatory Access Control to protect device resources and data from unauthorized access
- *Dual Persona*—Provides a secure environment within your device. You can continue to use your usual Android environment, and still have access to a protected space

Samsung KNOX enables you to employ a single device for both personal and business activities:

- Seamless and intuitive dual persona experience
- Ensures safety and privacy of personal data
- Helps users comply with company security policies
- Restricts company IT administrator access to enterprise data

The KNOX Container

The Samsung KNOX Application Container is a virtual Android environment within the mobile device complete with its own home screen, launcher, apps, and widgets.

Figure 2. Samsung KNOX Container

The KNOX container provides these apps:

- *Personal Information Manager*—Contacts, S Planner
- *Productivity*—E-mail, Internet browser
- *Utilities*—Phone, Camera, Gallery, My Files, Downloads, Samsung KNOX Apps. Note that the Phone utility is available on devices that can make cellular calls, but not on tablets with Wi-Fi only.

The container is managed using a third party Mobile Device Management (MDM) or Mobile Container Management (MCM) system.

Additional container apps may be installed by the enterprise IT administrator via MDM or by you from the container app store.

Isolate Your Private and Corporate Data

KNOX secures apps and data inside its container as follows:

- Separates the data file systems used by the personal space and the KNOX container
- Encrypts all data inside the KNOX container
- Ensures that apps outside the KNOX container cannot access apps and data in the container.
- Ensures that apps in the container cannot access apps and data outside the container

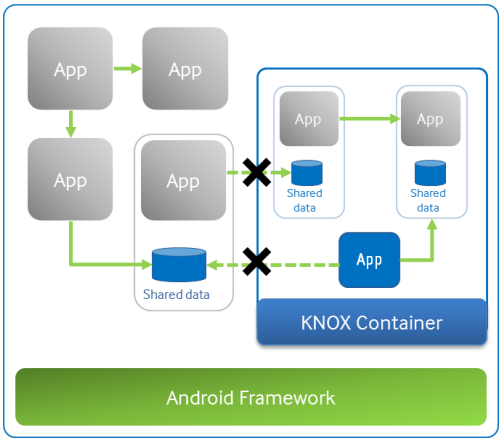

Figure 3. Samsung KNOX App Isolation

Restrictions

The look and feel of the personal space and KNOX container are similar. However, for security and technical reasons, there are some differences when you are using apps in the KNOX container:

- Cannot copy and paste text or images from the container into the personal space
- Cannot access container data like browser bookmarks, browsing history, call logs, S planner events, and so on, from the personal space
- Cannot move files from the container to the personal space
- Cannot use the multi-window function for the browser in the container
- Cannot use Google Text-to-Speech, and cannot install the Google Search bar widget
- You can use Air view but not Air gesture or Air command in the container

Device Support

Currently, the following Samsung devices support personal and enterprise versions of KNOX:

Table 1. Device Support

Device	How KNOX is installed
Galaxy 4	IT administrator
Note 3	IT administrator
Note 10.1 (2014 edition)	IT administrator

Currently, devices are available in selected countries only; devices will become available in other countries as they are introduced there.

As flagship Samsung devices are released and upgraded, you can check if they support KNOX; refer to the Samsung KNOX web portal.

2 How to Use Samsung KNOX

This chapter describes how to use Samsung KNOX, including how to set up, log in, and exit from a container, the various menu options, how manage your password, and how to manage security within a container.

Setting up a KNOX Container

Your IT administrator support group uses a Mobile Device Management (MDM) or Mobile Container Management (MCM) console to activate the Samsung KNOX container on your device. Once your administrator has activated Samsung KNOX, you can install it and set it up.

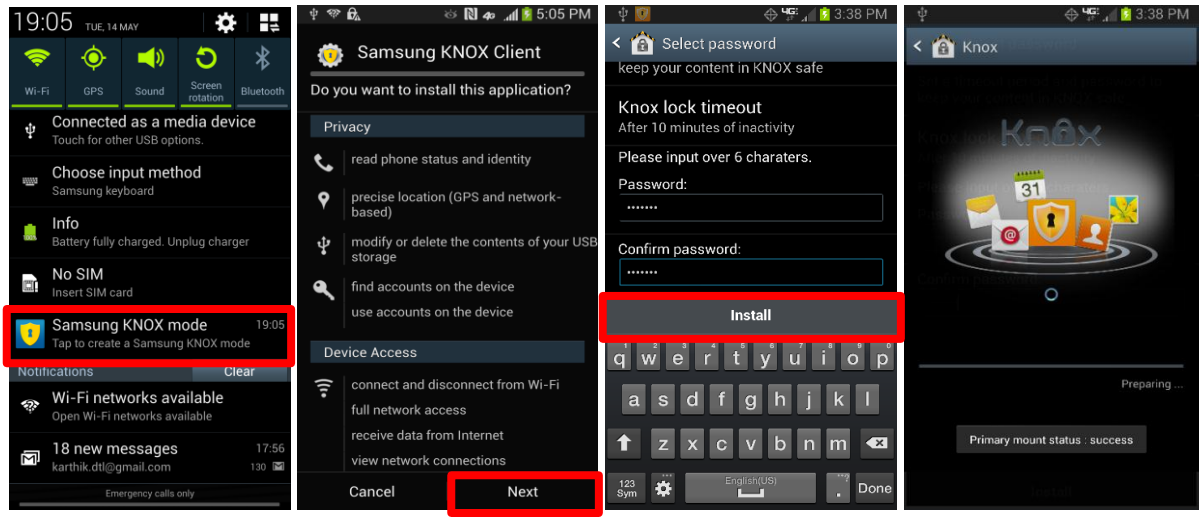

Figure 4. Samsung KNOX Installation

After your IT administrator registers your device:

1. In the Notifications bar, tap **Samsung KNOX**. The Samsung KNOX Terms and Conditions are displayed.
2. If you agree to the Terms and Conditions, tap **Next**.
3. Set the timeout. By default, it is 10 minutes. If you do not do anything in the KNOX container for this length of time, you will need to re-enter the KNOX password.
4. Set the container password, which you will need to enter to access the container. Your IT administrator defines the criteria for a valid KNOX password in your enterprise MDM or MCM system.

5. Tap **Install.** This action performs the following tasks:

   - Creates the KNOX container
   - Sets up a secure file system
   - Installs required components
   - Preloads apps

6. When complete, tap **Launch** to open the KNOX container.
   (Or, go to your personal home screen and log into KNOX later.)

Logging into the KNOX Container

1. To log into the KNOX container, either:

   - Tap the KNOX icon, or
   - Swipe down the Notifications bar, and then tap **KNOX Tap to start**

2. Enter the KNOX **password** you selected when you set up the container.

3. Tap **Done**. The KNOX home screen is displayed.

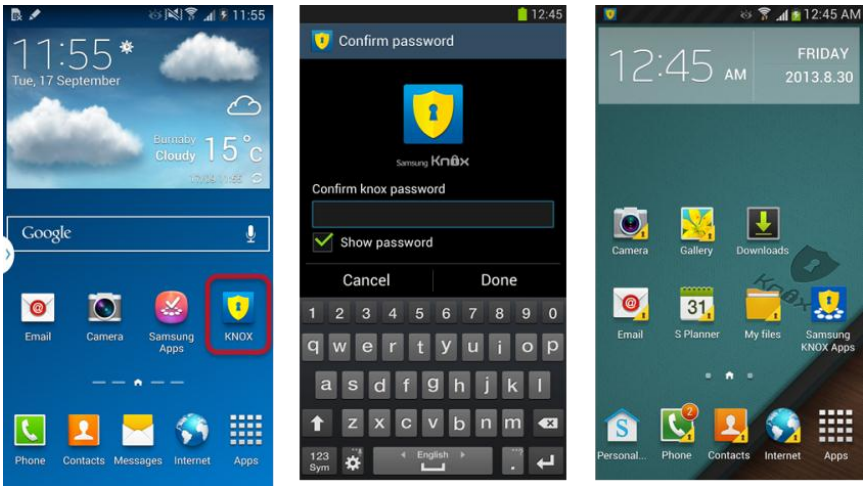

Figure 5. How to Log into the Container

KNOX Menu Options

In the KNOX container, tap the left hardware button to show a menu. The displayed options depend on whether you are in the KNOX Home, Apps, or Widgets screen:

Figure 6. KNOX Home, Apps, and Widgets Menus

Exiting the KNOX Container

To return to the personal space, either:

- Tap the **Personal** icon in the lower left corner of the KNOX home screen.
- Swipe down from the top to show the Notifications bar; then tap either:
  - **KNOX Tap to exit**—You can later re-enter the KNOX container without having to re-enter the password
  - **Lock icon**—To re-enter KNOX, you must enter the password

Managing KNOX Security

This section describes how to change your KNOX container password, timeout session, how to display your contacts in your personal space on your device, and set the SE for Android level.

Changing the KNOX Container Password

To change the KNOX container password:

1. On the KNOX home screen, tap the left hardware button to display the menu.
2. Tap **KNOX settings**.
3. Tap **Change password**.
4. Enter the old and new passwords.
5. Tap **OK**.

Resetting a Forgotten Password

The KNOX container password must first be reset at the IT administrator MDM/MCM console for a notification to be sent to the device.

To set a new password:

1. From **Notifications**, tap **Reset Samsung KNOX password**.
2. Enter **New password**; then **Confirm** password.
3. Tap **Save**.

Changing the KNOX Session Timeout

By default, the timeout is 10 minutes. If you do not do anything in the KNOX container for this length of time, you will need to re-enter the KNOX password.

1. On the KNOX home screen, tap the left hardware button to display the menu.
2. Tap **KNOX settings**.
3. Tap **Password timeout**.
4. Tap the new timeout.

Setting the SE for Android Level

The Security Enhancements (SE) for Android feature uses a policy file to define which apps can access which device resources. This policy file was tested on more than a thousand apps over a six month period. You can set the level of security:

1. On the personal home screen, tap the left hardware button to display the menu.
2. Select **Settings** > **General** > **Security** > **Change security level**.
3. Select either:
   - **High**—Blocks all unauthorized actions. For each such action, you will see an access denial message and be able to stop unauthorized apps.
   - **Normal**—Blocks only unauthorized actions against the essential system resources: kernel, container, and so on
4. For the **Auto update security** checkbox, either:
   - **Select**—Automatically checks for changes to the SE for Android policies and downloads any updates to improve security
   - **Clear**—Uses the last installed policy file. You can later select the checkbox to download the latest policy file.

Automatic security updates are sent over the air to your device. To accept an update, use the Notifications bar, as described in Notifications Bar. Once a week, your device will ask you if you want to send a record of the access denials to a Samsung network server. No personal

information is sent. This enables us to update our policy files as needed to improve security. You can opt out of this feature, as described in Notifications Bar.

Uninstalling, Backing Up, and Restoring KNOX

Only your IT administrator can uninstall, back up, or restore your KNOX container. Contact them for more details.

3 How to Use Single Sign-On Service

This chapter describes how to use the Single Sign-On (SSO) service with apps in the Samsung KNOX container.

About SSO Service

Samsung KNOX includes out-of-the-box SSO support for apps in the KNOX container. This SSO service is available as soon as you activate KNOX.

With SSO, apps in the KNOX container can use your company login to verify your identity. The first time you launch any of these SSO-enabled apps, you are asked to enter your company login.

SSO provides these benefits:

- You have one-click access to all KNOX apps that support SSO
- You do not need to remember a different password for multiple apps
- You can avoid managing many weak, easy-to-remember passwords that do not meet your company's password policies

SSO uses your company's Active Directory to check your login credentials.

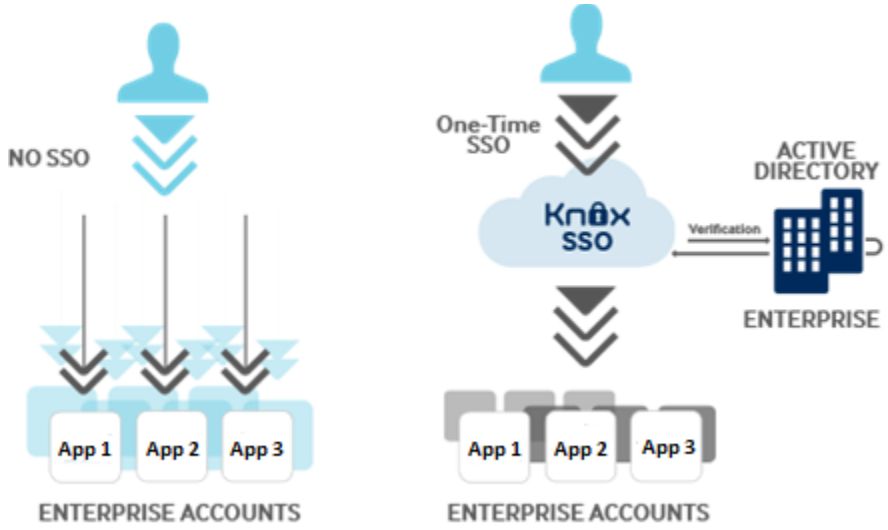

Figure 7. Single Sign-On Service

Your enterprise IT administrator can use an MCM or MDM to enable the SSO service for all container apps that support SSO, or just for selected (or whitelisted) apps.

Log in Via SSO Service

To log in via the SSO service, perform the following steps:

1. In the KNOX container, tap an **App Icon**.

   If the app uses the SSO service and has been whitelisted by your IT admin, the Centrify SSO login screen is displayed.

2. Enter your company login: **Username** and **Password**.

3. Tap the **Login** button**.**

4 How to Use Samsung KNOX Apps

The following apps are available in KNOX containers:

- Samsung KNOX Apps
- Camera
- Contacts
- Downloads
- E-mail
- Gallery
- Internet
- My Files
- Phone
- Polaris Office 5
- S Calendar
- S Memo
- S Planner

These default apps are described in the following sections.

Samsung KNOX Apps

The Samsung KNOX Apps store in the KNOX container offers a variety of business apps from Independent Software Vendors (ISVs). The store provides apps that have been secured to work in the KNOX container. You can browse and download apps the same way you do with Google Play.

Figure 8. Samsung KNOX Apps store

These apps and their data work within the container and are not accessible from the personal space.

Camera and Gallery

The camera in the KNOX container is the same camera available your personal space.

Photos that you take with the KNOX camera cannot be accessed outside of the container environment (just as photos taken with the camera in your personal environment cannot be accessed within the KNOX container).

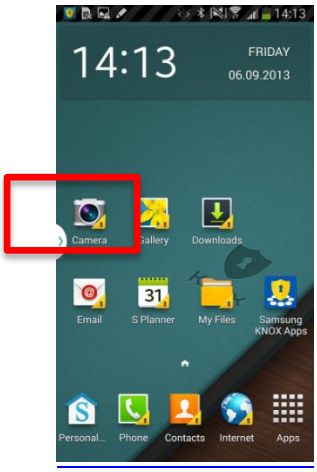

Figure 9. KNOX Container Camera App

Contacts

The Contacts in the KNOX container is the same Contacts app in the personal space.

In the KNOX container, you can see contacts from your personal space. In both the personal space and KNOX container, the KNOX contacts are marked with a shield.

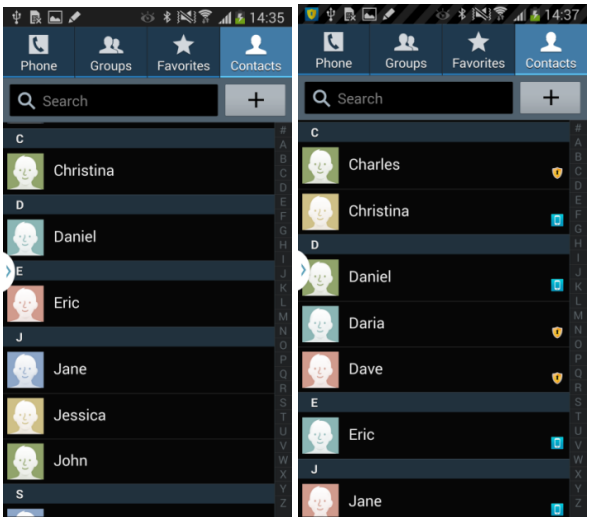

Figure 10. KNOX Contacts App

E-mail

The e-mail app in the KNOX container supports POP3, IMAP, and Microsoft Exchange ActiveSync mail accounts. For most popular email accounts, like Gmail, you just enter your e-mail address and password. The e-mail app automatically sets up the correct settings to get e-mail from the account. You just select a name for the account and how often to get e-mails.

If your workplace uses Microsoft Exchange ActiveSync, you can also read your work e-mail in the KNOX container. Use the **Manual setup** and ask your IT department for the correct settings to use

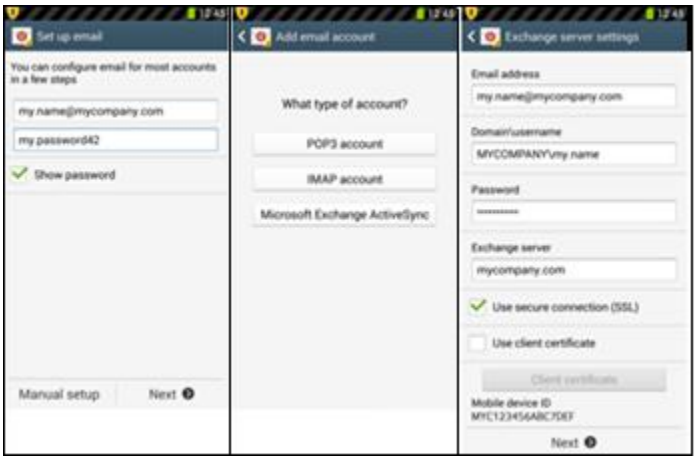

Figure 11. KNOX Email Setup

Emails, file attachments, and other data cannot be accessed outside of the KNOX container.

My Files

The file systems outside and inside the KNOX container are similar in appearance. However, you cannot see the KNOX files from your personal space, or the personal files from the KNOX container.

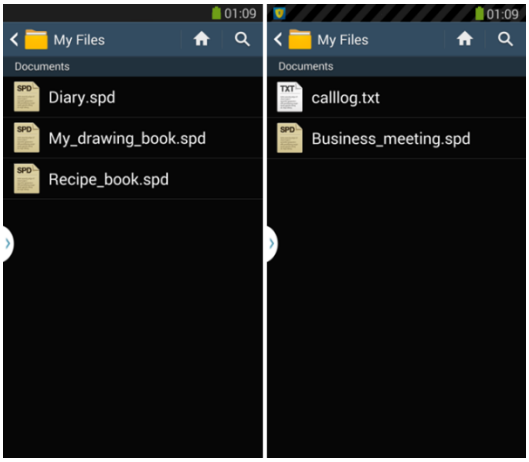

Figure 11. Personal and KNOX My Files

Phone

The Phone is available on devices that can make cellular calls, but not on tablets with Wi-Fi only.

Figure 12. KNOX Phone App

The Phone in the KNOX container is the same as the phone in your personal space. In the KNOX container, you can see contacts from your personal space. If contacts from your personal space call while you are using apps/tools in the KNOX Container, you will see their name (and photo if you provided one) and not just a phone number.

S Planner

In the KNOX container, the calendar displays events from your personal calendar. You can only see these personal events; to change the personal events, you must return to the personal space. In the personal space, you cannot see the events from the KNOX calendar.

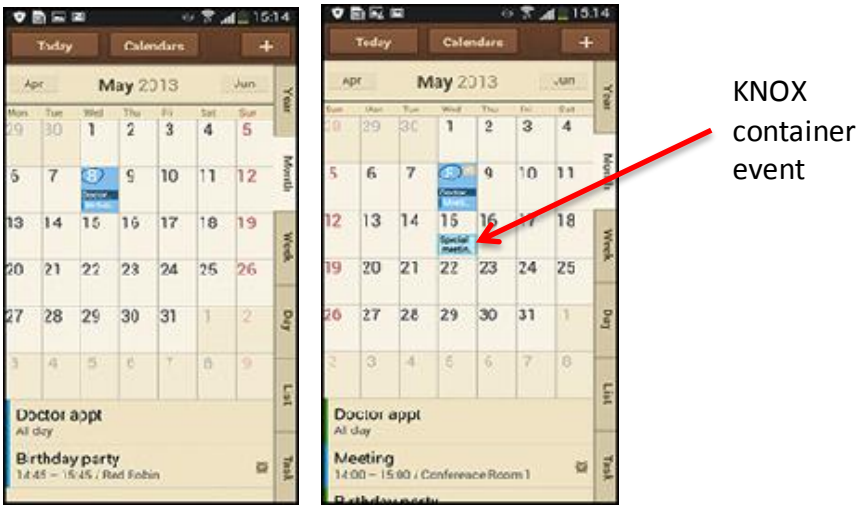

Figure 13. S Planner

5 How to Use Samsung KNOX Tools

Use the tools described in this chapter to check the status of KNOX. If you encounter an issue, you can also learn how to resolve the issue on your own. If you ask for support, your IT administrator or support agents might ask you to use these tools to help them troubleshoot.

About Device

Use this tool to check if your device supports KNOX.

To display this tool, perform the following steps:

1. On the personal home screen, tap the left hardware button to display the menu.
2. Tap **Settings** > **General** > **About Device**.

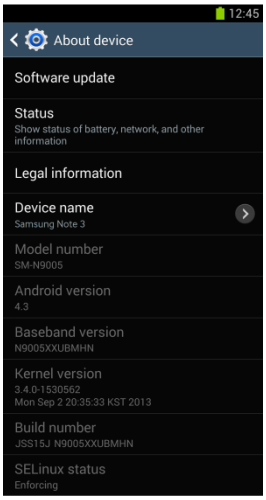

Figure 14. About Device

About device displays the following information:

- *Model number*—The way KNOX is preloaded depends on the model and operator. Use this number to check for these differences if you require support.
- *Android version*—KNOX requires Android version 4.3 (or later)
- *Build number*—Indicates the Android code family (J=Jellybean), branch (R=primary, S=secondary), date (S15=July 15, 2013), and build (J=#10)
- *Kernel version*—Version of the current kernel, and date the kernel was updated
- *SELinux status*—Status can be one of the following options:
    - *Permissive*—Device simply records any unauthorized access to resources. Device manufacturers use this information to improve their security policy files.
    - *Enforcing (default)*—Device prevents unauthorized access to resources

App Information

Use this tool if a KNOX app is not working properly. You can perform the following procedures:

- Check an app version number
- Stop the app
- Uninstall the app or its updates
- Check how much internal memory and storage is used
- Clear data stored by the app
- Clear cache used by the app

To display this tool:

1. Tap **Settings** > **General** > **Application manager**.
2. Tap the app name to view its app info.

Common Access Card (CAC)

Common Access Cards (CACs) are "Smart" ID cards used by active-duty military, selected Reserve, Department of Defense (DoD) civilian employees, and some contractors to enable access to DoD computers, networks, and facilities.

The KNOX platform extends CAC authentication to the container for Browser, E-mail, VPN, and lock screen functions.

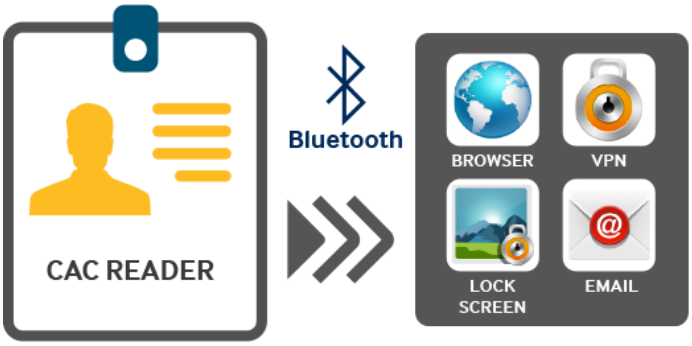

Figure 15. Common Access Card

CAC is used as a Public Key Infrastructure (PKI) authentication method for the following functions:

- E-mail
  - Sign E-mail with digital signature
  - Encrypt/decrypt E-mail message
  - Verify digital signature
- Browser
  - Access secure web pages

- Downloader
    - Download files from secure websites
- VPN
    - Complete a virtual private network (VPN) connection login
- Lockscreen
    - Secure device with SmartCard-based lock screen login

If a requesting app that needs the CAC is not in the foreground, it may show a notification status of "CAC PIN Expired". You must tap the CAC PIN Expired notification and enter the PIN again to re-authenticate.

CAC Screen Lock

In government apps where a CAC is used for authentication, the CAC PIN becomes the device unlock PIN.

To unlock the device, insert your card into the CAC reader and enter your CAC PIN.

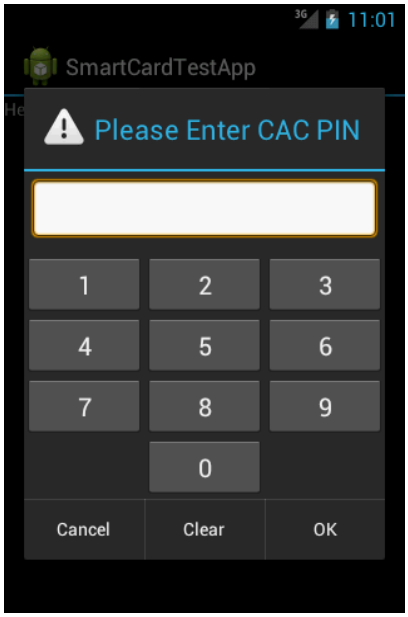

Figure 16. Common Access Card PIN

Notes

- When a CAC is configured using the BAI MP3000 Bluetooth reader, the device and the reader are paired to work together. For instructions on device pairing, refer to the *BAI M3000 Android Bluetooth Reader Users Guide*.
- After device pairing, a *CAC* menu item is added to the *Select screen lock* settings menu as a screen lock option (in addition to PIN, password, and so on).

Device Status

Use this tool if there are problems sending or receiving data (emails, web pages, and apps) to or from the Internet.

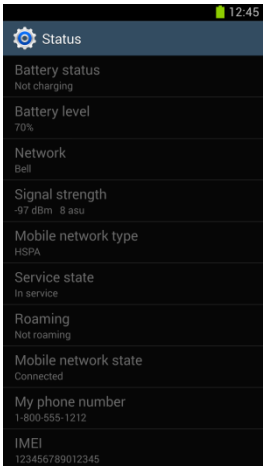

Figure 17. Device Status

You can check the following device status information:

- *Battery level*—If you need to send or receive a large file, ensure that there is enough power to avoid interrupting the file transfer.
- *Signal strength*—If you are using the cellular connection, check the signal strength. A value of:
  - 100-120 dBm—Indicates a location with weak reception
  - 60-80 dBm—Indicates strong reception
- *Mobile network state*—Also ensure that the cellular status is **Connected**.

To display this tool:

1. On the personal home screen, tap the left hardware button to display the menu.
2. Tap **Settings** > **General** > **About Device** > **Status**.

KNOX Settings

Use this tool to manage KNOX. You can perform the following tasks:

- Change the KNOX container password
- Change the KNOX session timeout
- Check the KNOX version installed

- Read the *Terms and Conditions*

To display this tool:

1. On the KNOX home screen, tap the left hardware button to display the menu.
2. Tap **KNOX settings**.

Notifications Bar

Use this tool to check KNOX status and switch between the personal space and KNOX container.

To display this tool, you must swipe downwards from the top of the screen.

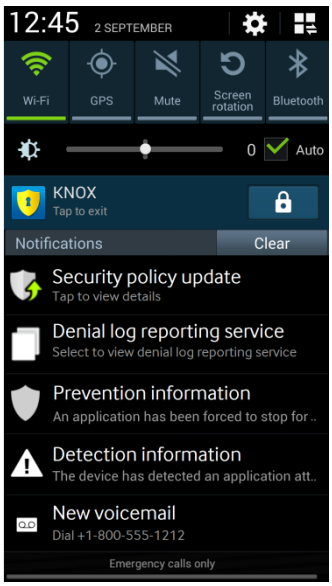

Figure 18. Notifications Bar

You can perform the following tasks:

- *KNOX Tap to exit*—To return to the personal space, you can tap either:
  - *KNOX Tap to exit*—You can later re-enter KNOX without having to enter the password
  - *Lock icon*—To re-enter KNOX, you must enter the password
- *Security policy update*—The policy file defines which apps can access device resources and data. You can accept the latest update to the file. See also: Setting the SE for Android Level.
- *Denial log reporting service*—The denial log records unauthorized access to resources and data. You can upload this log to a Samsung server so that we can update our policy files as needed to improve security. No personal information is recorded in the denial log.

- *Prevention information*—KNOX detects that an unauthorized app has tried to access a resource and has stopped the app. Tap to display the Application Manager to uninstall the app.
- *Detection information*—KNOX detects that an unauthorized app has tried to modify the operating system or disable SE for Android. KNOX recommends rebooting your device

Settings

The Android Settings tool enables you to perform the following tasks:

- Determine Version and Build Information
- Edit and check KNOX Settings
- Check Device Status
- Check Wi-Fi Status
- Check the Task Manager
- Check App Info

To display the Android Settings tool:

1. Tap the **Settings** icon on the home or Apps screen.

Task Manager

Use this tool to investigate performance issues and stop apps that are not working properly.

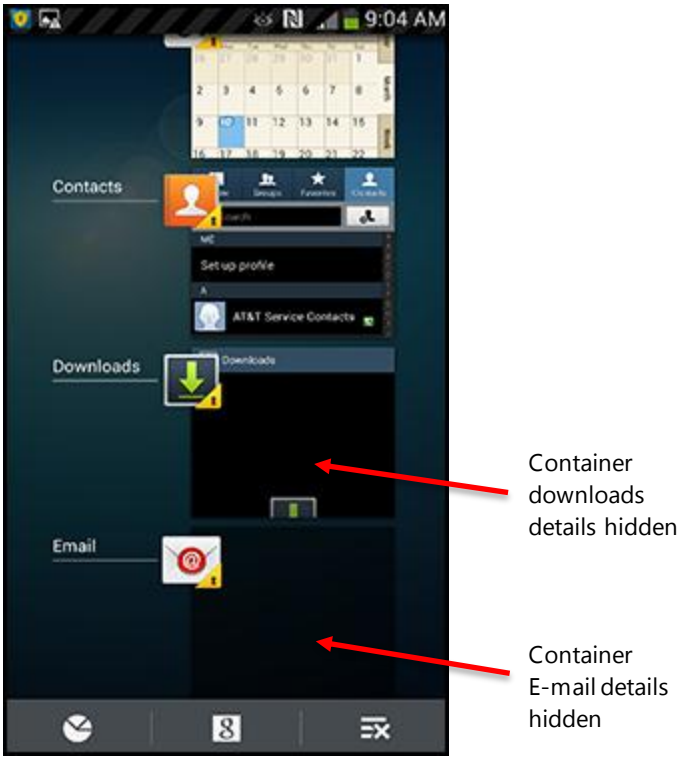

Figure 19. KNOX Task Switcher

To display this tool:

1. Push and hold the **Home** button. This displays the apps that are running in the background. The KNOX apps have a yellow lock on their icons.
2. To stop an app from running, long press its icon and select **Remove from List**.
3. In the bottom left corner of the screen, tap the task manager icon.
4. Tap either:
   - **Active applications**—View the apps that are running in the background, and stop an app
   - **Downloaded**—View the apps that have been downloaded, and remove an app
   - **RAM**—View how much memory is being used, and release memory to try to improve performance
   - **Storage**—View how much storage is being used

VPN

The Samsung KNOX platform includes an IPsec VPN solution which uses encryption to protect your data in transit. Your IT administrator configures your enterprise VPN profiles, and pushes them over the air to your device. Enterprise apps can then connect securely into the enterprise network over the VPN connection.

KNOX supports up to 5 separate VPNs. Your IT administrator can specify the apps that are allowed to send data over each VPN. All other apps, including those in your personal space, will not use VPNs, but will send data over your device's regular data connection.

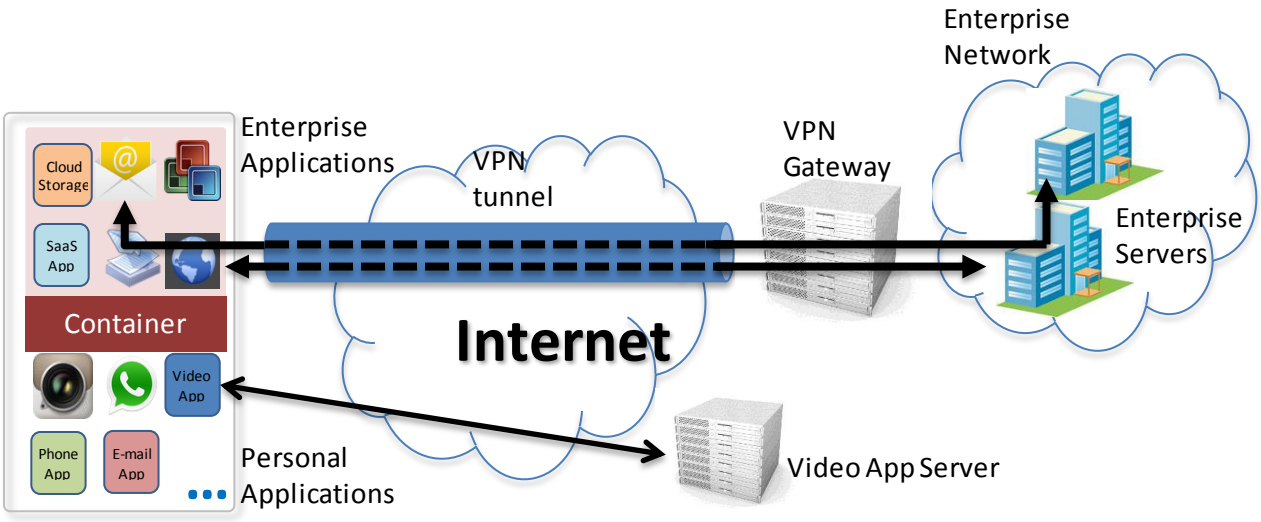

Figure 20. KNOX Using Per-App VPN with KNOX Containers

Figure 20 illustrates a KNOX platform configuration that uses a VPN to provide protection for selected enterprise apps inside the KNOX container. The IT administrator has configured a KNOX container on the employee's device with several apps, including two enterprise apps that need to connect back to the enterprise intranet servers.

In Figure 20, the browser and messaging apps have been added to the enterprise VPN profile. When you run either app, the KNOX platform automatically starts the VPN connection, if not already connected. The device will connect via the VPN service. If prompted, enter your credentials.

Wi-Fi Status

Use this tool to check Wi-Fi connectivity and signal strength. Some apps might allow file transfers over Wi-Fi only. For example, the email app can be set up to download attachments only when connected to Wi-Fi. Also, the package downloaded during a KNOX update is sent over a Wi-Fi connection.

To display this tool:

1. On the personal home screen, tap the left hardware button to display the menu.
2. Tap **Settings** > **Connections** > **Wi-Fi**. Then tap the connected Wi-Fi router.
3. Check the **Signal strength**.

6 How to Troubleshoot Issues

This chapter describes some issues you might experience while using Samsung KNOX. For any issues not covered here or for additional support, see How To Get Support.

Device Activation Issues

Consider the following guidelines in case you experience any of these device activation issues.

Cannot Activate KNOX

To activate KNOX, an update package must be downloaded to the device from a Samsung update server. The server may not be accessible, the device may not be adequately charged, or the server may be down or unable to respond to package requests within a specified timeout period.

Perform the following steps:

1. Verify the device battery charge level is greater than 70%. If not, plug the device into a charger and reattempt the activation.
2. If the battery level is OK, verify that Wi-Fi is on, with good Wi-Fi signal strength (if using Wi-Fi connection).
3. If you are using a cellular connection, check mobile data is on, with good cellular signal strength (if using a cellular connection).
4. In case this is due to a sporadic event, such as abnormally high network traffic or unplanned server maintenance, check with IT or try the device activation again at a later time.

If unsuccessful, escalate the issue to your IT administrator support group.

Message Displays: "Device Activation has failed"

KNOX activation was performed on a device, the update package was downloaded, and the device rebooted, but the device displays a message indicating that activation failed. There may be an issue with the update package.

Contact your IT administrator support group.

Password Issues

The following guidelines are provided for password-related issues.

Cannot Create Password

IT can set strict requirements for the Container password; for example, set up forbidden strings, restrict the re-use of past passwords, check password strength, or restrict the use of characters.

Perform the following steps:

1. Contact your IT administrator and verify that your password complies with the authentication policies.
2. If the Show password option is available, ensure that both passwords match, and case sensitivity is not an issue.
3. If the issue remains, remove and re-create the Container on your device.

If issues persist, escalate the issue to your IT administrator support group.

Locked Out of KNOX Container

If you cannot enter the correct KNOX password in the allowed number of tries, you are locked out of the KNOX container. Your IT administrator can set the maximum number of failed login attempts allowed.

To reset your password, contact your IT administrator.

Business E-mail not Synced

There may be a problem with device reception issues, ActiveSync issues, Active Directory issues, or the enterprise Exchange server.

There might be a problem with device reception, email account setup, the network, or your email provider's service. Try the following:

1. Check device reception:
   - Device has cellular or Wi-Fi connectivity
   - Reception is strong and stable
2. Reboot your device. This stops background apps, clears memory, and resets the email app in case it is slow or not responding.
3. Start the email app.
4. Ensure your email login and password are correct, and that you are logged in properly.
5. Tap the send/receive icon to see if you can get emails manually. To test, send an email to yourself to see if it is received.
6. Check your email account settings:
   - **Sync mail**—Enable this option if you want to get emails automatically

- **Sync schedule**—Check the frequency that emails are being received
- **While roaming**—Sync is disabled by default. Change if needed

7. If you have never received email on this account, ask your IT administrator to check the account settings on your device.
8. If you have received email before, ask your IT administrator if there are issues with ActiveSync, the email server, or the company network. Also check if IT has changed your email account, for example, disabled or reconfigured it.

Cannot Download from Samsung KNOX Apps

If you cannot download an app, try the following:

1. Ensure the device has a cellular or Wi-Fi connection.
2. You have logged in to the Samsung KNOX Apps with the right password.
3. Restart the app download.
4. Restart the device.
5. If issues persist, contact your IT administrator.

VPN Issues

Here are some guidelines for VPN issues.

No VPN Connection

An app that uses VPN is not able to access the internet, for example, Container-based browser cannot display web pages.

Perform the following steps:

1. Check the underlying network connection:
   - Wi-Fi is on, with good Wi-Fi signal strength
   - Cellular access is up, Mobile data is on
2. Reboot the device.
3. If issues persist, contact your IT administrator.

VPN Observed Timeout / Host Not Found

Perform the following steps:

1. Ensure that you have good signal strength if you're using a data connection.
2. Contact your IT administrator to verify that there is no firewall policy preventing access.

Error Messages

Here are some potential error messages and suggested workarounds.

System Has Been Compromised

When an app tries to modify your device operating system or disable SE for Android, the device displays one of the following messages:

```
The device has detected an application attempting unpermitted actions and has
stopped loading.  To protect your device, it is recommended you reboot.

The device has detected an application attempting unpermitted actions. To
protect your device, it is recommended you reboot.

SE for Android protection has been disabled. To protect your device, it is
recommended you reboot.
```

Do the following:

1. Reboot the device.
2. If issues persist, contact your IT administrator.

SE for Android Denial

When an app tries to access a resource that it is not allowed to, the Security Enhancements (SE) for Android blocks the attempt. SE for Android also notifies you through the Notifications bar and a popup window. If possible, this notification identifies the app and the resource it tried to access.

1. On the popup window, tap either:
   - Application manager—To display the Application manager to stop or uninstall the app
   - Close—If you do not want to do anything at this time.
2. Reboot the device.

Your Device is Not Authorized to Enter KNOX Mode

Samsung KNOX cannot be installed on a rooted device. (A rooted device bypasses installed security features by allowing user-installed software to run privileged commands, potentially enabling or deleting system files, or allowing access to the device's operating system or hardware.)

A warranty bit is applied to the device and Samsung can check whether device is rooted or not by checking this bit. If an incompatible kernel image is being loaded into memory, the warranty bit is changed from "**0x0**" to "**0x1**". Then it's impossible to install KNOX container on the device and a KNOX container which is already installed on the device can't be opened.

To Check the Warranty Bit

Boot the device in ODIN Mode to determine if warranty bit has been altered:

1. Simultaneously press **Volume down**, **Home**, and **Power** buttons.
2. When warning screen is displayed, press the **Volume up** button.

The Warranty Bit Status ("KNOX Warranty Void") is displayed in upper left hand corner of the display.

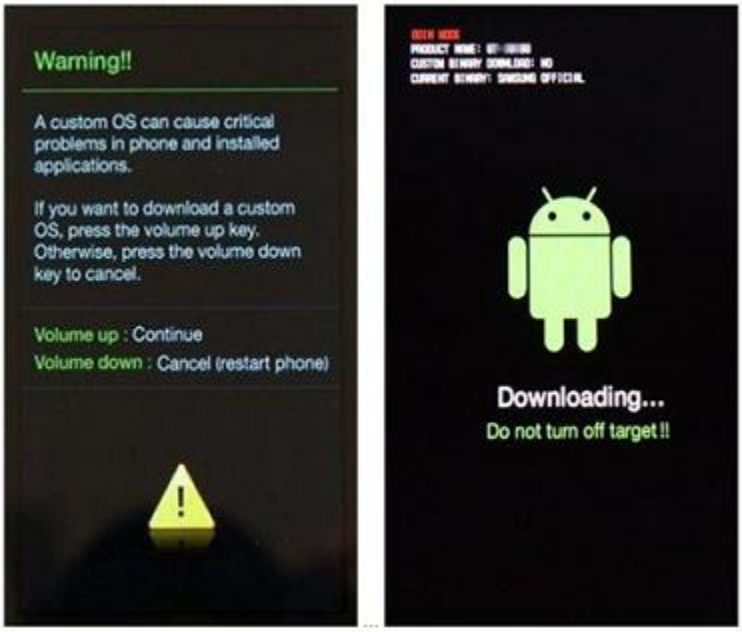

Figure 21. Checking Device Warranty Bit

See Figure 22 for the Warranty Bit status message:

Figure 22. Warranty Bit Status

CAC Issues (DoD)

Here are possible Common Access Card (CAC) error messages and their associated remedy actions:

- *CAC Card Removed*—Insert/reseat card in the reader
- *CAC PIN Error*—Verify and re-enter the PIN
- *CAC PIN Expired*—Re-enter PIN due to timeout
- *CAC PIN Locked*—DoD personnel using a CAC can encounter a Personal Identification Number (PIN) on the CAC that is locked. Usually this takes place after three unsuccessful login attempts. You must contact an appropriate DoD facility to accommodate resetting the CAC PIN.

  To unlock a CAC:

  - Contact any DEERS/RAPIDS issuing facility to request a reset CAC PIN. You can find your nearest DEERS/RAPIDS ID Card facility using the RAPIDS Site Locator.

    Additional CAC and CAC reader information:

    - http://www.cac.mil/
    - *BAI M3000 Android Bluetooth Reader Users Guide*
- *Uninitialized CAC Card*—Contact the CAC administrator
- *CAC Locked (after three incorrect login attempts)*—Contact the CAC administrator to unlock the card
- *No Connection*—Connection to the Smart Card does not exist. Possibly due to card not present in reader or reader is out of range.
- *Device Not Configured*—Indicates that the Smart Card Reader is not configured on the device. Possibly the device may not be paired.
- *Connection Busy*—Indicates that the connection is already established

Absolute Theft Recovery

This is an optional service that your company can use to recover lost or stolen devices. If a device is lost or stolen, you can perform the following steps:

1. Determine the location of the device and whether or not it's on the move.
2. Freeze the device to prevent unauthorized access.
3. Remotely retrieve important files or delete files immediately from the device.
4. Contact your IT administrator to alert them of the event.

Report a Missing or Stolen Device

1. Report the incident to the local law enforcement agency and receive a police case number.
2. Contact your IT administrator who will then contact the Theft Recovery Customer Center, and complete a report that includes the police case number.
3. Theft recovery personnel transmit commands to the Mobile Agent to activate monitoring and tracking, and coordinates with law enforcement to recover the device.

7 How to Get Support

Where to Get More Information

The KNOX web portal at samsungknox.com provides a lot of additional information about KNOX. You can also scan the following QR code to go to KNOX web portal; see Figure 23:

Figure 23. QR Code for Samsung Support Web Portal

For more information at the Samsung Support Web Portal, check out these tabs:

- **Overview**—For a video introduction. If you want more detail about the security features, select from the drop-down menu bar along the top: **Overview** > **Technical Details**.
- **Resources**—For a white paper, glossary, and interactive Flash simulator
- **Support**—For *Frequently-Asked Questions*

Who to Contact

If you encounter an issue that is not covered in How to Troubleshoot Issues, contact your IT administrator.

What to Provide

To resolve your issue as fast as possible, be prepared to collect the following information:

- From About Device:
  - Model number
  - Android version
  - Build number

- Kernel version

- From Device Status:
  - Mobile network state
  - Signal strength
- From Wi-Fi Status:
  - Status
  - Signal strength