Contents

Getting Started with Samsung SDS IAM & EMM User Suite
Understanding users and roles ............................................. 3
Creating user accounts ....................................................... 5
Bulk import user accounts .................................................. 8
Creating roles and adding users to roles ............................. 11
Verifying users have access to Samsung SDS IAM & EMM user portal ........... 13
Possible next steps .......................................................... 14

Chapter 1  Common tasks
How to configure Mobile Device Management or single sign-on only ........... 18
How to enroll devices ......................................................... 22
How to create a policy set and assign it to users ......................... 26
How to define authentication requirements ............................ 28
How to configure and deploy applications to users .................... 34
How to install the Samsung SDS IAM & EMM Browser Extension .......... 40
How to configure user self-service options ............................ 44
How to install a Samsung SDS IAM & EMM connector ................ 48
How to configure Integrated Windows authentication .................. 58
How to configure browsers for silent authentication ................... 64

Chapter 2  Advanced Tasks
How to configure inbound provisioning .................................. 72

Chapter 3  Services and components overview
Component summary ......................................................... 84
Which software is installed and where .................................. 87
Supported web and device browsers ..................................... 89
Supported devices .......................................................... 90
Foreign language support ................................................... 91
Logging in to the user and administrator portals with silent authentication .... 92
Samsung SDS IAM & EMM user portal overview ....................... 93
Selecting an identity repository ................................................. 94
Selecting a policy service ....................................................... 95

Chapter 4  Viewing dashboards
Interpreting the Security Overview dashboard ............................. 98

Chapter 5  Managing users
Account sources ......................................................................... 100
Using the Active Directory/LDAP and Samsung directory ID repositories ...... 101
Default user accounts ................................................................. 102
Managing Samsung directory accounts from the Users page ............... 103
Referencing accounts from Active Directory/LDAP ............................ 108
Sending invitations to users ....................................................... 110
Deleting accounts ...................................................................... 112
Specifying a user’s application login settings .................................. 113
Using search filters ................................................................... 115

Chapter 6  Managing applications
Deploying the Samsung SDS IAM & EMM User Portal application .......... 117
Viewing and sorting applications in the Apps page ............................. 118
Modifying the application description .......................................... 120
Configuring automatic versus optional deployment ............................ 121
Setting web application access policies ....................................... 122
Managing application access requests ......................................... 123
Application symbols .................................................................. 128
Removing an application ............................................................. 130
Adding web applications by using Admin Portal .............................. 131
Android for Work ..................................................................... 141
Deploying web applications to Knox containers ................................. 146
Deploying mobile applications to Knox containers .............................. 147

Chapter 7  Managing devices
Enrolling a device ...................................................................... 154
Using Admin Portal to manage devices ........................................ 160
Using Active Directory Users and Computers to manage devices .......... 162
Using the device management commands ..................................... 165
Chapter 8  Managing policies
- Using policy sets .................................................. 187
- General device management settings ............................ 189
- Authentication - Setting authentication policy controls ... 193
- Setting password controls ........................................ 199
- Configuring OATH OTP ............................................ 201
- Configuring derived credentials ................................ 202
- Managing Application policies .................................. 220
- Managing device configuration policies ......................... 221
- Mobile device configuration policies overview ................ 227

Chapter 9  Managing roles
- Predefined roles ..................................................... 249
- Removing users or groups from a role ......................... 250
- Assigning applications to and removing them from roles ... 251
- Creating Samsung service administrators ...................... 252
- Deleting roles ......................................................... 256

Chapter 10  Managing customer Samsung services
- About customer Samsung services .............................. 258
- Creating an Samsung service for a customer .................. 259
- Disabling and enabling a customer Samsung service ......... 261
- Logging in to a customer Samsung service ..................... 262
- Creating roles that can create and manage customer Samsung services ............................................. 263

Chapter 11  Managing reports
- What’s in the Report Library ..................................... 266
- Reports provided in Admin Portal ............................... 267
- Access to shared reports and report data ...................... 268
- Selecting report data ................................................. 270
- Common events that you can search for ...................... 275
- Working with reports .............................................. 277
- Report query examples: Built-in report definitions .......... 281
Chapter 12 Configuring Samsung service settings

- Customizing Samsung service user interfaces ........................................... 291
- Configuring connectors ......................................................................... 296
- Configuring Samsung SDS IAM & EMM RADIUS Support ..................... 298
- Adding LDAP as a directory service ......................................................... 309
- Adding Google as a directory service ...................................................... 311
- Managing Business Partner Federation .................................................... 312
- Managing social login users .................................................................. 317
- Enabling email quarantining ................................................................... 325
- Using Apple Configurator to mass deploy iOS devices ............................. 327
- Using DEP with Apple Configurator to mass deploy iOS devices ............... 330
- Generating an APNS certificate ................................................................. 332
- Enabling automatic log out from the Samsung SDS IAM & EMM user portal and Admin Portal ................................................................. 336
- Using login suffixes .............................................................................. 337
- Linking to the Apple Device Enrollment Program .................................... 340
- Setting Corporate IP ranges .................................................................... 343
- Tag devices as corporate owned ............................................................... 344
- Selecting the policy service for device policy management ....................... 345
- Managing security settings ..................................................................... 350
- Importing OATH tokens in bulk ............................................................... 353

Chapter 13 Samsung SDS IAM & EMM connectors and administrator consoles

- Supporting user authentication for multiple domains ............................... 356
- Modifying the default connector settings ................................................ 360
- Modifying connector account permissions ............................................. 362
- Using Active Directory certificates in devices for authentication ............. 365
- Uninstalling the Samsung SDS IAM & EMM Management Suite software ................................. 369

Appendix 1 Configuring the Samsung SDS IAM & EMM connector

- About the Samsung SDS IAM & EMM connector and the configuration program .................. 371
- Using the Status tab ............................................................................... 372
- Using the Samsung SDS IAM & EMM connector tab ............................... 373
Appendix 2  List of device configuration policies

Understanding licensing ......................................................377
Common Mobile Settings ..................................................378
iOS Settings .................................................................380
Samsung Knox Device Settings .........................................385
Samsung Knox Workspace Settings ....................................395
Touchdown Settings .......................................................404

Appendix 3  Re-enrolling a device in domains with a different customer ID
Welcome to the Samsung SDS IAM & EMM User Suite. This scenario is intended to guide system administrators through the initial setup of Samsung SDS IAM & EMM User Suite for single sign-on and only with the Samsung SDS IAM & EMM directory as your identity store. If you are using Active Directory/LDAP to store user accounts, want to continue using it as your primary identity store, and want to continue using the same tools (for example, Active Directory Users and Computers) to manage users and mobile devices, then you will need to install the Samsung SDS IAM & EMM connector before you see the Active Directory/LDAP groups when you add users to roles. See “How to install a Samsung SDS IAM & EMM connector” on page 48. When you use only the Samsung SDS IAM & EMM directory as your identity store, you do not need to install anything. Everything is configured using Admin Portal. See “Selecting an identity repository” on page 94 for more information on the different identity repositories.

To get here, you have most likely already completed a few key steps:

1. You have requested a free trial or subscription to the Samsung SDS IAM & EMM User Suite.

   If you did not get this guide as part of a free trial or subscription, you should start by filling out the following form to request access to the Samsung SDS IAM & EMM User Suite:


2. You have registered for a Samsung SDS IAM & EMM account with a valid email address and have received an “Activate Your Samsung SDS IAM & EMM Account” email followed by a “Your Samsung SDS IAM & EMM Account Is Ready - Next Steps” email with your account details.

   Your account details include the user name for an administrative account that is a member of the sysadmin role and a unique customer identifier. Members of the built-in sysadmin role have access to the Samsung service and can grant access rights to other users.

3. You have logged in to Admin Portal using your account details and set a new password for your administrative account.

   If you have not completed these preliminary steps, stop here and verify that you have received the “Your Samsung SDS IAM & EMM Account Is Ready - Next Steps” email and that you can log in to the Samsung service with the account information in the email.

The Samsung SDS IAM & EMM User Suite provides numerous features, functions, and configuration options. These getting started procedures will not include many of those options because they are only intended to get you going with the basic setup.
This getting started scenario includes the following topics:

- “Understanding users and roles” on page 3
- “Creating user accounts” on page 5
- “Bulk import user accounts” on page 8
- “Creating roles and adding users to roles” on page 11
- “Verifying users have access to Samsung SDS IAM & EMM user portal” on page 13
- “Possible next steps” on page 14
Understanding users and roles

Admin Portal roles are sets of user accounts. You use roles to assign applications, permissions, and policies to sets of users. Users can be members of multiple roles.

The Samsung service assigns applications and applies the selected administrative rights to all role members. For example, if you add an Active Directory/LDAP group to a role, the applications assigned to that role are now available to members of that group. Similarly, when you remove a user from a role, the Samsung service deletes all the web applications assigned to that role from the user portal and enrolled devices.

When you use the Samsung SDS IAM & EMM policy service to manage mobile device policies, the Samsung service installs the policy sets based on the users’ roles. Users belonging to multiple roles with different mobile device policies applied will inherit the highest prioritized policy.

This diagram shows:

- Mary belongs to roles A and B so she has access to all 5 applications (Slack, ADP, Salesforce, Gmail, and Office 365).
- Mary’s inherited mobile device policies depend on the prioritization of the policies. See “Using hierarchical policy sets” on page 187.
- All members of the Active Directory group 1 have access to Gmail and Office 365.
Changes that impact the assigned applications or administrative rights will take effect when the user next logs in to the user portal or device. You can push the changes to the users for immediate update by selecting the role members on the Users page and sending the **Reload** command.

See “Predefined roles” on page 249 for a list of predefined roles.

**Note** Your role must have the Roles Management administrative right to view, add, and modify roles. See “Creating Samsung service administrators” on page 252.

### Nesting a role

You can add a Samsung SDS IAM & EMM User Suite role to a role. This is referred to as “nesting a role.” When you add a role to a role, the nested role members get all of the applications and rights assigned in the parent role. However, the applications and rights inherited from the parent are *not* displayed when you select the nested role. Only the nested role members have use of the rights and applications assigned to the nested role—the parent role members do not.

Additionally, if you are also using Active Directory/LDAP as an ID repository, a role can contain Active Directory/LDAP user accounts and groups.
Creating user accounts

The Samsung service creates a default account when your organization signed up. This account is automatically added to the sysadmin role, giving you full administrator permissions. See "Default user accounts" on page 102 for information on how this default account is created.

Using this default account, you can create user accounts one-at-a-time or you can bulk import up to 10,000 user accounts from an Excel xls/xlsx spreadsheet or a CSV file.

To create user accounts one at a time:

1 Log in to Admin Portal using your administrator account.
2 Click **Users > Add User**.
3 Enter a login name and select a suffix.
   A user name can be composed of any of the UTF8 alphanumeric characters plus the symbols + (plus), - (dash), _ (underscore), and . (period).
   The suffix is the part of your account name that follows “@”. For example, if your account name is bob.smith@acme.com, then the suffix is acme.com. By default, the suffix associated with your default account is populated. See “Using login suffixes” on page 337 for more information on suffixes.
   All login suffixes are displayed in the list, including the login suffix for any Active Directory/LDAP domains you are using.
   **Important:** If you select the login suffix for an Active Directory/LDAP domain, the account is not added to Active Directory/LDAP. The account’s Source column will indicate Samsung directory as the source, rather than Active Directory/LDAP.
4 Enter the email address and display name for the user.
5 Enter a password.
   This is a one-time password for the user to log in to Samsung SDS IAM & EMM user portal when you select “Require password change at next login (recommended)” in the Status settings. This password is replaced with the password created by the user.
   The default minimum password requirements are:
   - 8 characters
   - 1 numeric character
   - 1 upper case letter
   - 1 lower case letter
   See “Setting password controls” on page 199 to change the default requirements.
6 Select the status settings.
The following settings are specific to creating a new user account:

<table>
<thead>
<tr>
<th>Option</th>
<th>Does this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send email invite for user portal setup</td>
<td>Sends an email to users with an invitation to log in to the Samsung SDS IAM &amp; EMM user portal. The email contains a link to the user portal and their account login name and a one-time password. If you don’t want to send the invitation when you create the account, you can send one later using the Invite Users button. You can customize the email message sent when you invite users—see “Customizing the email messages contents and logos” on page 293.</td>
</tr>
<tr>
<td>Send SMS invite for device enrollment</td>
<td>Sends an SMS message to the mobile number in the account to help the user enroll the device. The message contains a link that downloads the Samsung SDS IAM &amp; EMM client to the phone. Users then install the Samsung SDS IAM &amp; EMM client and proceed with enrolling the device. You can also send the SMS invitation using the Invite Users button.</td>
</tr>
</tbody>
</table>

The following settings can be updated at a later time:

<table>
<thead>
<tr>
<th>Option</th>
<th>Does this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked</td>
<td>Locks the account. Set this field to prevent the user from logging in to the user portal or launching applications from the Samsung SDS IAM &amp; EMM client.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>Overrides the default “Maximum password age” policy setting. Regardless of the “Maximum password age” setting, the password for this account never expires. The default maximum password age for user service accounts is 365 days. You use the Account Security Policies &gt; Password Settings &gt; Maximum password age policy on the Policies tab in Admin Portal to reset this value. <strong>Note:</strong> This setting and the “Require password change at next login” setting are interdependent. If you select one, the other is reset.</td>
</tr>
</tbody>
</table>
## Creating user accounts

### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Does this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require password change at next login (recommended)</td>
<td>Forces users to create a new password the next time they log in. When you select this option, users are immediately prompted to create a new password the next time they log in to the user portal with their current password. The user is also subject to any password reset policy controls and settings you have enabled (see Setting password controls). This setting is reset as soon as the user logs in and creates a new password. <strong>Note:</strong> This setting and the “Password never expires” setting are interdependent. If you select one, the other is reset.</td>
</tr>
<tr>
<td>Is Service User</td>
<td>Select this option for users who should NOT belong to the Everybody role. For example, you might select this option for contract or temporary users. See Managing roles for more information.</td>
</tr>
</tbody>
</table>

(optional) Enter information for the Profile and Organization fields.

7 Click **Create User**.

A notification will be sent to the newly created user via your selected method.
Bulk import user accounts

You use an Excel spreadsheet or CSV file in conjunction with Admin Portal to bulk import user accounts. The user account file can contain up to 10,000 accounts.

You should run bulk user import after you have assigned the web applications to the roles. The Samsung service sends the login email message to the new users immediately after creating the account. If you do not have the applications assigned, the users are presented with an empty Apps screen when they log in to the Samsung SDS IAM & EMM user portal.

To create the file, use the CSV file template provided (Option 1 in the import wizard) or create the file from scratch. Ensure that your user account file follows these guidelines:

- Each field must have a header.
- Headers must match exactly as shown in the following table, including upper case characters and spaces.

<table>
<thead>
<tr>
<th>Field</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Enter the full user name, including the login suffix in the form &lt;login name&gt;@&lt;loginsuffix&gt;</td>
</tr>
<tr>
<td></td>
<td>The login suffix must exist already.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>You can specify one email address only.</td>
</tr>
<tr>
<td>Display Name</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>You can enter the display name in Excel using either format:</td>
</tr>
<tr>
<td></td>
<td>• first last</td>
</tr>
<tr>
<td></td>
<td>• last, first</td>
</tr>
<tr>
<td></td>
<td>If you are editing the CSV file, use quotes if you specify the last name first (for example, “last, first”).</td>
</tr>
<tr>
<td>Description</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Do not use punctuation. Limit is 128 characters.</td>
</tr>
<tr>
<td>Office Number/Mobile number/ Home number</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>You must enter the area code. You can enter domestic US numbers in the following forms:</td>
</tr>
<tr>
<td></td>
<td>• 1234567890</td>
</tr>
<tr>
<td></td>
<td>• 123-456-7890</td>
</tr>
<tr>
<td></td>
<td>Use E.164 number formatting to enter an international number.</td>
</tr>
</tbody>
</table>
|                        | If you are using the phone or text message options for multifactor authentication, the Office and/or Mobile numbers must be accurate or the user will not be able to log in.
Using the Bulk User Import wizard to add Samsung service accounts

After you create the file, use the Bulk User Import wizard to create the accounts.

To add Samsung service accounts using the Bulk User Import wizard:
The procedure assumes you have already created the Excel or CSV file.

1 Log in to Admin Portal.
2 Click Users > Bulk User Import > Browse.

3 Navigate to the file.
4 Click Open > Next.
5 Review the entries.
The first 15 records are displayed. Use this display to ensure you have formatted the entries correctly.
6 Click Next.
The Samsung SDS IAM & EMM directory - Bulk Import Report field is automatically populated with your email address. Change the address if you want the email address to go to someone else.

7  Click **Confirm**.

After the wizard completes the import, the Samsung service sends two email messages:

- A Samsung SDS IAM & EMM directory - Bulk Import Report. This email message is sent to the email account that you had specified to receive the report. It indicates how many new users were specified in the file and how many were successfully added. An explanation is provided for each failed account.

- A Samsung SDS IAM & EMM directory - New User Account. This email message is sent to each user account created. The message includes a link to the user portal and a one-time password. When users open the link, they are prompted to create a new password (unless you have configured otherwise).

**Note**  You can customize this letter—see “Customizing the email messages contents and logos” on page 293.
Creating roles and adding users to roles

You create roles to assign applications, administrative rights, and policies to sets of users. Only members of the sysadmin role or members of role with the Role Management permission can create a role.

To create a role with users, administrative rights, and applications:

1. Log in to Admin Portal.
2. Click Roles > Add Role.
3. Enter the role name and a description.
   
   Note You cannot rename roles.
4. Click OK.
5. Click Members > Add.
   
   The Add Members dialog box appears.
6. Start entering the user name, Active Directory/LDAP group name, or an existing Samsung service role.
   
   Matching entries display.
   
   You must select a universal or security group. Local or distribution groups are not supported. If you have existing local or distribution groups and need help converting them to universal or security groups or if you want to confirm your existing group type, see KB-6906: How to convert a distribution group to a security group.

   If you are using Active Directory/LDAP as an identity store, all of the matching users accounts and groups in the Users container in the domains that the connector can “see” in the tree or forest are displayed. See “Supporting user authentication for multiple domains” on page 356 for more information on which domains can be “seen.”

   After you add an Active Directory/LDAP user or group to a role, the name is not shown on the Users page until the user logs in to the user portal or enrolls a device.
7. Select the check box associated with the account, group, or role you want to add and click Add.
8. Click Administrative Rights > Add.
9. Select the check box associated with the rights you want to assign.
   
   See “Admin Portal administrative rights” on page 252 for information on the rights.
10. Click Add.
11. Click Assigned Applications > Add.
The Add Applications page shows the applications you have added to your tenant. See Application Configuration Help for application-specific configuration instructions. Select the check box associated with applications you want to assign.

Click Add > Save.
Verifying users have access to Samsung SDS IAM & EMM user portal

It is important to verify that users have access to the Samsung SDS IAM & EMM user portal. This access is required for users to access additional SaaS applications and enroll mobile devices.

Users in the Everybody role automatically have access to the Samsung SDS IAM & EMM user portal. By default, users are added to the Everybody role. If you have users that are not in the Everybody role, you must explicitly deploy the Samsung SDS IAM & EMM user portal application to the role in which those users are members.
Possible next steps

You might be interested in the following scenarios:

- “How to install a Samsung SDS IAM & EMM connector” on page 48
- “How to configure Mobile Device Management or single sign-on only” on page 18
- How to create a policy set and assign it to users
- “How to enroll devices” on page 22
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- “How to configure user self-service options” on page 44
Possible next steps
Common tasks

Samsung SDS IAM & EMM User Suite provides many features and configuration options. The following topics provide instructions for configuring the more commonly used features:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- How to create a policy set and assign it to users
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- “How to configure user self-service options” on page 44
- “How to install a Samsung SDS IAM & EMM connector” on page 48
- How to configure Integrated Windows authentication
- How to configure browsers for silent authentication
How to configure Mobile Device Management or single sign-on only

This scenario is intended to inform system administrators about the differences between using Samsung service for Mobile Device Management or single sign-on only. You can use Samsung SDS IAM & EMM for single sign-only or also as a mobile device management. By default, the Samsung service is selected to provide mobile device management. The configuration setting is located in the Admin Portal > Policies > Mobile Device Policies > Device Management Settings > Use the Samsung service for mobile device management drop-down options (Yes or No).

You can have only one mobile device management provider. You cannot have some devices managed by the Samsung service and other devices managed by another mobile device management provider.

Note You must have a Samsung Knox Premium license to use the Samsung service for mobile device management.

This scenario includes the following topics:
- “Using Samsung SDS IAM & EMM for Mobile Device Management” on page 18
- “Using Samsung SDS IAM & EMM for single sign-on only” on page 19
- “Possible next steps” on page 19

Using Samsung SDS IAM & EMM for Mobile Device Management

When you use the Samsung service for mobile device management, it allows you to do the following:
- Define mobile device policies that the Samsung service automatically installs in the devices (see “Managing device configuration policies” on page 221).
- Send commands from Admin Portal to the device (see “Using the device management commands” on page 165).

Note When you use the Samsung service for mobile device management, the device owner can also send many of the same commands to the devices from the Samsung SDS IAM & EMM user portal.
- Deploy native iOS and Android mobile applications to the devices from Admin Portal.
- Simplify device enrollment for users with Samsung Knox devices that have the Universal Mobile Device Management Client (UMC) installed (see “Enabling Samsung KNOX UMC login suffix updates” on page 348 for the details).
Using Samsung SDS IAM & EMM for single sign-on only

If you already have mobile device management from another provider in place, you can configure the Samsung service for single sign-on only. When you configure the Samsung service for single sign-on only, it provides the following services:

- You can create policy sets to set the following policies:
  - Device Management Settings
  - Device Enrollment Settings
  - Account Security policies for authentication, password reset, and password settings
  - Application policies

- You can assign web applications to the user portal.

- You can assign web applications with single sign-on to users with Android, Knox-enabled devices, and iOS devices.

  Users must install the Samsung SDS IAM & EMM client on the device to open the web applications from the device. Optionally, users can also assign web applications to their devices from the user portal. You manage this option using the Application policies—see “Managing Application policies” on page 220.

When you use another service for mobile device management, Samsung service does not provide the following services:

- If you installed the Samsung SDS IAM & EMM connector, the IAM & EMM Mobile and Installed Applications tabs are not added to the device’s Active Directory Properties.

  This means you cannot send the device management commands to a device from Active Directory Users and Computers.

- The IAM & EMM Mobile tab is not added to the user’s Active Directory Properties.

  This tab lists the devices enrolled by the user and lets you send commands to the devices.

- Group policy profiles are not installed on the devices.

  On Android devices, the Samsung SDS IAM & EMM client does not have a Setup screen.

Users can still install the Samsung SDS IAM & EMM client on their devices and get single sign-on to the web applications you assign to them. However, they are limited to which commands they can send to the device (see “Using the device management commands” on page 165).

Possible next steps

You might be interested in the following scenarios:

- How to create a policy set and assign it to users
- “How to enroll devices” on page 22
• “How to define authentication requirements” on page 28
• “How to configure and deploy applications to users” on page 34
• How to install the Samsung SDS IAM & EMM Browser Extension
• “How to configure user self-service options” on page 44
• “How to install a Samsung SDS IAM & EMM connector” on page 48
How to configure Mobile Device Management or single sign-on only
How to enroll devices

This scenario is intended to guide system administrators through the procedures for enabling users to enroll devices. Users typically enroll their own devices, but system administrators must enable the relevant settings. When devices are enrolled, you can manage them in Admin Portal, install mobile device policies, and deploy mobile applications to specified devices.

This scenario includes the following topics:
- “Enabling users to enroll devices” on page 22
- “Possible next steps” on page 24

Enabling users to enroll devices

Before a user can enroll a device, you must provide this user with the relevant policy set.

To enable users to enroll devices:

1. Log in to Admin Portal.
2. Click Roles.
3. Create a new role or select an existing role.
4. Click Members > Add.
5. On the Add Members window:
   a. Enter the first few letters of the user, role, or Active Directory/LDAP account/group you want to add and click the search icon.
   b. Select the relevant user, role, or Active Directory/LDAP account/group and click Add.
6 Click Save to save the changes.

7 Click Policies and either click Add Policy Set or select an existing policy.

8 Click Mobile Device Policies > Device Enrollment Settings.

9 Select Yes in the Permit device enrollment policy.

10 Configure the remainder of the policy settings.

These settings apply regardless of whether you use the Samsung SDS IAM & EMM policy service or Active Directory group policies to manage device configuration policies:

<table>
<thead>
<tr>
<th>Device enrollment control settings</th>
<th>To enforce these limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of devices a user can enroll</td>
<td>Limit the number of devices a user can enroll.</td>
</tr>
<tr>
<td>Permit noncompliant devices to enroll</td>
<td>Prevent noncompliant devices from enrolling. To enable users to enroll a noncompliant device, select Yes in the drop-down menu. Open the tool tip for more information on this policy.</td>
</tr>
<tr>
<td>Permit Android device enrollments</td>
<td>Use the drop-down menu to select All to allow users to enroll any Android device, Filter to define enrollment rules for Android devices, None to prevent users from enrolling Android devices, or &quot;--&quot; (Not configured) to use the default setting. The default is All.</td>
</tr>
<tr>
<td>Permit iOS device enrollment</td>
<td>Use the drop-down menu to select All to allow users to enroll any iOS device, Filter to define enrollment rules for iOS devices, None to prevent users from enrolling iOS devices, or &quot;--&quot; (Not configured) to use the default setting. The default is All. If you select Filter, click Add Rule to specify a filter, condition, and value for each rule. Click Add to save each rule.</td>
</tr>
</tbody>
</table>

11 Click Save.

12 Click Policy Settings.

13 Specify the policy assignment:
   - All users and devices
     Applies this policy to all users and devices enrolled on the Samsung SDS IAM & EMM identity platform.
   - Specified Roles
     Click Add to select the roles to which you want this policy applied.
   - Sets (NOT applicable for unenrolled devices)
     Specify the set type (currently only Device type is supported) for enrolled devices and the set parameters (iOS devices, corporate owned devices, etc.). Sets are a collection of devices, users, etc.
**Important:** Do not use this option when configuring a policy for device enrollment. Sets only apply to enrolled devices. If you assign this policy to users who do not already have a device enrollment policy (via the All Users and Devices or Specified Roles option), device enrollment will fail.

14 Click **Save**.

**Possible next steps**

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to define authentication requirements” on page 28
- How to create a policy set and assign it to users
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- How to configure user self-service options
- “How to install a Samsung SDS IAM & EMM connector” on page 48
How to create a policy set and assign it to users

This scenario is intended to guide system administrators through the procedures for creating a policy set and assigning it to users. There are no default policy sets and numerous policy settings. The policy settings are categorized into mobile device policies, user security policies, and application policies. This scenario address the creation of a policy set only and does not address any specific policy settings.

You can apply a policy set to all users with accounts in the Samsung service, to users in specific roles only, or to users in specific collection parameters.

The policy set goes into effect when the user logs in to the user portal. If you are using the Samsung service for mobile device management, the device configuration policies are installed when the user enrolls the device.

This scenario includes the following topics:

- Creating a policy set and assigning it to users
- Using hierarchical policy sets
- Possible next steps

Creating a policy set and assigning it to users

To create a policy set and apply it to one or more roles:

1. Open Admin Portal, click Policies, and click Add Policy Set.
2. Enter a name for the policy set.
   
   You can use uppercase and lowercase characters, spaces, numbers, and most special characters (you cannot, for example, use the forward and backward slash). The Name text box outline turns red if you enter an illegal character.
4. Configure the Set policy to active option if necessary.
   
   This option is enabled by default.
5. Specify the policy assignment:
   
   - All users and devices
     
     Applies this policy to all users and devices enrolled on the Samsung SDS IAM & EMM identity platform.
   
   - Specified Roles
     
     Click Add to select the roles to which you want this policy applied.
   
   - Sets (NOT applicable for unenrolled devices)
How to create a policy set and assign it to users

Specify the set type (currently only Device type is supported) for enrolled devices and the set parameters (iOS devices, corporate owned devices, etc.). Sets are a collection of devices, users, etc.

**Important:** Do not use this option when configuring a policy for device enrollment. Sets only apply to enrolled devices. If you assign this policy to users who do not already have a device enrollment policy (via the All Users and Devices or Specified Roles option), device enrollment will fail.

6 Click **Save**.

**Using hierarchical policy sets**

You can apply multiple policy sets to the same role. For example, you might create a global policy set to define basic policies for all users and then create more policy sets for a subset of those users.

The Samsung service reads the policy sets from bottom to top on the Policy page when it installs the policies in a device. If the same policy has different settings in different policy sets, the setting in the last policy set—the top-most—is applied.

For users in multiple roles or collection parameters, the Samsung service first determines which policy sets apply to the user and then reads those policy sets from bottom to top to apply the policies. The hierarchical order of the roles has no effect upon the order in which the policy sets are read.

If you want one policy setting to be enforced over another one, drag that policy set up in the list.

**Possible next steps**

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- How to configure user self-service options
- “How to install a Samsung SDS IAM & EMM connector” on page 48
How to define authentication requirements

You can specify what authentication mechanisms your users need to provide to log in to the service, as well as if and when multifactor authentication is required. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

This scenario includes the following topics:
- “Creating authentication rules” on page 28
- “Creating authentication profiles” on page 30
- “Configuring authentication for all conditions” on page 31
- “Customizing session length and signed-in options” on page 31
- “Possible next steps” on page 32

Creating authentication rules

You create authentication rules to define the conditions in which a certain authentication profile is applied. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

To define an authentication rule:

1 Log in to Admin Portal.
2 Click Policies and select the policy you want to edit or click Add Policy Set to create a new one.
3 Click User Security Policies > Login Authentication.
4 Select Yes in the Enable authentication policy controls drop-down.
5 Click Add Rule.
   The Authentication Rule window displays.
6 Click Add Rule on the Authentication Rule window.
7 Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access the Samsung service from an IP address that is outside of your corporate IP range.

Supported filters are:

- **IP Address**: The authentication factor is the computer’s IP address when the user logs in.
  
  This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.

- **Identity Cookie**: The authentication factor is the cookie that is embedded in the current browser by the Samsung service after the user has successfully logged in.

- **Day of Week**: The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.

- **Date**: The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.

- **Date Range**: The authentication factor is a specific date range.

- **Time Range**: The authentication factor is a specific time range in hours and minutes.

- **Device OS**: The authentication factor is the device operating system.

- **Browser**: The authentication factor is the browser used for opening the Samsung SDS IAM & EMM user portal.

- **Country**: The authentication factor is the country based on the IP address of the user computer.

For the Day/Date/Time related conditions, you can choose between the user’s local time and Universal Time Coordinated (UTC) time.
8 Click the Add button associated with the filter and condition.

9 Select the profile you want applied if all filters/conditions are met in the Authentication Profile drop-down.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the Add New Profile option. See “Creating authentication profiles” on page 30.

10 Click OK.

11 Select a default profile to be applied if a user does not match any of the configured conditions in the Default Profile (used if no conditions matched) drop-down.

   Note If you have no authentication rules configured and you select Not Allowed in the Default Profile dropdown, users will not be able to log in to the service.

12 Click Save.

If you have more than one authentication rule, you can prioritize them on the Login Authentication page.

**Creating authentication profiles**

The authentication profile is where you define the required authentication mechanisms such as password, email confirmation code, mobile authenticator, etc. You use the authentication profile when you create your authentication rule.

To create an authentication profile:

1 Click Settings > Authentication.

2 Click Add Profile on the Authentication Profiles page.

3 Enter a unique name for each profile.

4 Select the authentication mechanism(s) you require and want to make available to users. See “Authentication mechanisms” on page 195 for information about the authentication mechanisms.

   For example, you can require the first challenge to be the user password and the second challenge users can choose between an email confirmation code, security question, or text message confirmation code. When you configure two different authentication mechanisms for challenge 1 and challenge 2, this is often called multifactor authentication.

5 (Optional) Select the pass-through duration. The default is 30 minutes.

6 Click OK.

If you have not created an authentication rule, see “Creating authentication rules” on page 28 to create one and associate this profile to it.
Configuring authentication for all conditions

You can require users to always authenticate, regardless of connection factors or conditions. For example, if you create an authentication profile with only the password mechanism selected and assign it to the Default Profile option, then all users (regardless of the log in computer’s IP address and browser identity cookie) will be asked to enter passwords.

To configure authentication for all conditions:

1. Log in to Admin Portal.
2. Click Policies and select the policy you want to edit or click Add Policy Set to create a new one.
4. Select Yes in the Enable authentication policy controls drop-down.
5. Select the authentication profile you want applied in the Default Profile drop down.

   The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the Add New Profile option. See “Creating authentication profiles” on page 30.

   If you have authentication rules configured, then those rules are processed first and users that do not fall under those rules will be processed using the authentication profile selected in the Default Profile.

   **Note** If you have no authentication rules configured and you select Not Allowed in the Default Profile dropdown, users will not be able to log in to the service.

6. Click Save.

Customizing session length and signed-in options

A session is that period of time during which the Samsung service accepts a previous log in from the same browser for authentication. For example, if the session length is 1 hour and the user logs in and then logs out, that user has 1 hour to access the user portal (from the same browser and machine) without needing to enter his credentials.

You can also give users the option to stay logged in, the default setting for this option, and define the maximum hours the user can stay signed in. By default, users do not have the option to stay signed in.

To change the default session length:

1. Log in to Admin Portal.
2. Click Policies and select the policy you want to edit or click Add Policy Set to create a new one.
3 Click **User Security Policies > Login Authentication**.

4 Select **Yes** in the Enable authentication policy controls drop-down.

5 Scroll to **Session Parameters** and enter the number of hours for the session length in the text box.

6 Click **Save**.

To display “Keep me signed in” on the login screen:

1 Log in to Admin Portal.

2 Click **Policies** and select the policy you want to edit or click **Add Policy Set** to create a new one.

3 Click **User Security Policies > Login Authentication**.

4 Select **Yes** in the Enable authentication policy controls drop-down.

5 Scroll to **Session Parameters** and configure the relevant **Keep me Signed In** options.
   - Select the **Allow “Keep me signed in” checkbox option at log in** option if you want users to see the “Keep me signed in” option when they log in to the Samsung service.
   - Select the **Default “Keep me signed in” checkbox option to enabled** option if you want the “Keep me signed in” checkbox enabled by default for users.
   - In the associated text box, enter the maximum number of hours users can stay signed in.

6 Click **Save**.

**Possible next steps**

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- How to create a policy set and assign it to users
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- “How to configure user self-service options” on page 44
- “How to install a Samsung SDS IAM & EMM connector” on page 48
• • • • • How to define authentication requirements
How to configure and deploy applications to users

This scenario is intended to guide system administrators through the procedures for configuring applications and deploying them to users. You need to configure and then deploy applications to users before they can use single-sign-on to access them from the user portal.

This scenario includes the following topics:
- “Configuring applications” on page 34
- “Deploying applications to users” on page 36
- “Possible next steps” on page 38

Configuring applications

This procedure highlights the general application configuration options. See Application Configuration Help for application-specific configuration instructions.

You can configure and deploy web applications (such as SAML apps, user password apps, SSO apps, etc.) and mobile applications (such as iOS App Store apps, iOS custom apps, Android Google Play apps, Android custom apps, etc.)

You must be a member of the sysadmin role or a role that has Application Management permission to configure and deploy applications.

At a high-level, to configure applications:

1. Log in to Admin Portal.
2. Click Apps > Add Web Apps or Add Mobile Apps.

3. Enter the application name in the Search field and click the Add button associated with relevant application.

   If you are adding a custom application, click the Custom tab and the Add button associated with relevant application type.
4 Confirm the Add Application action. Admin Portal adds the application.

5 Click Close to exit the Application Catalog.

The application that you just added opens to one of the application configuration pages. Where you land depends on the type of application you are configuring. For example, Web - User Password applications do not have an Application Settings option. It is best at this point to read the configuration instructions for the specific application (Application Configuration Help, ). If the application specific help content is not available, information in the following table can be useful.

<table>
<thead>
<tr>
<th>Options</th>
<th>Use to do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications Settings</td>
<td>For Web - SAML and Bookmark applications: Configure the URLs. For Web - SAML applications only, expand Additional Options to input the name or “target” that the mobile applications uses to find this application and select a security certificate. For Web- Office 365 applications: • For Office 365 version 1 applications, enter the Office 365 administrator user name and password application ID and expand Additional Options to input the name or “target” that the mobile applications uses to find this application and select a security certificate. • For Office 365 version 2 applications, enter the Office 365 administrator user name and password application ID and expand Additional Options to input the name or “target” that the mobile applications uses to find this application. Click Verify to confirm the administrator user name and password account. For iOS and Android custom in-house applications: Browse to and upload the binary file. For iOS and Android appstore applications: Enter the application package identifier. This option is not displayed for Web user - password applications.</td>
</tr>
<tr>
<td>Description</td>
<td>Modify the application name, description, and logo. See “Modifying the application description” on page 120 for an example.</td>
</tr>
<tr>
<td>User Access</td>
<td>Assign the application to one or more roles. See “Deploying applications to users” on page 36 for an overview of this process. When you specify the role, you can set the application for automatic or optional assignment—see “Configuring automatic versus optional assignment” on page 49 for the details.</td>
</tr>
</tbody>
</table>
Deploying applications to users

You must assign applications to a role before users can use single sign-on for those applications.

The Samsung service deploys web and mobile applications to members of the role or roles you select. After you assign a web application to a role, the Samsung service adds it to the role members’ Samsung SDS IAM & EMM user portal.

6 Make the necessary configurations and click **Save**.
For users with enrolled devices, the web applications are also displayed on the device as follows:

- Android and iOS devices: Web applications are displayed on the Web Apps screen in the Samsung SDS IAM & EMM client.
- On a Samsung Knox Workspace device, web applications are displayed in Samsung SDS IAM & EMM WebApps by default. You can also configure the device to show the applications in the Samsung SDS IAM & EMM client and Samsung SDS IAM & EMM WebApps.

After you assign mobile applications to a role, the Samsung service adds them to the Mobile Apps area of the Samsung SDS IAM & EMM client on the device.

You can assign applications to roles using two methods in Admin Portal:

- The User Access page in the application configuration area.
- The Assigned Applications page in the role configuration area.

To assign an application to a role using the User Access page:

1. Log in to Admin Portal.
2. Click Apps > the application you want to update.
   The application configuration page opens.
3. Click User Access.
4. Select one or more roles.
5. Select Automatic Install or Optional Install in the drop-down. By default, all applications are configured for automatic installation.
   - For web applications:
     When you specify Automatic installation, it is added automatically to the role members’ Samsung SDS IAM & EMM user portal, the Web Apps screen in the Samsung SDS IAM & EMM client, and, on Samsung SDS IAM & EMM WebApps workspace devices enabled for a Knox mode container, in the Samsung SDS IAM & EMM WebApps application.
     When you specify Optional installation, the web application is not displayed in any of these places. Instead, the application is only listed when the user clicks the Add Apps button in the user portal. If the user adds the application, it displayed among the applications deployed for automatic installation.
   - For mobile applications:
     On Android devices, only custom applications that you set for automatic installation are installed automatically on the devices. Play Store applications that you set for automatic installation are listed on the Samsung SDS IAM & EMM client Apps screen under the Recommended banner. The optional applications are listed under Optional.
Users must manually install all the deployed Play Store applications. Newly deployed applications have a “New” button indication.

On Samsung Knox Workspace devices, the custom applications set for automatic installation are installed automatically. However, if the application is configured for installation in the Knox mode container, it is not installed until the user creates the container. Users must manually install all Play Store applications, even the ones that you have set for automatic installation.

On Android for Work devices, Play Store applications that you set for automatic installation are automatically installed on to the device. In-house Android applications are not supported with Android for Work.

On iOS devices, mobile applications are displayed and managed in the Company Apps web clip. Company Apps is a web clip that is installed automatically when the device is enrolled. When the user opens the web clip, the screen lists the automatic and optional mobile applications deployed to this user.

6 Click Save.

To assign an application to a role using the Assigned Applications page:

1 Log in to Admin Portal.

2 Click Roles.

3 Select the role to which you want to assign the application

4 Click Assigned Applications > Edit.

5 Drag the application or applications in the Available pane to the Selected pane.

   The Available pane lists the applications you have already added to the Apps page in Admin Portal—it is not the full Samsung SDS IAM & EMM App Catalog.

6 Click Save.

   The next time the role members open the Samsung SDS IAM & EMM user portal or refresh their window, the application is displayed.

Possible next steps

You might be interested in the following scenarios:

- How to install the Samsung SDS IAM & EMM Browser Extension
- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- How to create a policy set and assign it to users
- How to define authentication requirements
- How to configure user self-service options
How to configure and deploy applications to users

- “How to install a Samsung SDS IAM & EMM connector” on page 48
How to install the Samsung SDS IAM & EMM Browser Extension

This scenario is intended to guide system administrators through the procedures for installing the Samsung SDS IAM & EMM Browser Extension. Some web applications require installation of the Samsung SDS IAM & EMM Browser Extension to provide single sign-on. Without the browser extension, users will not be able to open these applications. You only need to install the browser extension one time per browser type.

The browser extension is not required on mobile devices. The Samsung SDS IAM & EMM client and Samsung SDS IAM & EMM WebApps both incorporate an internal browser that provides single sign-on. When device users open an application that requires the browser extension, the application is automatically opened in the internal browser.

Browser extension dependent applications have the jigsaw puzzle symbol on the Apps page in the Samsung SDS IAM & EMM user portal.

After the browser extension is installed, the jigsaw symbol disappears.

You can install the browser extension for Internet Explorer (IE) browsers on remote Windows computers or users can install it themselves.

This scenario includes the following topics:

- Installing the Samsung SDS IAM & EMM browser extension for IE on remote Windows computers
- Options for user self installation
- “Possible next steps” on page 43

Installing the Samsung SDS IAM & EMM browser extension for IE on remote Windows computers

You can automate the installation of the Samsung SDS IAM & EMM Browser Extension (Internet Explorer version) onto remote Windows computers using a silent installation or using a Windows Group Policy Object (GPO).

To deploy the browser extension on remote Windows computers using a “silent” unattended installation or using a GPO, you need to specify the appropriate command line options and Microsoft Windows Installer (MSI) file. You can also use a software distribution
product, such as Microsoft System Center Configuration Manager (SCCM), to deploy software packages.

An automated installation may fail if remote computers do not have the appropriate configuration. If you are installing silently or from a GPO, verify that the remote Windows computers meet the following requirements:

- The computer is running a supported Windows operating system version.
- The computer is joined to Active Directory.
- The computer has sufficient processing power, memory, and disk space for the browser extension to use.
- The computer has the .NET Framework, version 3.5 SP1, or later.
- The computer has Windows Installer, version 3.1, or later.

To install the Samsung SDS IAM & EMM Browser Extension for Windows silently:

1. Open a Command Prompt window or prepare a software distribution package for deployment on remote computers.

   For information on preparing to deploy software on remote computers, see the documentation for the specific software distribution product you are using. For example, if you are using Microsoft System Center Configuration Manager (SCCM), see the Configuration Manager documentation.

2. Run the installer for the browser extension package for a 32-bit or 64-bit architecture.

   Note: If the system has a 64-bit operating system, use the 64-bit package, SamsungIEExtensionSetup(x64.msi).

   For example, on 32-bit operating systems, run the following command:
   
   msiexec /qn /i "SamsungIEExtensionSetup(x86).msi"

   On 64-bit operating systems, run the following command:
   
   msiexec /qn /i "SamsungIEExtensionSetup(x64.msi)"

To install the Samsung SDS IAM & EMM Browser Extension from a Group Policy Object:

1. Copy the SamsungIEExtensionSetup(x64.msi) files to a shared folder on the domain controller or another location accessible from the domain controller.

   If you are installing on a 32-bit architecture, the installer file name is SamsungIEExtensionSetup(x86).msi. When you select a folder for the installer file, you might want to right-click and select Share with > Specific people to verify that the folder is shared with Everyone or with appropriate users and groups.

2. On the domain controller, click Start > Administrative Tools > Group Policy Management.
3 Select the domain or organizational unit that has the Windows computers where you want to deploy the browser extension, right-click, then select **Create a GPO in this domain, and Link it here**.

For example, you might have an organizational unit specifically for Samsung SDS IAM & EMM-managed Windows computers. You can create a Group Policy Object and link it to that specific organizational unit.

4 Type a name for the new Group Policy Object, for example, **Samsung SDS IAM & EMM Browser Extension Deployment**, then click **OK**.

5 Right-click the new Group Policy Object, then click **Edit**.


7 Select Software installation, right-click, then select New > Package.

8 Navigate to the folder you selected in **Step 1**, select the .msi installation file, then click **Open**.

9 Select **Published**, then click **OK**.

10 Close the Group Policy Management Editor, right-click the **Samsung SDS IAM & EMM Browser Extension** and verify Link Enabled is selected.

By default, when computers in the selected domain or organizational unit receive the next group policy update or are restarted, the browser extension will be deployed and the computer will be automatically rebooted to complete the browser extension deployment. If you want to test deploy, you can open a Command Prompt window to log on to a Windows client as a domain administrator and force group policies to be updated immediately by running the following command:

```
gpupdate /force
```

For more information about how to configure and use Group Policy Objects, see the documentation on the Microsoft Windows website.

**Options for user self installation**

Users can install the Samsung SDS IAM & EMM browser extension using one of the following options:

- The user portal displays a banner on the Apps page above the application icons that has a link the user can click to initiate installation.

- The first time a user opens an application that requires the browser extension, the user portal opens a pop-up that prompts the user to initiate the installation.

- The systems administrator sends the link for installing the browser extension directly to users. When users click the link, the installer identifies the user’s default browser and installs the corresponding extension. The link and the browser extension files for
How to install the Samsung SDS IAM & EMM Browser Extension

Chrome, Firefox, Safari, and Internet Explorer are provided in the Downloads item in the account name drop down menu in Admin Portal.

Possible next steps
You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- “How to install a Samsung SDS IAM & EMM connector” on page 48
- How to configure Integrated Windows authentication
- How to configure browsers for silent authentication
- How to create a policy set and assign it to users
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- “How to configure user self-service options” on page 44
How to configure user self-service options

You can enable users to perform certain tasks related to their accounts. These tasks include password reset and account unlock options.

This scenario includes the following topics:

- “Configure password reset self-service options” on page 44
- “Configure account unlock self-service options” on page 45
- “Possible next steps” on page 47

Configure password reset self-service options

You can enable users to reset their passwords and specify additional authentication requirements for a password reset.

To enable the password reset self-service options:

1. Log in to Admin Portal, click the Policies tab, and select the policy set.
4. Enable the Password Reset option.

5. Limit who can reset their passwords.
   - The “Allow for Active Directory users” option enables users with Active Directory accounts who have forgotten their password to log in and reset their password. If you do not set this option, the “Forgot your password?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you will need to configure the Active Directory Self Service Settings.
How to configure user self-service options

- The “Only allow from browsers with identity cookie” option restricts password reset to those users who have already logged in successfully. If this box is not set, anybody can use the password reset options.

  The Samsung service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.

6 Select the authentication profile to specify the authentication mechanisms required for recovering from each situation.

See “Creating authentication profiles” on page 30 for more information.

7 Configure options for enabling password reset for Active Directory users.

- Select Use connector running on privileged account to run the connector under an account that has the Reset Password permission. Unless you have changed the connector account after you ran the connector installation wizard, the connector is run as a Local System account process. By default, a Local System account does not have the Reset Password permission. See “Permissions required for alternate accounts and organizational units” on page 362 to set the permission.

- Select Use these credentials to use an account with the required permission to reset the password. For example, any account in the connector’s Domain Admins group can reset another user’s Active Directory account password.

8 Set the additional policy parameters.

The additional policy parameters let you manage the following password reset behaviors:

- Maximum forgotten password resets allowed within window

  Use the drop-down list to set a maximum for the number of times users can reset their password within the capture window. If users exceed this limit, the next time they attempt to reset the password, they get a message that they have reset their password too often and must wait before attempting again.

- Capture window for forgotten password resets

  Use the drop-down list to set the time period for maximum forgotten password resets. When users exceed the number or resets in this time period, they cannot reset the password again. This value also specifies how long from the last reset attempt the user must wait before they are allowed to reset the password.

9 Click Save.

Configure account unlock self-service options

You can enable users to unlock their accounts.

To enable account unlock policies:

1 Log in to Admin Portal, click the Policies tab, and select the policy set.
How to configure user self-service options

2 Click User Security Policies > Self Service.

3 Select Yes in the Enable account self service controls drop-down.

4 Enable the Account Unlock option.

5 Limit who can unlock their accounts.
   - The “Allow for Active Directory users” option enables users with Active Directory accounts to unlock their accounts. If you do not set this option, the “Unlock your account?” link is not displayed in the login prompt for users with Active Directory accounts. If you set this option, then you will need to configure the Active Directory Self Service Settings.
   - The “Only allow from browsers with identity cookie” option restricts account unlock to those users who have already logged in successfully. If this box is not set, anybody can use the account unlock option.
     The Samsung service writes the identity cookie the first time the user logs in successfully. However, when users clear the history on their browsers, it removes this cookie.

6 Select the authentication profile to provide authentication mechanisms for users to recover from each situation.

See “Creating authentication profiles” on page 30 for more information.

7 Configure options for enabling account unlocking for Active Directory users.
   - Select Use connector running on privileged account to run the connector under an account that has the User Account Control permission. Unless you have changed the connector account after you ran the connector installation wizard, the connector is run as a Local System account process. By default, a Local System account does not have the User Account Control permission. See “Permissions required for alternate accounts and organizational units” on page 362 to set the permission.
   - Select Use these credentials and provide the account user name and password to use an account with the required permission to unlock the account. For example, any account in the connector’s Domain Admins group can unlock another user’s Active Directory account.

8 Click Save.
Possible next steps

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- How to create a policy set and assign it to users
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- “How to install a Samsung SDS IAM & EMM connector” on page 48
How to install a Samsung SDS IAM & EMM connector

The Samsung SDS IAM & EMM connector is a multipurpose software that enables secure communication between your internal network and the Samsung service.

You install the Samsung SDS IAM & EMM connector for the following purposes:

- If you are authenticating Samsung service users by using their Active Directory or LDAP account.
- Install additional Samsung SDS IAM & EMM connectors for load balancing and failover.

To integrate your Active Directory/LDAP service with the Samsung service, you need to install at least one connector on your network inside of the firewall.

You can install more than one connector for your organization to support fail-over and load balancing. You might also want to install more than one connector if you are using multiple Samsung service services. In most cases, you should install two connectors in a production environment.

**Note** You must have a Samsung Knox Premium license key to install a Samsung SDS IAM & EMM connector

This scenario includes the following topics:

- “Overall Requirements” on page 49
- “Firewall and external IP address requirements” on page 50
- “Installation and service account privilege requirements” on page 51
- “Permissions for managing mobile device objects in Active Directory” on page 52
- “Installing a Samsung SDS IAM & EMM connector” on page 53
- “Possible next steps” on page 55
How to install a Samsung SDS IAM & EMM connector

Overall Requirements

To install and configure a Samsung SDS IAM & EMM connector you need the following:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung SDS IAM &amp; EMM Management Suite installer</td>
<td>This program installs the connector, Active Directory/LDAP and group policy console extensions, and the Samsung SDS IAM &amp; EMM connector configuration program. To get the installer, you open Admin Portal, click Settings, Network, Samsung Connectors, and Add connector. Repeat this procedure every time you install a connector to ensure you get the latest version of the connector.</td>
</tr>
<tr>
<td>Host computer joined to the domain controller</td>
<td>You install the Samsung SDS IAM &amp; EMM connector on a Windows computer to establish the communications link between the Samsung service and Active Directory domain controller. If you are referencing accounts in an Active Directory tree or forest, the connector can be joined to any domain controller in the tree (it does not need to be the root). In addition, that domain controller must have two-way, transitive trust relationships with the other domain controllers. See “Supporting user authentication for multiple domains” on page 356 for the details. This computer must be in your internal network and meet or exceed the following requirements:</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2, 2012, 2012 R2, and 2016. All running 64-bit with 8 GB of memory, of which 4 GB should be available for connector cache functions.</td>
</tr>
<tr>
<td></td>
<td>• Has Internet access so that it can access the Samsung service.</td>
</tr>
<tr>
<td></td>
<td>• Has a Baltimore Cyber Trust Root CA certificate installed in the Local Machine Trusted Certificate root authorities store.</td>
</tr>
<tr>
<td></td>
<td>• Microsoft .NET version 4.5 or later; if it isn’t already installed, the installer installs it for you.</td>
</tr>
<tr>
<td></td>
<td>• Be a server or server-like computer that is always running and accessible.</td>
</tr>
<tr>
<td>Permissions on the connector machine</td>
<td>To install the Samsung SDS IAM &amp; EMM connector, you need to be the local administrator on the Samsung SDS IAM &amp; EMM connector machine. See “Installation and service account privilege requirements” on page 51 for more permissions requirements.</td>
</tr>
<tr>
<td>Firewall and external IP address requirements</td>
<td>See “Firewall and external IP address requirements” on page 50.</td>
</tr>
<tr>
<td>Execute VBScript</td>
<td>The server must be able to execute VBScript during the installation.</td>
</tr>
<tr>
<td>Web proxy server (optional)</td>
<td>If your network is configured with a web proxy server that you want to use to connect to the Samsung service, you specify this server during the installation process. The web proxy server must support HTTP/1.1 chunked encoding.</td>
</tr>
</tbody>
</table>
Firewall and external IP address requirements

All connections to the internet made by the Samsung SDS IAM & EMM connector are outbound in nature. No internet facing ingress ports are required. All outbound connections are made via TCP to either port 80 or 443.

To provide the redundancy and availability of an always available Samsung service, the destination resource, IP address, and host for outbound connections will vary over time amongst thousands of addresses. Additionally, the range of which also changes as new resources are provisioned or removed.

**Note:** Use of deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues with the Samsung SDS IAM & EMM Samsung SDS IAM & EMM connector service. In all cases, the ports and addresses discussed below should be excluded from packet inspection to allow for normal service operation.

**Option 1: Whitelist Source**

Given the variability of connection targets, the simplest whitelist configuration is typically one where filters are based on the traffic source. Specifically, configurations where you allow all outbound traffic from the host machine and account running the Samsung SDS IAM & EMM connector. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

**Option 2: Whitelist Source Ports**

You can also use a whitelist configuration where all outbound traffic on ports 80 and 443 is allowed from the host machine and account running the Samsung SDS IAM & EMM connector. This whitelist may be scoped at the machine, or machine + account, or machine + account + process level depending on the feature set of the security appliance or process in place.

**Option 3: Whitelist Destination**

In the case where destination whitelisting is required, the following outbound ports and addresses are required for hosts running the connector service:

<table>
<thead>
<tr>
<th>Port numbers</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>*.emm.samsung.com</td>
</tr>
<tr>
<td>443</td>
<td>*.windows.net</td>
</tr>
<tr>
<td>80</td>
<td><a href="http://www.public.trust.com">www.public.trust.com</a></td>
</tr>
<tr>
<td>80</td>
<td>mscrl.microsoft.com</td>
</tr>
<tr>
<td>80</td>
<td>privacy-policy.trust.com</td>
</tr>
</tbody>
</table>
How to install a Samsung SDS IAM & EMM connector

For Azure data center resources, you need to add the Microsoft Windows Azure Service Bus service to the whitelist. Use the following URL to get the most current list of IP addresses: www.microsoft.com/en-us/download/details.aspx?id=41653

**Note** We recommend that you whitelist all available IP ranges in the above list to ensure that any changes made by Samsung SDS IAM & EMM or within Microsoft Azure will allow the connector service to communicate with the Samsung service. Microsoft regularly updates their list, which necessitates periodic maintenance of any destination whitelist accordingly.

### Installation and service account privilege requirements

Installing the connector requires file installation (running the installer.exe file) and registration (running ProxyUI.exe for the first time). File installation requires local administrative permissions on the connector machine because you need to copy files to Program Files, set up Windows service, modify registry, etc. Registration also requires local administrative permissions because you need to write the settings to registry. However, additional permissions may be required depending on what you want to do.

### Services | Required Rights and Privileges
--- | ---
Manage mobile device objects in Active Directory | To manage mobile device objects in Active Directory, you need to delegate the necessary permissions to the connector.
  - At least read permission to the container that has the Samsung service user accounts.
  - A broader set of permissions (write all properties, delete, read permissions, and all validated writes) on the container that has the enrolled device objects.
  See “Permissions for managing mobile device objects in Active Directory” on page 52.

Synchronize deleted objects in Active Directory with Samsung service | When you delete users in Active Directory and want this deletion synchronized with the Samsung service, you have two options:
  - You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains.
  - Delegate read permissions to the service account for the deleted objects container in the corresponding domain.
If you do not take one of the above actions, users deleted in Active Directory will be listed on the Users page in Admin Portal until you manually delete them. However, they will not have access to any Samsung SDS IAM & EMM User Suite functionalities.

<table>
<thead>
<tr>
<th>Port numbers</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>ocsp.verisign.com</td>
</tr>
<tr>
<td>80/443</td>
<td>Azure data centers</td>
</tr>
</tbody>
</table>
All Active Directory accounts are members of the built-in Authenticated Users group. By default, members of the Authenticated Users group have list and read permissions on most Active Directory objects. The specific permissions vary for different object types and Active Directory versions.

You can also install the Samsung SDS IAM & EMM connector on non-Active Directory computers. In this case, you can use local (i.e. non-Active Directory) accounts.

Permissions for managing mobile device objects in Active Directory

If you want to manage your mobile device objects in Active Directory, you need to delegate the necessary permissions to the Samsung SDS IAM & EMM connector:

- At least read permission to the container that has the Samsung service user accounts.
- A broader set of permissions on the container that has the enrolled device objects.

To set the Read access permission to the user account container or organizational unit:

1. Open Active Directory Users and Computers, select the user account container, and open the Properties.
2. Select the Security tab and then click Add to add the user account you are using to run the connector service. Click OK after you add the user account.
3. Click the user account in Group or User Names and click the Allow box for the Read permission.
4. Click OK.

To set the permissions to the enrolled device object container or organization unit:

1. Open Active Directory Users and Computers, select the enrolled device object container, and open Properties.
2 Select the **Security** tab then the **Advanced** button to view the Advanced Security Settings.

3 Click **Add** to add a new permission entry.

4 Click **Object Types** and confirm that the object type for your connector is selected.

5 Click **OK**.

6 Navigate to Select User, Computer, Service Account, or Group window.

7 Enter the first few characters of the object name into the object name text box then click **Check Names**.

8 Select the object name for your connector and click **OK**.

9 Select **Allow** for the Create Computer objects permission.

10 Click **OK**.

11 Click **Add** to add another permission entry.

12 Click **Object Types** and confirm that the object type for your connector is selected.

13 Select the object name for your connector and click **OK**.

   The Permission Entry for MobileDevices window opens.

14 Click the **Allow** box for the following permissions on the Object tab:
   - Write all properties
   - Delete
   - Read permissions
   - All validated writes

15 Click **OK** on the succeeding windows to exit the Properties configuration windows.

### Installing a Samsung SDS IAM & EMM connector

You install the Samsung SDS IAM & EMM connector to integrate your Active Directory/LDAP service with the Samsung service. The connector allows you to, among other things, specify groups whose members can enroll and manage devices. It also monitors Active Directory/LDAP for group policy changes, which it sends to the Samsung service to update enrolled devices.

To install the connector, you must first get the Samsung SDS IAM & EMM Management Suite package then run the installation wizard.

To install a connector on a host computer:

1 Log in to the host computer with an account that has sufficient permissions to install the connector.
How to install a Samsung SDS IAM & EMM connector

2 Open Admin Portal.

3 Click Settings > Network > connector > Add connector.

4 Click 64-bit in the Download pane.
   The download begins.

5 Extract the files.

6 Double-click the installation program: Cloud-Mgmt-Suite-rr.rr-winaa.exe
   In the file name, rr.rr indicates the release version and aa indicates the processor
   architecture (64-bit).

7 Click Yes to continue if the User Account Control warning displays.

8 Click Next on the Welcome page.

9 Select I accept the terms of the license agreement, then click Next.

10 Select the components to install, then click Next.
   The default is to install all components. Use the description on the installation UI
determine what you want to install.

11 Click Install > Finish to open the Samsung SDS IAM & EMM connector configuration
   wizard.

12 Click Next on the Welcome page.

13 Type the administrative user name and password for your Samsung SDS IAM & EMM
   account, then click Next.
   Note  Click the Advanced button if you need to change the default URL—https://
   cloud.samsungemm.com/— for the Samsung service. In most cases, you should not
   change this address.

14 Click Next unless you are using a web proxy server to connect to Samsung service.
If you are using a web proxy service, select the associated check box and specify the IP address, port, user name, and password to use.

15 Specify the monitored domains and relevant credentials to synchronize deleted objects in Active Directory/LDAP with Samsung service, then click Next.

When you delete users in Active Directory and want this deletion synchronized with the Samsung service, you have two options:

- You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains.
- Delegate read permissions to the service account for the deleted objects container in the corresponding domain.

If you do not take one of the above actions, users deleted in Active Directory will be listed on the Users page in Admin Portal until you manually delete them. However, they will not have access to any Samsung SDS IAM & EMM User Suite functionalities.

The configuration wizard performs several tests to ensure connectivity.

16 Click Next if all of the tests are successful.

As the final step, the connector registers your customer identifier with your tenant, then runs in the background as a Windows service.

17 Click Finish to complete the configuration and open the connector configuration panel, which displays the status of the connection and your customer ID.

18 Click Samsung SDS IAM & EMM connector to view or change any of the default settings.

19 Click Close.

After you have installed and configured at least one connector, you can use either Admin Portal or your default browser to log on to the Samsung service. The next time you log on and see the welcome page, select Don’t show this to me again, then click Close.

Possible next steps
You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- How to create a policy set and assign it to users
- “How to enroll devices” on page 22
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
• "How to configure user self-service options" on page 44
• How to configure Integrated Windows authentication
• How to configure browsers for silent authentication
How to install a Samsung SDS IAM & EMM connector
How to configure Integrated Windows authentication

The Samsung service lets you accept an Integrated Windows authentication (IWA) connection as sufficient authentication for users with Active Directory accounts when they log in to Samsung SDS IAM & EMM user portal or Admin Portal. With IWA enabled, the browser uses the current user’s Active Directory information to prove its knowledge of the password through a cryptographic exchange with the in-process web server built into the connector. IWA is not available to users with Samsung service accounts.

To use IWA, users must be inside the corporate IP range and specify their login suffix in the portal URL in the following form:
- Samsung SDS IAM & EMM user portal: https://cloud.samsungemm.com/my?customerID=<loginsuffix>

where <loginsuffix> is the login suffix for their account (see “Using login suffixes” on page 337).

This scenario includes the following topics:
- Configuring IWA
- Certificate Requirements
- Verifying IWA over HTTPS
- Using IWA with identity cookie
- Using IWA to authenticate application access
- Disabling IWA
- Possible next steps

Configuring IWA

Integrated Windows authentication (IWA) is enabled by default when you install the connector. However, you may want to make configuration changes (for example defining your corporate IP range) and ensure that browsers used by your users are configured properly for IWA. See “Configuring browsers for silent authentication” on page 1.

Using HTTPS is the most secure means by which IWA can work, as a result, the ability to use HTTP only will be removed in a future version of the product. To ensure the continued security of the platform, note the following:
- If you have enabled IWA (on by default when you install a connector) but have not setup your Corporate IP Range (under Settings> Network> Corporate IP Range), IWA will not work.
- If you cannot use IWA on the corporate network over HTTP with SSL, then disable IWA by de-selecting “Enable Web Server” on the Samsung SDS IAM & EMM connector Configuration window.
To configure IWA:

1. Log in to Admin Portal.
2. Click **Settings > Network > Samsung SDS IAM & EMM connector.**
3. Select the relevant connector or add a new one.

You can modify the following settings:

<table>
<thead>
<tr>
<th>Setting or property</th>
<th>Change to do the following</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable web server</td>
<td>The default value is Enabled. This setting supports Integrated Windows Authentication and Office clients. If you disable the web server, you cannot change the DNS Hostname, HTTP Port Number and HTTPS Port number values.</td>
</tr>
<tr>
<td>DNS Hostname</td>
<td>The default is the connector’s host computer’s name. You can enter a DNS short name here or the fully qualified domain name in the IE local intranet zone.</td>
</tr>
<tr>
<td>IWA Detection Timeout</td>
<td>The length of time Integrated Windows Authentication (IWA) will wait for response from the connector. The default is 10 seconds.</td>
</tr>
<tr>
<td>HTTP Port Number</td>
<td>The default port is 80. Port 80 is the standard port. If you change the port number to a non-standard number (for example, 111), Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know the implications.</td>
</tr>
<tr>
<td>HTTPS Port Number</td>
<td>The default port is 8443. Port 8443 is the standard port. If you change the port number to a non-standard number, Firefox and Chrome may require additional configuration because these browsers block some non-standard ports. Do not change the port number unless you know about the implications.</td>
</tr>
<tr>
<td>connector Host Certificate</td>
<td>The host certificate used by the Samsung SDS IAM &amp; EMM connector must be issued by a trusted issuer. You can trust the tenant specific CA we have created for you by default, or provide your own. Click <strong>Upload</strong> to upload a certificate into the Samsung service. See <strong>Certificate Requirements</strong> for certificate requirement information. Click <strong>Download</strong> to download a certificate you have previously uploaded. Click <strong>Download your IWA root CA certificate</strong> to save a copy of the certificate from the IWA root CA.</td>
</tr>
</tbody>
</table>

4. Click **Save.**
How to configure Integrated Windows authentication

5 Click Corporate IP Range.

6 Click Add to enter a your corporate IP range.

   IWA will not work for users whose computers are outside of the defined corporate IP range.

7 Click OK.

Certificate Requirements

If an Enterprise CA is already available and trusted by your endpoints, you can upload a certificate issued by this CA using Admin Portal. Samsung service then disseminates the certificate to the connector. The issued certificate must satisfy the following requirements:

- Certificate is issued by a trusted CA
- SAN or Subject matches machine’s short name
- SAN or Subject matches the machine’s hostname as configured in the management portal
- Key Usage field must enable “Digital Signature” and “Key Encipherment”
- Enhanced Key Usage field must enable “Server Authentication”

The certificate must be available as a PKCS#12 file (.pfx or .p12) which includes the private key to upload it to the Samsung service. For additional information, please refer to the following Microsoft article How to Export a Certificate with the Private Key.

Verifying IWA over HTTPS

You can test the validity of the Samsung SDS IAM & EMM connector host certificate by doing the following:

1 Open a web browser from an endpoint machine

2 Navigate to the following address: https://<yourconnectorhostname>:<httpsport>/iwa/ping

   Replace <YourConnectorHostname> and <httpsport> with the corresponding values. For example: https://2008WindowsServer:8443/iwa/ping

3 Look for the green certificate in the browser.
How to configure Integrated Windows authentication

Using IWA with identity cookie

When you enable Integrated Windows Authentication (IWA), the Samsung service can write a cookie in the current browser after a successful IWA-based log in. The Samsung service checks the browser for this cookie when the user logs in to the user portal. As long as the cookie is there, the user is not prompted for multifactor authentication.

To use IWA with identity cookie:

1. Log in to Admin Portal.
2. Click Policies and select the relevant policy set.
4. Click the Enable authentication policy controls drop-down and select Yes.
5. Select a default authentication profile (in the Default Profile dropdown) for the Samsung service to use if IWA is not available and other authentication conditions are not met.

See Creating authentication profiles for more information on authentication profiles.

6. Enable the Allow IWA connections option (enabled by default) in the “Other Settings” area.
7. Enable the Set identity cookie for IWA connections option.

This option tells the Samsung service to write a cookie in the current browser after a successful IWA-based log in.

2. Click Save.

Using IWA to authenticate application access

You can configure the Samsung service to use IWA to override all application specific authentication requirements. For example, you can configure the Box application to require two authentication challenges if users are accessing the application from inside the
network. However, you can tell the Samsung service to ignore those authentication requirements if IWA is available.

To allow IWA for applications that require authentication:

1. Log in to Admin Portal.
2. Click **Policies** and select the relevant policy set.
3. Click **User Security Policies > Login Authentication**.
4. Click the **Enable authentication policy controls** drop-down and select **Yes**.
5. Select a default authentication profile (in the **Default Profile** dropdown) for the Samsung service to use if IWA is not available and other authentication conditions are not met.

   See [Creating authentication profiles](#) for more information on authentication profiles.
6. Enable the **Allow IWA connections** option (enabled by default) in the “Other Settings” area.
7. Enable the **IWA connections satisfy all MFA mechanisms** option.

   This option tells the Samsung service to allow IWA to override all application specific authentication requirements.
8. Click **Save**.

### Disabling IWA

IWA is not required for manual authentication using Samsung SDS IAM & EMM. If you cannot use IWA on the corporate network, you can disable it.

To disable Integrated Windows authentication:

1. Log in to Admin Portal.
2. Click **Settings > Network > Samsung SDS IAM & EMM connectors**.
3. Select the relevant connector.
4. Unselect the **Enable Web Server** option.
5. Click **OK**.

### Possible next steps

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
How to configure Integrated Windows authentication

- How to create a policy set and assign it to users
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
- How to configure user self-service options
How to configure browsers for silent authentication

Silent authentication applies to Integrated Windows Authentication (IWA) and certain RADIUS authentication methods. For silent authentication to work when logging in to the Samsung SDS IAM & EMM user portal or Admin Portal, a few browser configuration tasks may be necessary.

- **Firefox**: Either set `network.negotiate-auth.allow-non-fqdn` to True or add the connector host name to the `network.negotiate-auth.trusted-uris` list of trusted sites (see Configuring Firefox to allow silent authentication).

- **Internet Explorer**: Make sure Integrated Windows Authentication (IWA) is enabled, and then in most cases silent authentication works without further configuration. Additional details are included here in case you need to make some configuration changes (see Configuring Internet Explorer security zones).

- **Chrome** and **Safari**: In most cases, silent authentication works without further configuration. Additional details are included here in case you need to make some configuration changes (see Configuring Google Chrome on Windows for silent authentication).

**Note**  Silent authentication works as installed with Windows Firewall. If you are using a different firewall system, be sure to allow traffic on the port specified in Samsung SDS IAM & EMM connectors in Settings in Admin Portal. By default, this port is 80.

This scenario includes the following topics:

- Configuring Firefox to allow silent authentication
- Configuring Internet Explorer security zones
- Configuring Edge to allow silent authentication
- Configuring Google Chrome on Windows for silent authentication
- Possible next steps

Configuring Firefox to allow silent authentication

To enable silent authentication for users logging in to the Samsung SDS IAM & EMM user portal or Admin Portal, you must import the tenant root CA to the browser and do one of the following in the users' browser:

- If you did not change the connector host name to a fully qualified domain name (by default it is not), you set `network.negotiate-auth.allow-non-fqdn` Preference Name to true.

  **Note** By default, the host name used by the Samsung service uses the format of http://hostname, where hostname is the host name of the connector.
If you did change the connector host name to a fully qualified domain name, you need to add the fully qualified domain names for the connector host computers to the `network.negotiate-auth.trusted-uris` Preference Name.

You can add the fully qualified domain names as a— for example, `mycompany.com` (do not enter a character)—or list each one individually. Listing them individually is more secure. However, you must remember to add the fully qualified domain name every time you add a new connector host.

To configure silent authentication in Firefox using `network.negotiate-auth.allows-non-fqdn`:

1. Open Firefox.
2. Type `about:config` as the target URL.
3. Type `neg` in the Filter field.
4. Select `network.negotiate-auth.allows-non-fqdn`. If it is set to false, right-click and select **Toggle**. If it is already set to true, do not change it.
5. Close the about:config tab and close Firefox.

To configure silent authentication in Firefox using `network.negotiate-auth.trusted-uris`:

1. Open Firefox.
2. Type `about:config` as the target URL.
3. Type `neg` in the Filter field.
4. Select and right click `network.negotiate-auth.trusted-uris` and select **Modify**. Enter a comma-separated list of the fully qualified domain name for each connector as string values, then click **OK**.

   For example, if you have two connectors—`hosta.mycompany.com` and `hostb.mycompany.com`—you click Modify, enter the following and click OK.
   `hosta.mycompany.com,hostb.mycompany.com`

   The less-secure alternative would be to enter just the domain name. For example, you would click Modify, enter the following and click OK.
   `mycompany.com`
5. Close the about:config tab and close Firefox.

**Configuring Internet Explorer security zones**

For users to be authenticated silently when they use Internet Explorer to open the Samsung SDS IAM & EMM user portal or Admin Portal two conditions must be met:
How to configure browsers for silent authentication

- Internet Explorer must have integrated Windows authentication enabled. For details, see “Enabling Integrated Windows Authentication” on page 66.

- If you are using a fully qualified domain name (FQDN) URL, the connector must be in the local intranet Internet Explorer security zone or explicitly configured as part of the local intranet security zone.

For Internet Explorer, a server is recognized as part of the local intranet security zone in one of two ways:

- When the user specifies a URL that is not a fully qualified DNS domain name. For example, if you access an application with a URL such as http://acme/index.html, Internet Explorer interprets this as a site in the local intranet security zone.

  **Note** By default, the connector host name is not a fully qualified DNS domain name. The Samsung service uses the format of https://hostname, where hostname is the host name of the connector.

- When the user specifies a URL with fully qualified name that has been explicitly configured as a local intranet site in Internet Explorer (see instructions below). For example, if you access an application with a URL such as http://acme.mycompany.com/index.html, Internet Explorer interprets this as a site that is not part of the local intranet unless the site has been manually added to the local intranet security zone.

Depending on whether users log on to Web applications using a local intranet URL or a fully-qualified path in the URL, silent authentication may require modifying the local intranet security zone in Internet Explorer.

**Enabling Integrated Windows Authentication**

Use the following procedure to enable silent authentication on each computer.

To enable Integrated Windows Authentication for Internet Explorer:

1. Open Internet Explorer and select **Tools > Internet Options**
2. Click the **Advanced** tab.
3. Scroll down to the **Security** settings.
4. Check the **Enable Integrated Windows Authentication** box.
5. Restart Internet Explorer.

**Adding a web site to the local intranet security zone**

By default, the Samsung SDS IAM & EMM connector host name is not a fully qualified domain name. When this is the case, you do not need to add the URL—https://hostname—to the local intranet, and users get silent authentication when they log in to the Samsung SDS IAM & EMM user portal or Admin Portal.
However, if you change the connector host name to a fully qualified domain name, you need to add the connector host FQDN URL (https://hostname.domain.com) in each user’s Internet Explorer Local Intranet before they can get silent authentication.

To add the connector host FQDN URL to the Internet Explorer local intranet:

1. Open Internet Explorer and select **Tools > Internet Options**
2. Click the **Security** tab.
3. Click the **Local intranet** icon.
4. Click **Sites**.
5. Click **Advanced**.
6. Type in the URL https://hostname.domain.com in the text box and click **Add**. Then click **Close**.
   
   **Note** If there is a URL in the text box already, either delete it our click **Add** to save it.
7. Click **OK** to accept the local intranet configuration settings, then click **OK** to close the Internet Options dialog box.

**Configuring Edge to allow silent authentication**

When using Microsoft Edge to open the Samsung SDS IAM & EMM user portal or Admin Portal, users can only be authenticated silently when the browser has integrated Windows authentication enabled. For details, see “Enabling Integrated Windows Authentication” on page 66.

For Edge, a server is recognized as part of the local intranet security zone when the user specifies a URL with a fully qualified name that has been explicitly configured as a local intranet site in Edge (see instructions below). For example, if you access an application with a URL such as [http://acme.mycompany.com/index.html](http://acme.mycompany.com/index.html), Edge interprets this as a site that is not part of the local intranet unless the site has been manually added to the local intranet security zone.

**Enabling Integrated Windows Authentication**

Use the following procedure to enable silent authentication on each computer.

To enable Integrated Windows Authentication for Edge:

1. Open the Windows Settings and search **Internet Options**.
   
   The following window opens.
How to configure browsers for silent authentication

2 Click **Local intranet > Sites**.

3 Click **Advanced**.

4 Enter the tenant specific URL into the Websites text box.
5 Click Close.

**Configuring Google Chrome on Windows for silent authentication**

In most cases, silent authentication works for Google Chrome without additional configuration, if the connector host name is available in your DNS.

**Possible next steps**

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- “How to define authentication requirements” on page 28
- “How to configure and deploy applications to users” on page 34
- How to create a policy set and assign it to users
- How to configure user self-service options
Advanced Tasks

Samsung SDS IAM & EMM User Suite provides many features and configuration options. Many are commonly used, while others are advanced features and typically performed by fewer people. See Common tasks for the commonly used scenarios.

The following topics provide instructions for configuring the more advanced features:

- How to configure inbound provisioning
How to configure inbound provisioning

You can synchronize user data from specified systems to Active Directory using Samsung SDS IAM & EMM inbound provisioning. This feature is currently in the beta phase and we only support synchronization from Workday. As a beta feature, you must contact Samsung SDS IAM & EMM Support to turn it on.

If you have existing Workday users in Active Directory, we perform a lookup at sync time using the Workday ID and Active Directory SamAccountName. Users with these matching data are considered the same user and paired up accordingly.

This scenario includes the following topics:

- Prerequisites
- Configuring Workday
- Adding source
- Defining provisioning rules
- Synchronizing Data
- Attribute Mapping
- Possible next steps

Prerequisites

Before you start configuring inbound provisioning on Admin Portal, confirm that you have done the following:

- Configured Workday for inbound provisioning. See Configuring Workday.
- Populated the relevant user data in Workday.
- Contacted Samsung SDS IAM & EMM Support to enable this feature.
- Installed the Samsung SDS IAM & EMM connector. See How to install a Samsung SDS IAM & EMM connector.

Configuring Workday

You must configure Workday for inbound provisioning before you start configuring Admin Portal. The high level steps for configuring Workday are:

- Creating an integration system user
- Creating a security group
- Assigning the integration system user to the security group
- Configuring security group options
- Activating security policy changes
Creating an integration system user

You will need the integration system user name and password when adding the Workday source in Admin Portal.

To create an integration system user:

1. In the Workday Workbench, enter “create user” in the search box, and then click the Create Integration System User link.

2. Provide a user name and password for a new Integration System User.
   Make note of the user name and password because you will need this information to configure the source in Admin Portal.

3. Leave the Require New Password at Next Sign In option unchecked, because this user will be logging on programmatically.

4. Leave the Session Timeout Minutes with its default value of 0, which will prevent the user’s sessions from timing out prematurely.

5. Click OK.

Creating a security group

This procedure helps you to create an unconstrained integration system security group.

To create a security group:

1. Enter “create security group” in the search box, and then click the Create Security Group link.

2. Select Integration System Security Group—Unconstrained from the Type of Tenanted Security Group drop-down list, to create a security group to which members will be explicitly added.
3 Click OK.

Assigning the integration system user to the security group

You are now ready to assign the integration system user to the security group.

To assign the integration system user to the security group:

1 Enter “edit security group” in the search box, and then click the Edit Security Group link.
2 Search for the security group using the Security Group search box and select it.
3 Click OK to add it.

Configuring security group options

This procedure allows the systems administrator to grant to the new security group permissions for Get and Put operations on the objects secured by the following domain security policies:

- External Account Provisioning
- Worker Data: Public Worker Reports
- Worker Data: All Positions
- Worker Data: Current Staffing Information
- Worker Data: Business Title on Worker Profile

To configure security group options:

1 Enter “domain security policies” in the search box, and then click the Domain Security Policies for Functional Area link.
2 Search for “system” and select the System functional area.
3 Click OK.
4 Expand Security Administration in the list of security policies for the System functional area and select the External Account Provisioning domain security policy.
5 Click the **Edit Permissions** button.

The Edit Permissions screen opens.

6 Add the new security group to the list of security groups with Get and Put integration permissions.

7 Repeat steps 1 to return to the screen for selecting functional areas. This time, search for “staffing” and select the Staffing functional area.

8 Click **OK**.

9 Expand **Worker Data: Staffing** in the list of security policies for the Staffing functional area and repeat steps 5 and 6 for each of these remaining security policies:

   - Worker Data: Public Worker Reports
How to configure inbound provisioning

- Worker Data: All Positions
- Worker Data: Current Staffing Information
- Worker Data: Business Title on Worker Profile

10 Click OK.

Activating security policy changes
To activate the security policy changes:

1 Enter “activate” in the search box and click the Activate Pending Security Policy Changes link.
2 Enter a comment for auditing purposes.
3 Click OK.
4 Enable the Confirm check box.
5 Click OK.
Adding source

You must contact Samsung SDS IAM & EMM Support to set the inbound provisioning entitlement on your tenant before you can see the configuration options on Admin Portal.

To add and configure a source:

1. Log in to Admin Portal.
2. Click **Settings > Users > Inbound Provisioning**.
3. Click **Add Source** to start defining the Workday service information.
   
   The Provisioning Source window opens.
4. Select the source environment type for which you are configuring.
   - **Workday (Integration)**: Select if you are configuring the synchronization or a test environment.
   - **Workday (Production)**: Select if you are configuring the synchronization for a production environment.
5. Select the **Enable** check box to enable the feature.
6. Enter a **Name** for this source.
7. Enter the Workday server URL in the specified format (https://<workday_cloud_host_name>/ccx/service/<tenant>) into the **URL** field.
   
   Sample production URL: https://wd-sample-services.workday.com/ccx/service/companyFoo
   
   If you are setting up a test environment (you have selected Workday (Integration) in step 4), then you must append _pt1 to the URL.
   
   Sample integration URL: https://wd-sample-services.workday.com/ccx/service/companyFoo_pt1
8. Enter the Integration User Name appended with @ and your tenant ID.
   
   For example if the integration user name in Workday is johnIntegrationUser and your tenant ID is fooCompany, then you must enter johnIntegrationUser@fooCompany here.
   
   See [Creating an integration system user](#) for instructions on generating the user name.
9. Enter the **Integration Password**.
10. Click **Verify** to verify the integration user name and password combination.
11. Click **OK**.
   
   Your configured source is listed in the Sources table.
Defining provisioning rules

You can define more than one rule for each source. You must first add and configure a
 rule for each source.

To define a provisioning rule:

1 Log in to Admin Portal.

2 Click Settings > Users > Inbound Provisioning.

3 Click the + icon associated with the source you have previously configured.

4 Enter a Name for this rule.

5 Select a Provisioning Rule Mode:
   - Active -- Makes a rule active. Not recommended until you have finished all
     configurations. You must activate a rule before synchronizing.
   - Preview -- (not working for the beta release) Sets the rule in preview mode. Select
     this option for a production environment to verify the user mapping between
     Workday and Active Directory before you make the rule Active.
   - Inactive -- Sets the rule as inactive. Recommended until you have finished all
     configuration steps. You can come back to this option and activate the rule when you
     are ready.

6 Select the Target Selection Rule to define the users to which these rules apply.

7 Click Next to define the target directory and active directory organizational unit (OU).

8 Select your target directory from the Target drop-down list.

9 Expand your directory in the Domain area to see the organizational units and select the
   OU to which you want user accounts synchronized.

10 Click Next to map the attributes.

11 Review the required and automatically mapped attributes:
   - Cn
   - DisplayName
   - EmployeeId
   - SamAccountName
   - UserPrincipalName (you must enter the domain manually)

12 (Optional) Click Add and select the Target Attribute (attribute name in Active
   Directory) to add more attributes.
   - If there is only one match in Workday, then no corresponding Workday attributes are
     displayed; click Add again to add the attribute and view the mapping in the table.
   - If more than one Workday attributes can be mapped to the selected Active Directory
     attributed, then select a corresponding Source Attribute (attribute name in Workday)
from the drop-down list; click Add again to add the attribute and view the mapping in the table.

See Attribute Mapping for information on the more obscure attributes.

Continue mapping attributes until all necessary attributes are mapped.

**Important:** Scripting for attribute mapping is not supported for the beta release.

13 Click Next to configure additional provisioning rule options.

14 The following options are enabled by default:
   - Set user’s manager attribute -- If enabled, users’ manager attributes in Workday will be synchronized to Active Directory.
   - Disable user in AD if worker employment status is terminated -- If enabled, users with the terminated employment status in Workday is automatically disabled in Active Directory.

15 Enter the following information for new users:
   - The email address to which we will send all new users’ temporary passwords. This should typically be a system administrator address.
   - Specify the **Password Type** for the system generated passwords associated with the new user accounts.
     - Static: Uses the same password for all new users. If you select this option, you must specify the **Password**.
     - Generated: The system randomly generates different passwords for each new user.
   - Enable the **Require password change at next login** option to require that new users change their passwords after the initial log in using the auto generated passwords.

16 (Optional) Specify the Active Directory group to which you want users added. This option assigns the users to the selected Active Directory group.
   a Verify that the Add users to groups check box is enabled.
   b Select the Add button within the Active Directory Group Options area. The Add Active Directory Group window opens.
   c Confirm that the appropriate source is selected.
   d Start entering the group name into the Search box to find the group.
   e Select the group and click Add.

17 (Optional) Select **Map Workday Provisioning Groups to Active Directory Groups** if you want to map specific Workday provisioning groups to Active Directory groups.
   a Select the Map Workday Provisioning Groups to Active Directory Groups check box is enabled.
   b Select the associated Add button.
c Select the **Provisioning Group Name** from the drop-down list.

d Confirm that the appropriate source is selected.

e Start entering the group name into the Search box to find the group.

f Select the group and click **Add**.

18 Click **Save** to save the rule configuration.

The provisioning rule has been configured and the rule is listed in the Sources table.

19 Click the rule to change its status if you did not set the rule to Active in step 5.

20 Click **Save**.

**Synchronizing Data**

After you have configured the source and provisioning rule, you are ready to synchronize user data from Workday to Active Directory. You have the option to manually trigger full or incremental syncs or schedule incremental syncs. Full syncs are time and resource intensive so it must be triggered manually and we recommend doing it only when necessary. For the initial sync, you must perform a full one. You can only schedule incremental syncs.

To trigger a full sync:

1 Log in to Admin Portal.

2 Click **Settings > Users > Inbound Provisioning**.

3 Confirm that you have the source and provisioning rule configured and click the **Settings** tab located next to the Sources tab.

4 Select **Full** in the Manual Sync Options area.

5 Select the source environment in the associated drop-down list.

6 Click **Run Sync**.

To schedule an incremental sync:

1 Log in to Admin Portal.
2 Click Settings > Users > Inbound Provisioning.

3 Confirm that you have the source and provisioning rule configured and click the Settings tab located next to the Sources tab.

4 Enable the Run incremental sync automatically check box.

5 Specify how frequently you want to run the sync in the Frequency text box.

6 Click Add to select source from which want the data.

7 Click Add again to add the source.

8 (Optional) Enable the Send report on sync completion check box if you want to receive a sync report and enter an email address.

9 Click Save.

Attribute Mapping

Most attributes map logically. However, a few attributes may require additional guidance. This table documents those attributes.

<table>
<thead>
<tr>
<th>Active Directory Attributes</th>
<th>Possible Workday Attributes</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>C, Co</td>
<td>Alpha2WorkCountry or Alpha3WorkCountry</td>
<td>Options for mapping country code. Alpha2 maps to a 2 character country code (for example, US). Alpha3 maps to a 3 character country code (for example, USA).</td>
</tr>
<tr>
<td>CountryCode</td>
<td>Numeric3WorkCountry</td>
<td>Use if the country code is numeric.</td>
</tr>
<tr>
<td>L</td>
<td>WorkMunicipality</td>
<td>Maps to the user’s city</td>
</tr>
<tr>
<td>Mail</td>
<td>WorkEmail</td>
<td>Maps to the user’s email address</td>
</tr>
<tr>
<td>Sn</td>
<td>LastName</td>
<td>Maps to the user’s last name</td>
</tr>
<tr>
<td>St</td>
<td>WorkRegion</td>
<td>Maps to the street name</td>
</tr>
</tbody>
</table>

Important: Scripting for attribute mapping is not supported for the beta release.

Possible next steps

You might be interested in the following scenarios:

- “How to configure Mobile Device Management or single sign-on only” on page 18
- “How to enroll devices” on page 22
- How to create a policy set and assign it to users
- “How to define authentication requirements” on page 28
How to configure inbound provisioning

- “How to configure and deploy applications to users” on page 34
- How to install the Samsung SDS IAM & EMM Browser Extension
Services and components overview

The Samsung SDS IAM & EMM User Suite is a set of services that simplify provisioning applications, managing users, setting policies, and managing remote devices.

This sections contains the following topics:

- “Component summary” on page 84
- “Which software is installed and where” on page 87
- “Supported web and device browsers” on page 89
- “Supported devices” on page 90
- “Foreign language support” on page 91
- “Logging in to the user and administrator portals with silent authentication” on page 92
- “Samsung SDS IAM & EMM user portal overview” on page 93
- “Selecting an identity repository” on page 94
- “Selecting a policy service” on page 95
Component summary

The Samsung service is composed of the following services, web portals for administrators and users, and mobile applications users can install on their iOS and Android devices.

**Policy Service**: A service that provides integrated mobile security management. You configure policies for managing mobile device settings and the Samsung service automatically installs the policies in enrolled devices.

You can also use the Active Directory Group Policy Management Editor to set mobile device policies. See “Selecting a policy service” on page 95 to learn more about your options.

**App Catalog**: The set of SaaS web applications ready for immediate assignment to users. Application templates are also provided so you can also assign your own web and mobile applications and free applications from Google Play or the Apple App Store. See
“Managing applications” on page 116 when you are ready to start adding applications to your Samsung service and deploying them to users.

- **Samsung CA**: A certification authority that generates certificates for devices when you use the Samsung SDS IAM & EMM policy service for device policy management. The certificates are automatically generated when you enable wi-fi, VPN, or Exchange ActiveSync policies and select certificates for authentication. The certificates are automatically installed when the user enrolls the device.

- **Admin Portal administrator portal**: Admin Portal is the web portal you use to configure the Samsung service, deploy web applications, manage users, generate reports, and monitor user activity. If you are using the Samsung service for mobile device management, you use Admin Portal to manage the enrolled devices too.

- **Samsung SDS IAM & EMM user portal**: The Samsung SDS IAM & EMM user portal is your users’ interface to the Samsung service. They open the user portal from their computer’s browser to open the web applications deploy to them, monitor their activities, and manage their Samsung service profile. If you use the Samsung service for mobile device management, users can also self-manage their devices from the user portal.

- **Samsung SDS IAM & EMM client**: A free mobile application for Android and iOS devices that users install on their devices to enroll their devices in the Samsung service. It provides single sign-on to the applications you deploy to them.

  The Samsung SDS IAM & EMM client includes a browser that is opened in place of the device’s default browser for web applications that require a browser extension to provide single sign-on. This lets users run the same applications they open from their desktop browser on their devices. If the web application does not require the browser extension, the application opens in the user’s selected browser.

- **Samsung SDS IAM & EMM WebApps application** (not shown): A free mobile application that users with Samsung Knox Workspace devices install in their Samsung Knox container. It provides single sign-on to the web applications you assign to the user from inside the container.

- **Samsung SDS IAM & EMM Browser Extension** (not shown): A free browser add-on that’s required to provide single sign-on for some applications. The user portal prompts the user to install the extension when the user opens one of these applications. The Samsung SDS IAM & EMM user portal helps to provide Samsung SDS IAM & EMM Browser Extension installation instructions for Firefox, Windows Explorer, Chrome, and Safari browsers.

  The browser extension can also be used to add applications that are not listed in the Samsung SDS IAM & EMM App Catalog. See “Adding web applications by using Samsung SDS IAM & EMM Infinite Apps” on page 134 for the details.

The Samsung SDS IAM & EMM also includes the optional Samsung SDS IAM & EMM connector. This is a software package you install on Windows computers inside your firewall that lets you use your Active Directory/LDAP accounts to authenticate users with Active Directory/LDAP accounts for access to the administrator and user portals. Optionally, this lets you use the following:

- Active Directory Certificate Service to generate user and computer certificates.
- Active Directory Users and Computers to manage devices.
- Windows Group Policy Management to manage mobile device policies.

See “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355 to download and run the installer.

You install one set of connectors when all of the Samsung service users are in domain trees or forests that have two-way, transitive trust relationships between the domain controllers. If your organization has multiple, independent domain trees or forests, you install a separate sets of connectors for each tree or forest. See “Supporting user authentication for multiple domains” on page 356 for the details.

When you use the connector to authenticate Active Directory users, the installer includes the following extensions:

- **Active Directory Users and Computers console extension**: A console extension that adds tabs to the mobile device’s and user’s Active Directory Properties windows with Samsung service information. When you install the console extension, you can use Active Directory Users and Computers to manage devices.

- **Group Policy console extension**: A console extension that adds a comprehensive set of mobile device policies for Samsung, Android and iOS devices. When you install this console extension, you can use Windows Group Policy Management to create group policy objects and install them on mobile devices.
Which software is installed and where

The software you and your users install depends upon whether you are using the Samsung SDS IAM & EMM User Suite for single sign-on, mobile device management, or both. After you have made that decision, the components you install depend upon whether you are using the Samsung SDS IAM & EMM directory or Active Directory/LDAP to store user account and device data.

Using the Samsung SDS IAM & EMM User Suite for single sign-on

When you use the Samsung SDS IAM & EMM User Suite for single sign-on only with the Samsung SDS IAM & EMM directory as your identity store, there is nothing for you to install. In this environment, you use Admin Portal to assign the web applications and create the user accounts and roles in the Samsung directory. In this case, the users log in to the Samsung SDS IAM & EMM user portal from their browser to open the applications with single sign-on.

**Note** It may be necessary for users to install the Samsung SDS IAM & EMM Browser Extension on their browser. Many popular applications require the browser extension to provide single sign-on.

You can also provide single sign-on to the web applications from the users’ devices. In this case, the users need to install the free Samsung SDS IAM & EMM client on their devices and enroll their devices in the Samsung service.

If you want to use your Active Directory/LDAP accounts to authenticate Samsung service users, you install the Samsung SDS IAM & EMM connector and the Active Directory Users and Computers console extension on a Windows computer inside your firewall. Note that Active Directory Users and Computers is for Active Directory deployments only. See “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355 for the details.

Using the Samsung SDS IAM & EMM User Suite for mobile device management

When you use the Samsung SDS IAM & EMM User Suite for mobile device management with the Samsung SDS IAM & EMM directory as your identity store, there is nothing for you to install. You use Admin Portal to create user accounts, create policy sets for the devices, and deploy mobile applications.

The users install the free Samsung SDS IAM & EMM client on their devices and enroll their devices in the Samsung service. After the device is enrolled, the Samsung service installs the mobile device policies and mobile applications and deploys web applications. Users then use the Samsung SDS IAM & EMM client to open the mobile and web applications you deploy to them.
Users open the Samsung SDS IAM & EMM user portal from their browser to monitor their devices and send self-service commands to them. If they are also using the user portal to open the web applications you deploy to them, they may also need to install the Samsung SDS IAM & EMM Browser Extension.

If you want to use your Active Directory accounts to authenticate users, you install the Samsung SDS IAM & EMM connector, the Active Directory Users and Computers console extension, and the Group Policy console extension on a Windows computer inside your firewall. See “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355 for the details.
Supported web and device browsers

This version of Samsung SDS IAM & EMM User Suite has been tested with the following web browsers:

- **Internet Explorer:**
  - version 11 on Windows 2008 server and Windows 2012 server, and Windows 7 and Windows 8
- **Microsoft Edge:** on Windows 10
- **Mozilla Firefox:** latest version available at release
- **Google Chrome:** latest version available at release
- **Apple Safari:** 8

For silent authentication to work correctly, some web browsers need additional configuration (see “Configuring browsers for silent authentication” on page 1) or a browser extension (see How to install the Samsung SDS IAM & EMM Browser Extension).

On devices, the Samsung SDS IAM & EMM client and Samsung SDS IAM & EMM WebApps open the web applications in the native browser unless that application requires a browser extension to provide single sign-on. For these applications only, the Samsung SDS IAM & EMM client and Samsung SDS IAM & EMM WebApps open the application in its built-in browser.
Supported devices

If you are using the Samsung service for mobile device management, it supports enrolling the following devices and computers:

- An Android device running Android 4.0 or later
- Samsung Knox Workspace devices running Knox Enterprise SDK versions 1.x and Knox 2.x. This includes transparent integration with the Samsung Universal Mobile device Management Client (UMC) and the Samsung Enterprise Gateway.
- An iOS device (for example, an iPhone, iPad, or iPod Touch) running iOS 9.0 or later. Devices using iOS 8 can still be enrolled and will be supported, but they will need to use the 16.11 or earlier iOS 8 applications.
Foreign language support

Foreign language support is provided for the following components:

- Samsung SDS IAM & EMM user portal help
- Samsung SDS IAM & EMM user portal text strings.
- Admin Portal text strings

**Note**  Not all of the languages listed below are available for the Admin Portal text strings.

For the user and administrator portals, you select the language in the browser. For example, to change the language in Firefox you click the Firefox drop-down menu, click **Options**, and then click the **Content** tab. Click the **Choose** button to select a different language. To change the language in Chrome, you click the browser menu, click **Settings**, click **Show Advanced Settings**, and scroll down to **Languages** to choose another language.

For the Samsung SDS IAM & EMM client, you select the language in the device settings.

In this release, translations are provided for the following languages:

- Brazilian Portuguese
- Chinese—Simplified and Traditional
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Russian
- Spanish

Additional languages are being added over time—see the Release Notes for the most recent additions.
Logging in to the user and administrator portals with silent authentication

If you have Integrated Windows authentication enabled on the Samsung SDS IAM & EMM connector (Integrated Windows authentication is enabled by default—see “Configuring connectors” on page 296 for the details) and your browser is configured properly (see “Configuring browsers for silent authentication” on page 1) you can log in to Admin Portal without entering your Active Directory credentials. You simply add your login suffix to the Admin Portal URL in the following format:

https://cloud.samsungemm.com/manage?customerID=<loginsuffix>

For example, if your Active Directory login name is bob.smith@bigcorp.com, you would enter the following:

https://cloud.samsungemm.com/manage?customerID=bigcorp.com

Similarly, users with an Active Directory account can login to the Samsung SDS IAM & EMM user portal with silent authentication. For example, bob.smith@bigcorp.com would enter the following URL to log in to the user portal:

https://cloud.samsungemm.com/my?customerID=bigcorp.com

See “Using login suffixes” on page 337 to learn about login suffixes.
Samsung SDS IAM & EMM user portal overview

See the user web portal online help for an overview.

Note You can control which users can open the user portal and when. For example, you can configure the user portal application so that only users in specific roles can open it and they can open it only when they are on your organization’s intranet. See “Deploying the Samsung SDS IAM & EMM User Portal application” on page 117 for the details.

The user portal help also provides the user instructions for installing the Samsung SDS IAM & EMM client on devices and enrolling devices in the Samsung service.

Normally, you send users an invitation to get them started on the user portal—see “Sending invitations to users” on page 110. However, users can open the user portal from their browser by entering the following URL: https://cloud.samsungemm.com/my

After they log in, the user portal opens to the Devices page. This, in turn, prompts them to enroll their devices as soon as they open the user portal. Alternatively, users can click on the Apps page to run the web applications you assigned to them. The following image shows the Apps page in the user portal populated with web applications.

Users click Help in the title bar to open the online help and use the drop-down menu to reload privileges and, in Settings, select the default applications filter and turn off device tracking for devices.

Note For administrator accounts only, the drop-down menu also includes an option to switch from the user portal to the administrator portal.
Selecting an identity repository

The Samsung service requires an identity repository for storing data about your organization’s users and mobile devices. You can use either or both of the following:

- **Samsung SDS IAM & EMM directory**: The Samsung service includes this built-in identity repository. When you select this option, the Samsung service uses the Samsung directory account to authenticate users and, if you are using the Samsung service for mobile device management, to store the enrolled device records.

- **Active Directory/LDAP**: The Samsung service securely connects with your existing Active Directory/LDAP infrastructure through the Samsung SDS IAM & EMM connector to authenticate users when they log in to the web portals and enroll a device. The Samsung service does not replicate Active Directory/LDAP accounts or attributes in the Samsung service.

If your organization is heavily invested in Active Directory/LDAP, you can continue to use it as your primary identity store and use the same tools (for example, Active Directory Users and Computers) to manage users and mobile devices. When you use Active Directory/LDAP, your users enter their Active Directory/LDAP credentials to log in to the Samsung SDS IAM & EMM user portal and enroll devices.

You can use both identity stores simultaneously, too. For example, even if you decide to use Active Directory/LDAP as your primary identity store, the Samsung directory can provide a convenient supplemental repository for the following types of users:

- **Emergency administrators**: If there is ever a network break down to the Active Directory domain controller, no one with just an Active Directory/LDAP account can log in. However, if you create administrator accounts in Samsung directory, these users can log in to Admin Portal and the user portal and launch web applications.

- **Temporary users**: If you have temporary users—for example, customers, contractors, and partners—who need to run your web applications, it may be easier and less risky to add them as Samsung directory accounts rather than Active Directory/LDAP accounts.

---

*Cloud Manager user’s guide*
Selecting a policy service

If you use the Samsung service for mobile device management, you can use either of two resources to set mobile device policies:

- Admin Portal: You create policy sets and then link them to roles.
- Windows Group Policy Management Editor: You create a group policy object and link them to an Active Directory/LDAP organizational unit. You then specify the organizational unit in the policy set that enables users to enroll devices.

The Samsung service installs the policies on the role’s members’ devices only.

Both resources provide a comprehensive set of mobile device configuration policies for managing iOS, Android, and Samsung Knox devices. See “List of device configuration policies” on page 376 for a summary of the policies provided.

Which service you should use depends upon which identity repositories you are using.

- If some of the users who will be enrolling devices have their accounts in the Samsung SDS IAM & EMM directory and others have their accounts in Active Directory/LDAP, you must use the Samsung SDS IAM & EMM policy service to define policy sets for the devices.
- If all of your users who will be enrolling devices have their accounts in Active Directory, you can use either the Windows Group Policy Management Editor or the Samsung SDS IAM & EMM policy service.
Viewing dashboards

The Dashboard pages provide a getting started guide, handy summaries and graphical representations of your Samsung service usage.

The Dashboards page opens to the Getting Started page. This page provides guidelines for each phase of Samsung service deployment and provides links to the full descriptions in the Admin Portal online help.

Use the drop down menu to select the other dashboard pages. The Overview page, for example, provides a broad summary indicating the number of users and devices, user login locations, Active Directory/LDAP connector information, and related information.

The other Dashboards pages illustrate your mix of devices and user activities.

Use the Settings drop-down in the upper right corner to select the current page as the default.
Displaying user login activity

The map on the Overview page and the entire User Activity page show you users’ locations when they log in to the user portal and the number of logins from each location. You can then open the User Activity dashboard to zoom in. Hover over or click the location to show the login activity.

For privacy reasons, user location data in Admin Portal is based on the IP address used to access the identity platform. This IP address is often virtually assigned, so it may not reflect the actual user portal log in location. On the user portal, users have access to their device GPS so the location data is more accurate.
Interpreting the Security Overview dashboard

The Security Overview dashboard shows data related to user logins and password resets. Data includes:

- **Authentication Events (Timeline)**
  
  A timeline that shows all login events over the last 24 hours, 7 days, or 30 days. The timeline uses a color coded bar chart to indicate the different login outcomes (successful and failed logins). The timeline includes handles on either end that you can dragged to scope the data to a particular day/hour which will update all other data in the dashboard. The default scope is 7 days.

- **Authentication Events by Type**
  
  A pie chart that shows the type of events that occurred at each login or authentication challenge event (successful login, failed challenges, password resets, etc.). When you select a pie slice, the system filters the other data in the dashboard.

- **Challenges by Type**
  
  A pie chart that shows the Authentication mechanisms each login or challenge event. When you select a pie slice, the system filters the other data in the dashboard.

- **Failed Challenges**
  
  A counter that shows the number of failed authentication challenges in the range specified by the dashboard timeline. When you select this data point, the system filters the other data in the dashboard.

- **Failed Logins**
  
  A counter that shows the number of failed logins in the range specified by the dashboard timeline. When you select this data point, the system filters the other data in the dashboard.

- **Login Locations**
  
  A map that shows all login/authentication challenge events.

- **Self Service Events**
  
  A counter that shows the number of self service events enabled for the tenant in the range specified by the dashboard timeline. See How to configure user self-service options for configuration instructions. When you select this data point, the system filters the other data in the dashboard.

- **User Inspector**
  
  A dialog window that is available when you select a user in the Authentication Details table. The dialog window shows information specific to that user. For Samsung SDS IAM & EMM directory user accounts, an option to lock the account is available.
Managing users

The Users page in Admin Portal lists all of the user accounts in the Samsung service. This includes all of the users you create in the Samsung SDS IAM & EMM directory and, if you are using Active Directory/LDAP for user authentication, the Active Directory/LDAP users who have logged in to the Samsung SDS IAM & EMM user portal or enrolled devices.

Your role must have the Samsung service Users Management administrative right to view, add, and modify user accounts.

This section contains the following topics:

- “Account sources” on page 100
- “Using the Active Directory/LDAP and Samsung directory ID repositories” on page 101
- “Default user accounts” on page 102
- “Managing Samsung directory accounts from the Users page” on page 103
- “Referencing accounts from Active Directory/LDAP” on page 108
- “Sending invitations to users” on page 110
- “Deleting accounts” on page 112
- “Specifying a user’s application login settings” on page 113
- Using search filters
Account sources

The Source column indicates the ID repository that contains this user account.

- **Active Directory/LDAP**

  These users are authenticated using their Active Directory/LDAP accounts. The Active Directory/LDAP account domain is shown in the parenthesis.

  The Samsung service does not replicate Active Directory/LDAP accounts and their attributes in the Samsung service. Instead, the accounts are referenced when the user logs in to the user portal, enrolls a device, or opens a password-protected application.

  **Note** If you have multiple connectors managing multiple, independent domain trees or forests, the Source column also shows the source domain.

  To use Active Directory/LDAP as a source, you must install the Samsung SDS IAM & EMM connector. See “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355 for the details.

- **Samsung SDS IAM & EMM directory**

  These users have a Samsung SDS IAM & EMM directory account. The account information resides in the Samsung service only.

  You must create Samsung SDS IAM & EMM directory accounts explicitly before these users can log in to the user portal or enroll a device. You can add Samsung SDS IAM & EMM directory accounts individually or in bulk from a CSV file or Excel spreadsheet.
Using the Active Directory/LDAP and Samsung directory ID repositories

The Samsung service can use Active Directory/LDAP and Samsung SDS IAM & EMM directory accounts to authenticate users. You must have the connector installed to use Active Directory/LDAP accounts.

When the Samsung service receives an authentication request, it checks the ID repositories for the account name in the following order for the initial successful login session:

1. Samsung directory by name
2. Active Directory/LDAP user by user
3. Active Directory/LDAP user by email
4. samAccountName

This ID repository check order applies to the initial successful login session because browser caching and synchronization schedules between Active Directory/LDAP and Samsung service can impact this order.

To avoid users logging in to unintended repository accounts and other account related confusion, we recommend that you do not create duplicate accounts (same user name/password) in both the Samsung SDS IAM & EMM directory and Active Directory/LDAP.

If you plan to use Active Directory/LDAP as your ID repository, there are some use cases that justify creating either alternate or exclusive accounts in the Samsung service:

- Emergency access: If the network connection to the domain controller breaks down and users cannot be authenticated against their Active Directory/LDAP account, they can instead be authenticated against their Samsung SDS IAM & EMM directory account. Thus, they can continue to use the applications from the Samsung SDS IAM & EMM user portal and their devices.

- Temporary user: Some organization’s security policy can make adding a short-term user to Active Directory/LDAP a complex and time-consuming task. If you have a temporary worker who needs access to just the applications you deploy through the Samsung service, it may be simpler to add the account to Samsung service.

- Contractors or less-trusted users: Sometimes you do not want users to have the full set of privileges and access rights an Active Directory/LDAP account provides. In this case, you create the account in the Samsung directory only and these users are limited to the Samsung service applications.
Default user accounts

The Samsung service creates a default Samsung SDS IAM & EMM directory account when your organization signed up. The login name of the default account is based on the work email account entered in the Samsung service sign-up form. Generally, the login name to the default Samsung directory account is the same as the full email account—for example, if the email account is bob.smith@acme.com, the default Samsung directory account is bob.smith@acme.com.

However, if the login suffix in the email account is already in use by another Samsung service customer, a number is appended to the login suffix. The login suffix is that part of the full account name following “@”, “acme.com” in this example. For example, if “acme.com” is already in use, the default Samsung directory account would be bob.smith@acme.com.2 (or another number).

The account name is provided in the email you received after you signed up. You use this account to log in to Admin Portal and the user portal. This account is automatically added to the sysadmin role, giving you full administrator permissions in the Samsung service.
Managing Samsung directory accounts from the Users page

You create, modify, and delete Samsung SDS IAM & EMM directory accounts from Admin Portal. You create, delete, and modify Active Directory accounts from Active Directory Users and Computers only. You must be a member of the sysadmin role or any Samsung service role that has the User Management administrative right to create, delete, and modify Samsung SDS IAM & EMM directory accounts.

Admin Portal provides two actions you can initiate from a user’s account listing on this page:

- Click a user to display the user’s account details page. For Samsung SDS IAM & EMM directory accounts, you can edit the account properties from this page.
- Right-click a user to invoke a command on the user’s account.

Understanding account statuses

The Status column indicates the account state.

<table>
<thead>
<tr>
<th>Status</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>The user has either logged in to one of the portals or enrolled a device.</td>
</tr>
<tr>
<td>Invited</td>
<td>An administrator has sent an invitation to login to the user portal or enroll a device, however, the user has not responded. You can send an invitation when you create a Samsung SDS IAM &amp; EMM directory account (see “Creating user accounts” on page 5) or separately to accounts in all sources using the Invite User button (see “Sending invitations to users” on page 110). The Last Invite column indicates the date and time of the most recent invitation. When you add accounts to the Samsung directory using Bulk import (see “Bulk import user accounts” on page 8), Admin Portal automatically sends an email invitation to all new accounts by default.</td>
</tr>
<tr>
<td>Not Invited</td>
<td>The account was created in the Samsung directory but no email invitations have been sent.</td>
</tr>
</tbody>
</table>
Managing users from their account details page

When you click a user, Admin Portal displays the account details and provides a set of tabs along the left side that offer more information about the account. The following table describes each tab and the tasks you can perform after you click the link.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Contains</th>
<th>Tasks you can perform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>Account and profile information</td>
<td>For Active Directory/LDAP accounts: You cannot change any of these fields using Admin Portal. For Samsung directory accounts: You change any Account, Status, or Profile field value.</td>
</tr>
<tr>
<td>Activity</td>
<td>Event log of user’s</td>
<td>Read the user’s activity log.</td>
</tr>
<tr>
<td>Application Settings</td>
<td>Applications with custom login settings</td>
<td>You can specify login credentials for a specific application. See “Specifying a user’s application login settings” on page 113.</td>
</tr>
<tr>
<td>Assigned Applications</td>
<td>Applications assigned to the user</td>
<td>Review the applications assigned to the user. Clicking on an application opens the application configuration area.</td>
</tr>
<tr>
<td>Devices</td>
<td>Devices enrolled by the user</td>
<td>You can click the check box for one or more devices and send a command to the device. See “Using the device management commands” on page 165 for the device command descriptions. You can also click on the device to show the device’s details page.</td>
</tr>
<tr>
<td>Roles</td>
<td>Admin Portal roles in which the user is a member and the associated administrative rights</td>
<td>Review the user’s roles and the associated administrative rights for those roles. You can click on the role to see more information about that role and change the user’s roles.</td>
</tr>
<tr>
<td>Provisioned Applications</td>
<td>A list and status of applications that were provisioned to this user</td>
<td>None Provisioning is available for a limited number of applications. See the release notes for the current list.</td>
</tr>
<tr>
<td>Policy Summary</td>
<td>Listing of policies set for this users</td>
<td>None Click Policy Summary to see which policies are enabled for this user. The display indicates the setting for each policy enabled and the policy set in which the policy is enabled. Open the policy set to change the setting. <strong>Note:</strong> The mobile device policy settings are only displayed when you use the Samsung SDS IAM &amp; EMM policy service to manage device policy.</td>
</tr>
</tbody>
</table>

Modifying a user account

Click the Account tab to view a user’s account properties and status.

For Active Directory accounts, you must use Active Directory Users and Computers to update the account details. The field values are updated in the Samsung service according to
Managing Samsung directory accounts from the Users page

the Active Directory user verification interval you set in the connector (see “Using the Samsung SDS IAM & EMM connector tab” on page 373).

For Samsung SDS IAM & EMM directory accounts, you can change all of the fields in the Account tab. Be careful when you change the user’s login suffix because this affects their role memberships and policies. If you have users who will be enrolling devices or you are using mobile devices as a form of multi-factor authentication, be sure to put the device’s phone number in the Mobile Number field.

You can update the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Does this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locked</td>
<td>Locks the account. Set this field to prevent the user from logging in to the user portal or launching applications from the Samsung SDS IAM&amp;EMM client.</td>
</tr>
<tr>
<td>Password never expires</td>
<td>Overrides the default “Maximum password age” policy setting. Regardless of the “Maximum password age” setting, the password for this account never expires. The default maximum password age for user service accounts is 365 days. You use the Account Security Policies &gt; Password Settings &gt; Maximum password age policy on the Policies tab in Admin Portal to reset this value.</td>
</tr>
<tr>
<td>Require password change at next login (recommended)</td>
<td>Forces users to create a new password the next time they log in. When you select this option, users are immediately prompted to create a new password the next time they log in to the user portal with their current password. The user is also subject to any password reset policy controls and settings you have enabled (see Setting password controls). This setting is reset as soon as the user logs in and creates a new password.</td>
</tr>
<tr>
<td>Is Service User</td>
<td>Select this option for users who should NOT belong to the Everybody role. For example, you might select this option for contract or temporary users. See Managing roles for more information.</td>
</tr>
</tbody>
</table>
**User Management commands**

Admin Portal provides several user management commands. They are displayed when you right-click the name on the Users page and in the **Actions** menu on the account's details page.

<table>
<thead>
<tr>
<th>Command</th>
<th>ID repository</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Deletes a Samsung directory account from the Samsung service. The user is no longer listed on the Users page and is no longer able to log in to the Samsung SDS IAM &amp; EMM user portal or Admin Portal. For Active Directory/LDAP user accounts, the deleted account is only removed from the Users page. You must use Active Directory Users and Computers to delete the Active Directory/ LDAP account.</td>
</tr>
<tr>
<td>MFA Unlock</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Suspends multi-factor authentication for 10 minutes. Multi-factor authentication requires users to perform additional steps (such as verify their identity by email or phone call) to log in to the Samsung SDS IAM &amp; EMM user portal and Admin Portal. If the user is having trouble logging in, select the user and select this action to let the user log in with just a user name and password.</td>
</tr>
<tr>
<td>Send email invite for user portal setup</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Sends an email to the selected users with their login account name and a link to the user portal.</td>
</tr>
<tr>
<td>Send SMS invite for device enrollment</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Sends an SMS message with a link that downloads the Samsung SDS IAM &amp; EMM client to the device. The user account must have a mobile phone number to use this command.</td>
</tr>
<tr>
<td>Reload</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Updates the user’s rights immediately to put into effect any changes you have made to the account—for example, if you added the user to a new role or changed the user’s administrative privileges. Use this command immediately after modifying the user’s role or rights.</td>
</tr>
<tr>
<td>Sync All Apps</td>
<td>Active Directory/ LDAP and Samsung SDS IAM &amp; EMM directory</td>
<td>Force synchronization for all applicable applications. Note: This only applies to web applications that support provisioning. If Sync Daily is selected, the Samsung service synchronizes user accounts for all provisioned applications for this user.</td>
</tr>
</tbody>
</table>
Managing Samsung directory accounts from the Users page

<table>
<thead>
<tr>
<th>Command</th>
<th>ID repository</th>
<th>Result</th>
</tr>
</thead>
</table>
| Set Password  | Samsung SDS IAM & EMM directory only | Prompts you to reset the user’s Samsung directory account password.  
**Note:** You must reset the password for Active Directory/LDAP accounts by using Active Directory Users and Computers. In the window that appears, you enter a new password for the user. |
Referencing accounts from Active Directory/LDAP

Generally, when you use Active Directory/LDAP accounts to authenticate Samsung service users, you do not add them to the Samsung SDS IAM & EMM connector. Instead, the Samsung service automatically adds the Active Directory/LDAP accounts to the Users page when they log in to the Samsung SDS IAM & EMM user portal or enroll a device. You manage the account’s properties (for example, email address and phone numbers), entirely in Active Directory/LDAP.

However, you do need to add an Active Directory/LDAP account to a role to deploy applications to that user. You can add either the user’s Active Directory/LDAP account or the user’s Active Directory/LDAP group to the role. See “Creating roles and adding users to roles” on page 11 for the details.

Notes

- After you add an Active Directory/LDAP user or group to a role, the name is not listed on the Users page until the user logs in to the user portal or enrolls a device.
- The Samsung SDS IAM & EMM User Portal web application must be assigned to a role in which users are a member before they can log in. By default, Samsung SDS IAM & EMM User Portal is assigned to the Everybody role so this is normally not a problem. In addition, when you use the Invite User button (see “Sending invitations to users” on page 110), the role you specify is automatically added to the Samsung SDS IAM & EMM User Portal User Access settings.

You can delete an Active Directory/LDAP account from either Active Directory/LDAP or the Samsung SDS IAM & EMM directory. When you remove the account using Admin Portal, the account is automatically deleted from the Samsung service, but it is unchanged in Active Directory.

Deleted object detection from Active Directory to Admin Portal requires that each Samsung SDS IAM & EMM connector has permission to read the deleted objects container in Active Directory. For the connector to detect a user account deletion performed in Active Directory and update the Users page in Admin Portal, you need to run a few commands on each connector. After permission has been granted for each connector, deletions are automatically detected.

- If you do not have the necessary permissions to change the permissions of the deleted objects container, then run this command:

  ```
  dsacls "CN=Deleted Objects, DC=<EXAMPLE>, DC=<COM>" /takeownership
  ```

- The following command grants the Samsung SDS IAM & EMM connector permission to read the deleted objects container in Active Directory:

  ```
  dsacls "CN=Deleted Objects, DC=<EXAMPLE>, DC=<COM>" /user:administrator@<EXAMPLE.COM> / passwd:* /g <EXAMPLE>
  ```

Admin Portal user’s guide
Notifying users with Active Directory/LDAP accounts

Users with Active Directory/LDAP accounts log in to the user portal and enroll devices using their Active Directory/LDAP credentials.

To get Active Directory/LDAP users started with the Samsung service, you can send them an invitation (see “Sending invitations to users” on page 110) or you can provide the following URL to the users and tell them to use their Active Directory/LDAP credentials to log in:

https://cloud.samsungemm.com/my

They use the same credentials to enroll devices.

Simplifying logging in to Samsung service portals for Active Directory/LDAP accounts

Users with Active Directory accounts can log in to the user portal and Admin Portal without entering their user name and password from computers that are within your organization’s intranet. For example, you can log in to Admin Portal without entering your credentials by appending the login suffix to the portal’s URL as follows:

https://cloud.samsungemm.com/manage?customerid=<loginsuffix>

If you have not yet defined any other login suffixes, you can use the default suffix—your Active Directory account’s UPN suffix. For example, if your domain name is abcorp.com, you would enter the following URL to log in without entering your user name and password:

https://cloud.samsungemm.com/manage?customerid=abcorp.com

See “Using login suffixes” on page 337 to learn about login suffixes.

Similarly, users can log in to the user portal by adding the login suffix to their URL. In this case the syntax is as follows:

https://cloud.samsungemm.com/my?customerid=<loginsuffix>

Both of these methods use Integrated Windows Authentication to authenticate the user using their Active Directory credentials and require the user to be on your organizations intranet. You may need to reconfigure the default Integrated Windows Authentication settings and define IP Addresses on your Samsung SDS IAM & EMM connector to use this feature. See “Configuring connectors” on page 296 to configure a connector.

You can also define a login suffix as an alias for a long Active Directory/LDAP UPN suffix. See “Creating an alias for long Active Directory domain names” on page 339 for the details.
Sending invitations to users

If you did not send invitations for users to log in to the user portal or enroll a device, you can do so using the Invite Users button. You can send an email and/or SMS message.

<table>
<thead>
<tr>
<th>Option</th>
<th>Select to do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send email invite for user portal setup</td>
<td>Sends an email to users with an invitation to log in to the Samsung SDS IAM &amp; EMM user portal. The email contains a link to the user portal and their account login name and a one-time password. You can customize the email message sent when you invite users—see “Customizing the email messages contents and logos” on page 293.</td>
</tr>
<tr>
<td>Send SMS invite for device enrollment</td>
<td>Sends an SMS message to the mobile number in the account to help the user enroll the device. To use the SMS invitation, the user’s account must have the device’s phone number in the Mobile Number field. The message contains a link that downloads the Samsung SDS IAM &amp; EMM client to the phone. Users then install the Samsung SDS IAM &amp; EMM client and proceed with enrolling the device. To enroll a device, the user must be enabled to enroll devices—see “Enabling users to enroll devices” on page 22.</td>
</tr>
</tbody>
</table>

Sending an invitation

To send an invitation:

1. Open Admin Portal and click the Users tab.
2. Click Invite Users.
3. Filter your search by account source (Samsung SDS IAM & EMM directory or Active Directory/LDAP) and by user status.
4. Enter the first characters of the user name or Active Directory/LDAP group. The search results are filtered as you enter each character.
5. Select each account or security group that you want to invite.
   - You must select a universal or security group. Local or distribution groups are not supported. If you have existing local or distribution groups and need help converting them to universal or security groups or if you want to confirm your existing group type, see KB-6906: How to convert a distribution group to a security group.
6. Click Invite.
7. Select the invitation method -- email and/or SMS.
8 Select the user’s role.

A default Samsung directory role is “Invited Users.” If this role does not already exist, Admin Portal creates it. To select a different role, enter the role name in the text box.

User accounts that are not already a member of the role are added, and the Samsung SDS IAM & EMM User Portal application is automatically assigned to that role.

9 Click **Send Invites**.
Deleting accounts

For Samsung SDS IAM & EMM directory accounts, deleting the account means that it is disabled and no one can log in using those account credentials. For Active Directory/LDAP user accounts, the deleted account is only removed from the Users page. People can still use those account credentials to log in to the Samsung SDS IAM & EMM User Suite. You must use Active Directory Users and Computers to truly disable the account.

To delete multiple users with one command:

1. Open Admin Portal and click Users.
2. Select the relevant accounts.
3. Click Delete from the Actions menu.
4. Click Yes to confirm.
Specifying a user’s application login settings

By default, the Samsung service provides single sign-on to web applications that use SAML (Security Assertion Markup Language) or a user name and password for authentication based on the user’s Active Directory/LDAP or Samsung SDS IAM & EMM user service user name and password. You use the Applications Settings page to provide different credentials for the web applications.

If you don’t specify the user name and password for the application, users are prompted to enter them once. The Samsung service saves the credentials and silently authenticates the user for subsequent logins.

Notes

- If the application prompts the user for login credentials, you must enter the login name, however, you do not need to enter the password. If you don’t, the user is prompted to enter the password.
- If multiple users open the application with a shared user name, you must specify the login name and password.

To specify application settings for a user:

1. Open Admin Portal, click Users, and click the desired user.

2. Click the Application Settings link in the left pane and click Add.

   The Select an Application dialog box appears.

3. Select the application for which you want to specify login settings.

   Either enter a part of the application name or scroll through the list to select an application at a time.

   The Setting Username/Password dialog box appears.

4. Enter the user name or user name and password required by this application to authenticate the user.

   The user name is required for all applications. For user-password applications that prompt users for login credentials, you can optionally specify a password. For user-password applications that share a user name, the password is required.

   Note  SAML web applications just prompt you for the account name.

5. Click OK.

   The application now appears in the user’s Application Settings list. The next time the user opens this application from the user portal or the Samsung SDS IAM & EMM client on
the user’s device, the Samsung service uses these application settings to authenticate the user.

To modify a user’s existing application login setting:

1. On the **Users** page, click the user account.
2. Click **Applications Settings**.
3. In the Application Settings area, select an application. The Actions dropdown list provides options to delete or modify the application selection.
4. Select **Modify**.

   Change the user name and password as necessary and click **OK**.

To delete a user’s existing application login setting:

1. On the **Users** page, click the desired user.
2. Click **Applications Settings**.
3. In the Application Settings area, select the application or applications you want to delete. The Actions dropdown list provides options to delete or modify the application selection.
4. Select **Delete**.
5. Click **Yes**.
Using search filters

You use the user search filters to find specific users. Most of the search filters are self explanatory. The following filters require more explanations:

- All Active Users: Users who have logged in to or been invite to the Samsung service.
- All Invited Users: Users who have not logged in to or been invite to the Samsung service.
- All Non-Active Users: Users who have been application provisioned but have never logged in or have never been invited to log in to the user portal or enroll a device.

User state (active or suspended) does not have any impact on these queries.
Managing applications

You use the Apps page in Admin Portal to assign web applications to users. If you are using the Samsung service for mobile device management, you can also deploy mobile applications from the Apps page.

This section describes the following application management tasks:

- “Deploying the Samsung SDS IAM & EMM User Portal application” on page 117
- “Viewing and sorting applications in the Apps page” on page 118
- “Modifying the application description” on page 120
- “Configuring automatic versus optional deployment” on page 121
- “Setting web application access policies” on page 122
- “Managing application access requests” on page 123
- “Application symbols” on page 128
- “Removing an application” on page 130
- “Adding web applications by using Admin Portal” on page 131
- “Adding web applications by using Samsung SDS IAM & EMM Infinite Apps” on page 134
- “Adding and deploying mobile applications using Admin Portal” on page 138
- “Android for Work” on page 141

If you are managing Samsung Knox Workspace devices with a Samsung Knox container, there are some procedural and operational differences for deploying mobile and web applications. See the following sections for the details.

- “Deploying web applications to KNOX containers” on page 146
- “Deploying mobile applications to KNOX containers” on page 147
Deploying the Samsung SDS IAM & EMM User Portal application

Users use the Samsung SDS IAM & EMM User Portal application for single-sign-on access to deployed applications. If the relevant policies have been configured, then users can also use the application to enroll devices and deploy applications. By default, this application is deployed to all users in the Everybody and Invited Users roles. If the user does not belong to either of these roles, you must assign this user to a role with the Samsung SDS IAM & EMM User Portal application deployed before the user can access the user portal. See “Deploying applications to users” on page 36 for the specific deployment instructions.
Viewing and sorting applications in the Apps page

The Apps page lists all of the applications you have added to the Samsung service. You can use the column headers to sort the applications by name, type, description, and status.

**Note** Your role must have the Samsung service Applications Management administrative right to view, add, and modify applications.

**Application Status**

An application can have one of the following statuses:

- **Not Configured**: (mobile applications) All required fields have not been defined.
- **Ready to Deploy**: (web applications) All required fields have not been defined and you have not assigned the user access.
- **Deployed**: All the required fields have been defined and user access has been assigned. Users assigned to the roles with this application deployed can now access the application from their Samsung SDS IAM & EMM user portal or devices.

**Application Types**

You can also filter the applications displayed by type. Use the Search drop-down menu to select the type. The application types are defined as follows:

<table>
<thead>
<tr>
<th>Application type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android Custom Mobile</td>
<td>In-house applications for Android-based devices for which you supplied the binary file (*.apk).</td>
</tr>
<tr>
<td>Android Google Play Mobile</td>
<td>Android applications downloaded from Google Play.</td>
</tr>
<tr>
<td>Android Mobile</td>
<td>All Android applications</td>
</tr>
<tr>
<td>Bookmark Web</td>
<td>Web applications launched using a browser bookmark (URL only)</td>
</tr>
<tr>
<td>Custom Mobile</td>
<td>All iOS and Android custom applications</td>
</tr>
<tr>
<td>iOS</td>
<td>iOS applications selected from the iTunes App Store. The user downloads the application from the Apple App Store.</td>
</tr>
<tr>
<td>iOS App Store Mobile</td>
<td>iOS applications downloaded from the App Store</td>
</tr>
<tr>
<td>iOS Custom Mobile</td>
<td>In-house iOS applications for which you supplied the binary file (*.ipa).</td>
</tr>
<tr>
<td>Mobile</td>
<td>All iOS and Android in-house applications.</td>
</tr>
<tr>
<td>SAML Web</td>
<td>Web applications that use SAML for authentication</td>
</tr>
<tr>
<td>SSO Web</td>
<td>Web applications that use either SAML, WS-Federation, or vendor specific federated authentication</td>
</tr>
</tbody>
</table>
If you’re an Express customer, you can add, remove, configure, and deploy up to three web and three mobile applications. If you’re a licensed customer, you can add, remove, configure, and deploy unlimited web and mobile applications. If your license expires, all web and mobile applications return to Ready to Deploy status.

<table>
<thead>
<tr>
<th>Application type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Password Web</td>
<td>Web applications that use user name and password for authentication</td>
</tr>
<tr>
<td>Web</td>
<td>All Web applications.</td>
</tr>
</tbody>
</table>
Modifying the application description

You can modify the application’s name, description, and icon using the Description option associated with each application.

For application icon images, use a 60x60 pixel image that is one of the following file types: PNG, JPG, GIF, or ICO.

**Note** You must be a member of the sysadmin role or a role that has Application Management permission to modify an application’s configuration.

To modify an application’s settings:

1. In the **Apps** page, click the application.
2. If the Description page is not displayed, click **Description** in the left pane.
3. Click the **Name** field to modify the application’s name.
4. Click the **Description** field to modify the application’s description.
5. To change the logo icon, click **Browse** and select the desired file.
6. Click **Save**.
Configuring automatic versus optional deployment

You have two application deployment options: automatic or optional installation. These deployment options are handled differently for web and mobile applications.

- For web applications:

  When you specify Automatic installation, it is added automatically to the role members’ Samsung SDS IAM & EMM user portal, the Web Apps screen in the Samsung SDS IAM & EMM client, and, on Samsung SDS IAM & EMM WebApps workspace devices enabled for a Knox mode container, in the Samsung SDS IAM & EMM WebApps application.

  When you specify Optional installation, the web application is not displayed in any of these places. Instead, the application is only listed when the user clicks the Add Apps button in the user portal. If the user adds the application, it displayed among the applications deployed for automatic installation.

Mobile application deployed for automatic versus optional installation are handled differently—see “Adding and deploying mobile applications using Admin Portal” on page 138 for the details.
Setting web application access policies

The **Policy** link lets you specify the following access policies for web applications:

- **Restrict app to clients within the Corporate IP range:** The device or computer must be inside the organization’s intranet or within specified IP ranges.

  If the device or computer is outside the intranet or the specified IP ranges, the application cannot be opened. You set the IP ranges using the Settings page in Admin Portal—see “Setting Corporate IP ranges” on page 343.

- **Require Strong Authentication:** To open the application, the user must provide the multifactor authentication specified in the Policy Authentication settings in the Policies tab in Admin Portal.

  See “Authentication - Setting authentication policy controls” on page 193 to learn about multifactor authentication.
Managing application access requests

In most cases, you give users access to applications by assigning them to one or more specific roles. You can also selectively define a “request and approval” work flow that gives specific users or members of specific roles the ability to approve or reject access requests for specific applications. You can configure the “request and approval” work flow for any of the individual web applications for which you want to manage access requests.

By defining a work flow, users can request access to an application and, if their request is approved, be added to a role with access privileges and see their new application available when they log on to the User Portal. A designated “approver” might be a specific user or any member of a specific role. If you configure a role as an approver, the first member to respond to the request is given the authority to approve or reject the request.

For more information about defining a work flow and managing application access requests, see the following topics:

- “Configuring a request and approval work flow” on page 123
- “Creating roles for work flow administration” on page 124
- “Creating roles for approvers” on page 125
- Configuring work flow for applications
- “Requesting access to an application” on page 125
- Responding to application access requests
- “Viewing request status and history” on page 125
- Viewing request details

Configuring a request and approval work flow

As a member of the sysadmin role or a role with the Role Management administrative right, you can configure roles for all other users. Initially, only the members of the sysadmin role have the ability to enable a “request and approval” work flow and can configure the work flow for selected applications, specify the users or roles with authority to approve access requests, and identify the role or roles to which users will be assigned if their request is approved.

At a high level, the steps involved in configuring a work flow are these:

- Create one or more roles that can enable a “request and approval” work flow.
- Create one or more roles that can approve access requests for the applications that have a “request and approval” work flow.
- Select an application and click User Access to select the role into which requesters who are approved will be placed.
- Click Workflow for the selected application to enable the work flow option.
Select the user or role with authority to approve requests.

Creating roles for work flow administration

The first few steps in configuring the “request and approval” work flow are optional and involve creating one or more roles for users who are allowed to define a “request and approval” work flow for applications and the roles that can approve access requests. These steps are optional because you can choose to only allow members of the `sysadmin` role to be the users permitted to configure a work flow and members of the `sysadmin` role can assign approval authority to individual users without creating any approval roles. In most cases, however, creating roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval.

If you don’t create any intermediary roles with the appropriate administrative rights to enable a work flow, only members of the `sysadmin` role will be able to configure any “request and approval” work flow you might want to implement.

In most cases, if you are configuring a request and approval work flow for applications, you should create at least one role for users who are allowed to add, modify, or remove applications and who have permission to change which roles are assigned to a specific applications. If you don’t create a role with the Application Management and Role Management rights, only members of the `sysadmin` role can configure the “request and approval” work flow for applications.

To configure roles that can enable a work flow

1. Select **Switch to Admin Portal** from the account name menu.
2. Click the **Roles** tab.
3. Click **Add Role** or select an existing role to display the role details.
   
   If you are creating a new role, you must provide at least a unique name for the role.
4. Click **Members**, then click **Add**.
5. Type a search string to search for and select users and groups for this role.
6. Click **Administrative Rights**, then click **Add**.
7. Select the appropriate rights, then click **Add**.
   
   For example, if you are creating a role with permission to enable a work flow for access to applications, select Application Management and Role Management. You can select any additional rights you want included in this role, but you must select at least one of the required administrative rights.
8. Click **Save** to save the role.
Creating roles for approvers

You can assign approval authority to individual users. However, in most cases, creating “approver” roles for different sets of users provides greater flexibility and helps to reduce the number of requests left pending an approval. If you don’t create any intermediary roles with the appropriate administrative rights to approve access requests, only members of the sysadmin role will be able to approve access requests. You can follow the same steps described in Creating roles for work flow administration to create roles for approvers.

Keep in mind that if you are creating a role with permission to approve access requests for applications, you should include the Application Management and Role Management rights. You can select any additional rights you want included in this role.

Requesting access to an application

Any user who has an account in the Samsung SDS IAM & EMM User Suite can request access to applications that the administrator has configured with a “request and approval” work flow. No special privileges are required to make requests or approve requests.

No special privileges are required to make requests or approve requests.

To request access to an application

1 Log on to the Samsung SDS IAM & EMM user portal.

2 Click the Apps tab, if needed.

3 Click Add Apps.

4 Type a search string to find the application of interest in the catalog, then click Request.

   Only applications that have a “request and approval” work flow configured display a Request button.

5 Type the business reason for requesting access to the application, then click Yes to continue.

6 Click Close to close the App Catalog.

An email notification of your request is sent directly to the designated approver and a Requests tab will be visible the next time you go to the User Portal. You can click the Requests tab to see the status of your request. You will also receive an email notification when your request is approved or rejected. If your request was approved, the email will include a link to open the User Portal.

Viewing request status and history

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity. Depending on your role, you might
click the Requests tab from Admin Portal or the user portal to see the status of your own pending requests, the requests awaiting your approval, or the results of request activity. Regardless of the entry point for viewing the Requests tab, the list of requests includes the following information:

- **Description** provides a brief summary of the request indicating the type of access or application requested.
- **Status** displays the current status of the request as Pending, Approved, Rejected, or Failed.

You can review the request details to see the reason the request failed. For example, a request might fail if the email address for the approver or requester is invalid. A failed request might also indicate that the time allowed for taking the requested action has expired. For example, assume the request was for permission to use the root account to log on to a resource and the request was approved with a duration of 60 minutes. If the requester did not log on within 60 minutes of the request approval, the request status will display Failed.

- **Posted** displays the date and time of the most recent activity for each request.
- **Approver** displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.
- **Requester** displays the user who submitted the request.
- **Latest Log Entry** displays the most recent information recorded for the request.

**Viewing request details**

You will only see the Requests tab if you have made a request or approved a request. After you have made or responded to at least one request, you can click the Requests tab to view the status of requests and the history of request activity. Depending on your role, you might click the Requests tab from Admin Portal or the user portal to see the status of your own pending requests, the requests awaiting your approval, or the results of request activity. You can then select any request displayed on the Request tab to see request details.

If you are an approver, you can also go directly to Request Details by clicking the link in the email notifying you of the request.

Regardless of the entry point for viewing request details, the request information table displays details appropriate for the current state of the request. For example, you might see the following information:

- **Posted** displays the date and time of the most recent activity for each request.
- **Description** provides a brief summary of the request indicating the type of access or application requested.
- **Requester** displays the user who submitted the request.
• Requesters Reason displays the business reason provided by the user who submitted the request.

• Approver displays the user or role designated for approving access requests if the approval is pending or the specific user who approved or rejected the request if the request has been resolved.

• Status displays the current status of the request as Pending, Approved, Rejected, or Failed.

  Depending on the status of the request, you might see the reason the request was rejected or the reason why the request failed.

**Responding to application access requests**

There are no special privileges required to respond to requests. Anyone with access to the identity service can be designated as an approver.

If you have been designated as an approver for application access requests, you will receive email notification when others request access. You can click the View Application Request link in the email to view the request details. If you are authorized to approve the request and the request is still pending a response, the Request Details displays the options to Approve or Reject the request.

• Click Approve to approve the request and add the requester to the role selected for user access when the “request and approval” work flow was configured. If you click OK to continue with the approval, the request details are updated with the date and time the request was resolved and the approved status.

• Click Reject to reject the request and type the reason you are rejecting the request. If you click OK to continue with the rejection, the request details are updated with the reason the request was rejected, the date and time the request was resolved, and the rejected status.

After you respond to the request, the Requests tab is also updated with the latest activity and email is sent to the requester as notification of your response to the request.
Application symbols

The Samsung service displays symbols in the application icon shown in the Samsung SDS IAM & EMM user portal and in the Samsung SDS IAM & EMM client on the device. For example, if you set the application for use when the user is on the organization’s intranet only, the blocked symbol is added to the icon.

The symbols displayed in the user portal have the following meaning:

- **Key symbol**
  The key symbol means that the application is tagged as a gateway application but the assigned user is not logging in from within the corporate firewall.

- **Blocked symbol**
  The blocked symbol means that users cannot access the application. This would happen, for example, when the user logs in from outside the organization’s intranet when the application’s policy says that it is intranet-only.

- **Puzzle-piece symbol**
  The puzzle-piece symbol means that users must install the Samsung SDS IAM & EMM Browser Extension in their browser to run the application. See How to install the Samsung SDS IAM & EMM Browser Extension for the details.

- **Shared symbol**
  The shared symbol means that users never have to enter any log in credentials to access the application. The identity platform recognizes the shared credentials configuration and automatically logs users in using those credentials.
On devices, the following symbols are used:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>What it means</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚖️</td>
<td>User name and password setting is required. Users tap this symbol to enter or modify the user name and password they use to log in to this application</td>
</tr>
<tr>
<td>🚫</td>
<td>Blocked. The user cannot open this application from the device. This symbol indicates that the application is not supported on the device’s web browser.</td>
</tr>
<tr>
<td>⚠️</td>
<td>Blocked. You cannot open this application from your device. This symbol indicates that the application is only available when the user is logged in from a computer or device that is on the organization’s network.</td>
</tr>
<tr>
<td>🍀</td>
<td>Shared app. Indicates that users do not need to enter any log in credentials to access the application. The system administrator has configured for all users to use the same log in credentials, so the identity platform automatically logs users in using those credentials.</td>
</tr>
</tbody>
</table>
Removing an application

After you have deployed an application to a role you can remove it either from the Apps or Roles pages.

- From the Apps page: Click the application, click User Access, and click the role’s box to remove the check mark.

- From the Roles page: Click the Role, click the Assigned Applications Edit button, and drag the application from the Selected pane to the Available pane.

Web applications are deleted immediately from the user’s Samsung SDS IAM & EMM user portal and when the user refreshes the Samsung SDS IAM & EMM client on the device. However, mobile applications are not physically removed from the device. See “Removing a mobile application” on page 140 for the details.
Adding web applications by using Admin Portal

You can add web applications and then configure and deploy them to users in one session. Alternatively, you can add the applications to your Admin Portal Apps page and then configure and deploy them at a later time. The Status column shows the application status—see “Application Status” on page 118. You need to configure an application and deploy it to a role before users can use single-sign-on to access it.

Note Users can also add web applications (user password applications only) from the user portal. See the user portal help for user-specific information. You can, however, disable this feature—see “Managing Application policies” on page 220.

You can add web applications using the following methods:

- From the Samsung SDS IAM & EMM App Catalog—see “Adding web applications from the Samsung SDS IAM & EMM App Catalog” on page 131.
- Using a template. You can use this method if the application is not in the application catalog. See “Using a template” on page 132.
- Using Samsung SDS IAM & EMM Infinite Apps. You can use this method if the application is not in the application catalog. You can add an application using the App Capture feature in Samsung SDS IAM & EMM Infinite Apps. See “Adding web applications by using Samsung SDS IAM & EMM Infinite Apps” on page 134.
- Cloning, exporting, and importing. Cloning is a time-saver when you need to have two similar but not identical configurations for the same application. Importing and exporting are useful when you want to assign an application that you have previously assigned in another instance—for example, exporting an application from a pilot implementation and then importing it into a production environment. See “Cloning, exporting, and importing web applications” on page 132 for the details.

Adding web applications from the Samsung SDS IAM & EMM App Catalog

The Samsung SDS IAM & EMM App Catalog contains an ever-expanding list of web applications ready for assignment to users. If the web application is not in the catalog, you can open a template in the catalog and fill in the details.

To add a web application from the App Catalog:

1. Open Admin Portal and click the Apps tab.
2. Click Add Web Apps.
   The Add Web Apps window opens.
3. Use the information on the Search tab to select the application or applications.
Adding web applications by using Admin Portal

See “Using a template” on page 132 to add an application using one of the application templates.

See “Cloning, exporting, and importing web applications” on page 132 to add an application from another application that you previously exported.

4 Select the application or applications.

Click the Add button to select one or more applications.

You can continue to select categories and add more applications. You can add up to 30 applications in one session.

If you change your mind, click Remove.

5 Click Close.

If you added just one application, Admin Portal opens the configuration window for that application. If you added more than one application, Admin Portal opens the Apps page. You click the application name to configure it. Click Help for this application for the configuration instructions.

Using a template

The Samsung SDS IAM & EMM App Catalog includes templates you can open and fill in to add applications. Click the Custom tab to display the list of templates. Click the information icon associated with each template for a description.

To add an application from a template:

1 Open Admin Portal and click the Apps tab.

2 Click Add Web Apps.

This opens the Add Web Apps window.

3 Click the Custom tab.

4 Click Add for the template you want and click Yes in the confirmation window.

5 Click Close.

This closes the Add Web Apps window and opens the configuration window.

6 Click Help for this application for the configuration instructions.

Cloning, exporting, and importing web applications

You can clone an existing application to save yourself some time assigning applications that have similar but different configurations. You can also export an application you have
already configured in a test environment for example, so that you can import it into your production environment.

**Cloning an application**

When you need multiple instances of an application, each with a slightly different configuration, you can generate a clone and then modify just the properties that differ in the clone. When you create a clone, the copy has “(Cloned)” appended to the application name. Click the clone to modify the fields you need to change (including the application name).

To clone an added on the Apps page:

1. Open Admin Portal and click **Apps**.
2. Right click the application and click **Clone**.

Alternatively, you can open the application listing on the Apps page, click Actions, and then select **Clone**.

**Exporting one or more applications**

You can export one or more applications that you have already configured for use in another environment or as a back up. You can select multiple applications for export. Admin Portal creates a zip file you can then import into the other environment to add the applications.

**Note** You cannot unpack the zip file and import individual applications if you export multiple applications.

To export one or more applications:

1. Open Admin Portal and click **Apps**.
2. To export a single application, right click the application and click **Export**.

To export multiple applications, select each application and click Export in the Actions menu.

3. Transfer the zip file to the target environment.

**Importing exported applications**

You add applications that you have exported using the zip file created by the Admin Portal Export command.

**Note** You cannot unpack the zip file and import individual applications if you export multiple applications.

To add applications using a zip file created by the Export command:

1. Open Admin Portal and click **Apps**.
2. Click the **Add App** button.
3 Click the **Import** button in the Applications Catalog window.

4 Navigate to the zip file created by the Export command and click **Open**.

   “(Imported)” is appended to the application name on the Apps page.

5 (Optional) Click the application to change the name using the Description properties.

---

**Adding web applications by using Samsung SDS IAM & EMM Infinite Apps**

Infinite Apps is a feature of the Samsung SDS IAM & EMM Browser Extension that simplifies adding a SaaS user-password application that is not in the Samsung SDS IAM & EMM App Catalog. Infinite Apps provides the App Capture utility, which automatically discovers the user name and password fields on the web application log in page and adds the application to your portal Apps page. After you add the application, you can deploy it with single sign-on to user portals and devices. If the App Capture utility cannot discover the user name and password fields, it allows you to select them manually.

By default, users can also use the browser extension to add applications to their user portal Apps page and devices. You can configure this setting using the “Allow users to add personal apps” policy (see “Managing Application policies” on page 220).

This section contains the following topics:

- “Installing the Samsung SDS IAM & EMM Infinite Apps” on page 134
- “Adding a web application by using App Capture” on page 135
- “Manually adding an application by using App Capture” on page 136

---

**Installing the Samsung SDS IAM & EMM Infinite Apps**

To use the Infinite Apps feature, you must install another version of the Samsung SDS IAM & EMM Browser Extension in a Firefox browser. Infinite Apps only supports Firefox and the privacy setting must be configured for “Remember History”. After the application is captured, users can use any browser to open it from the user portal.

After you add the extension, the App Capture utility is available from the drop-down menu when you click the Samsung SDS IAM & EMM Browser Extension icon in the toolbar. Go to “Adding a web application by using App Capture” on page 135 to add an application.

To install the Samsung SDS IAM & EMM Browser Extension with Infinite Apps:

1 If Firefox is not installed on your computer, install and open it.

2 Log in to Admin Portal using your system admin account.

3 In the user name drop down menu, click **Downloads**.
4 Click the link for the Firefox browser.

5 In the pop-up window, click Allow.
   The browser displays a dialog box for installing the browser extension.

6 Click Install Now.
   A dialog box appears for restarting the browser.

7 Click Restart Now to restart the browser and finish installation.
   After the browser restarts, the Samsung SDS IAM & EMM Browser Extension icon is added to the toolbar. If it is not, right-click the toolbar, select Customize, and drag the icon to the toolbar.

Adding a web application by using App Capture

The App Capture utility is designed to discover the login user name and password fields in the login page automatically. If it can’t find them, it gives you the option to select them manually. In addition, it lets you select a third field for applications that require another login identifier, for example, a company ID.

To add an application by using App Capture:

1 Open Firefox and go to the sign-in page for the application that you want to add.

2 Click the Samsung SDS IAM & EMM Browser Extension icon in the toolbar.
   If the browser extension icon is gray, then you need to log in to the Samsung SDS IAM & EMM User Suite (user portal or Admin Portal) before continuing.

3 Click Capture.
   App Capture displays a pop up window that guides you through the capture process.
   After you click Capture, App Capture attempts to discover the user name and password fields in the login page. If it is successful, it displays the message and highlights the user name and password fields.
   If App Capture is not successful or selects the wrong fields, you need to set the fields manually. Click Set Manually and go to “Manually adding an application by using App Capture” on page 136 to capture this application.

4 Determine how the login credentials are submitted.
   If App Capture selected the user name and login fields correctly, you need to capture how users submit their credentials for this web site. App Capture supports two cases:
   • Users press the Enter key (on the keyboard) to submit their credentials.
     For example, after entering the user name and password, the user clicks the Enter key to submit their credentials to this web site.
If this is how users submit their credentials, click **Next**.

- **Users click a separate log in or sign in button to submit their credentials.**

  If the application has a separate button, such as “Sign me in” in the picture, it may require the user to click the button. In this case, you need to capture the application manually.

  Click **Set Manually** and go to “Manually adding an application by using App Capture” on page 136) to complete capturing this application.

If you are not sure which method the application requires, selecting the Enter key is the easier procedure for capturing the application and more reliable than trying to capture the submit button. After you assign the application, try opening it from the user portal. If single sign-on is not automated the next time you log in after you have provided your credentials, you will need to recapture the application using the manual method.

5 Add an additional field, if necessary.

Some web applications have a third login field that requires the user to provide additional login information—for example, a corporate ID.

If this web site does require an additional field, click **Yes** and then **Next**. Then click the additional field in the application’s login screen. App Capture highlights your selection and the pop-up window prompts you for the next entry.

**Note** You enter the value you want to put in this field (for example, your organization’s ID number for this application) in the Advanced page when you open the application details in Admin Portal. See the Advanced page description in “Configuring applications” on page 34 for the details.

6 (optional) Modify the application properties -- application name, description, and icon.

7 Click **Finish** to proceed.

8 Select where to add the application -- user portal or Admin Portal.

Adding the application to the user portal is for your use only.

Adding the application to Admin Portal allows you to assign it to other users. The Admin Portal option is only available if you are in a role that has the Application Management right.

9 Click **Submit**.

You can now assign this application to users. See “Deploying applications to users” on page 36.

### Manually adding an application by using App Capture

If you opened the application and App Capture did not find the user name and password fields or selected the wrong fields, use the following procedure to identify them.
In addition, you must use this procedure to add the application if you want to use a Submit button rather than use the Enter key to proceed with the sign-in.

To set fields manually while adding an application:

1. Open Firefox and go to the sign-in page for the application that you want to add.
2. Click the Samsung SDS IAM & EMM Browser Extension icon and click Capture from the drop-down menu.
   App Capture displays a pop up window that guides you through the capture process.
3. Click Set Manually.
4. Click the <app name> Name field to identify this application’s username field.
   For example, click the Skype Name field for Skype:

   ![App Capture screenshot](image)

   App Capture tags Skype Name as the Username field and prompts you to select the Password field.
5. Click the Password field to identify this application’s password field.
6. Select an additional login field.

   Some web applications have a third login field that requires the user to provide additional login information—for example, a corporate ID.

   If this web site does require an additional field, click Yes and then Next. Then click the additional field in the application’s login screen. App Capture highlights your selection and the pop-up window prompts you for the next entry.

   Note: You enter the value you want to put in this field (for example, your organization’s ID number for this application) in the Advanced page when you open the application details in Admin Portal. See the Advanced page description in “Configuring applications” on page 34 for the details.
7. Determine how the login credentials are submitted.

   After they enter their credentials, users either press the Enter key (on the keyboard) or click a button to submit their credentials.
Adding and deploying mobile applications using Admin Portal

- **Use keyboard Enter key event (Recommended):** Select this option when users press the Enter key (on the keyboard) to submit their credentials.
  
  Capturing the Enter key is more reliable than trying to capture a sign-in button.
  
  Click **Next** to continue.

- **Right-click the Sign in button on the Web page to capture it:** Select this option when the user must click a separate “login” or “sign-in” button to submit their credentials to this web site.
  
  After you select this option, **right-click** the login/sign-in button on the Web page to capture it, then click **Next** to continue.
  
  This option is useful if you capture using the Enter key option and deploy the application, but your users are unable to log in. Often times, recapturing the application and selecting the sign-in button option corrects the problem.

8  (Optional) Modify the application properties -- application name, description, and icon.

9  Click **Finish**

10 Select where to add the application -- user portal or Admin Portal.

   Adding the application to the user portal is for your use only.
   
   Adding the application to Admin Portal allows you to assign it to other users. The Admin Portal option is only available if you are in a role that has the Application Management right.

11 Click **Submit** to add the application to the selected portal.

12 Click **Close** when the confirmation message appears.

   Continue with “Configuring applications” on page 34 if you want to assign the application to other users.

Adding and deploying mobile applications using Admin Portal

This section describes adding and deploying mobile applications by using Admin Portal from the conceptual level. See *Application Configuration Help* for complete, application-specific configuration and deployment instructions.

The Samsung SDS IAM & EMM User Suite supports the following device operating systems:

- Android
- iOS
The mobile applications you add are displayed on the Admin Portal Apps page. You deploy native device mobile applications to sets of users based on their roles. In addition, the mobile applications that users have installed on their devices are listed in the “Installed Applications” list when you open the device details page.

For Android devices, you can deploy any free application from Google Play or an Android application for which you have the binary (.APK) file.

**Note** If you are deploying applications to Samsung Workspace devices with Knox mode version 1 containers, the application must be wrapped to be installed in the container.

For iOS devices, you can deploy any free application from the Apple App Store or an iOS application for which you have the binary—the .IPA—file. See “Installing mobile applications on iOS devices” on page 140 for the details.

If you have the binary file, you can use the Custom option in Admin Portal to add the mobile application.

**Automatic versus optional installation**

When you select role for application deployment, you can select either Automatic or Optional installation. Automatic versus optional application installation is handled differently on Android and iOS devices.

**Installing mobile applications on Android devices**

On Android devices, only custom applications that you set for automatic installation are installed automatically on the devices. Play Store applications that you set for automatic installation are listed on the Samsung SDS IAM & EMM client Apps screen under the Recommended banner. The optional applications are listed under Optional. Users must manually install all the deployed Play Store applications. Newly deployed applications have a “New” button indication.

On Samsung Knox Workspace devices, the custom applications set for automatic installation are installed automatically. However, if the application is configured for installation in the Knox mode container, it is not installed until the user creates the container. Users must manually install all Play Store applications, even the ones that you have set for automatic installation.

On Android for Work devices, Play Store applications that you set for automatic installation are automatically installed on to the device. In-house Android applications are not supported with Android for Work.

On all devices, optional applications are displayed with a “New” button and are not installed until the user taps **New**.

After the application is installed, its icon is also displayed in the device’s App application.
Installing mobile applications on iOS devices

On iOS devices, mobile applications configured for automatic installation are not installed automatically. Instead, the user is prompted to install each application you deploy. The prompt is displayed right after the user enrolls the device or within ten minutes after you deploy the application from Admin Portal. The dialog box indicates the server and the application name. The user taps **Install** to proceed with the installation. The application is displayed on the home screen after installation.

Users can select **Cancel** to prevent installation. When users select Cancel, they are prompted the next time they open the device to install the application. If they select cancel again, they are not prompted anymore. They can, however, still install the application by opening the **Company Apps** web clip.

Company Apps is a web clip that is installed automatically when the device is enrolled. When the user opens the web clip, the screen lists the automatic and optional mobile applications deployed to this user. The user can then click the application icon for a short description and choose which applications to install.

Removing a mobile application

If you don’t want to deploy a mobile application any more, you have two options:

- You can just reset the role setting in the application’s User Access setting.
  
  This leaves the application listing on the Apps page. The status is changed to “Ready to Deploy” when it is not assigned to any roles.

- You can delete the application from the Apps page.
  
  This removes the application from all roles.

After you stop deploying a mobile application, it is no longer listed in the Samsung SDS IAM & EMM client on Android devices and Company Apps webclip on iOS devices. However, if the user has already installed the application, it remains installed on the device. For example, the user can still open the application from the device’s Apps catalog. Removing the application from the device can only be done by the user.

**Note** The same is true when a device is unenrolled from the Samsung service. That is, any application installed from the Mobile Apps screen remain installed after the device is unenrolled.
Android for Work

Android for Work makes Android devices enterprise ready in two ways, a work profile on your personal phone or a company issued phone that is placed in device owner mode. A work profile is a container-like environment where corporate applications can co-exist with personal applications on one device while keeping the corporate data separate and secure. A device in device owner mode provides the system administrator with full control of the device.

Configuring a work profile

A work profile is a container-like environment where corporate applications can co-exist with personal applications on one device while keeping the corporate data separate and secure.

The high-level procedures for setting up a work profile are:

1. Verify that you have fulfilled the pre-requisites. See “Pre-requisites” on page 141.
2. Map your company’s domain to Samsung service. This mapping binds the Google generated Android for Work token to the Samsung service and identifies Samsung SDS IAM & EMM as the MDM provider. See “Mapping Domains” on page 142.
3. Create a work profile policy set in Admin Portal. See “Creating a Work Profile policy set” on page 142.
4. Add and configure a Google SAML application with user provisioning in Admin Portal. Provisioning is optional but highly recommended because it allows for users that are created in the Google Apps account to be automatically added to the Samsung service and visa versa. See Configuring Google Apps for Work and Configuring user provisioning for Google Apps for Work.
5. Configure applications that you want added to the work profile. See “Configuring applications” on page 143.

Pre-requisites

Android devices must be on 5.0 Lollipop or newer.

When you create a Google Apps administrator account, configure the following:

- Enable the Android for Work service.
- Disable the “Enforce EMM policies on Android devices” option.

You can create the Google Android for Work account from the Google website.
Mapping Domains

Domain mapping binds the Google generated Android for Work token to the Samsung service and identifies Samsung SDS IAM & EMM as the MDM provider. This is a required step for enabling work profile on the Samsung service.

Before performing this mapping, you must have a Google account with your company’s domain configured in it.

To perform the domain mapping:

1. In Admin Portal, go to Settings, Android for Work.
2. Click Add.
3. Select your company domain from the drop down.
   
   If you do not see a domain, verify that you have created your Google account correctly and the Android for Work service was enabled. The “Your Primary Domain in Google Apps for Work” setting on the Google SAML app configuration page determines the available domain in this drop down.
4. Enter the Android for Work token generated by Google when you add your domain to the Google account.
5. Click OK.

Creating a Work Profile policy set

You enable users with the work profile by creating the work profile policy set and pushing it to specified devices/users. The Samsung SDS IAM & EMM client is automatically deployed to the work profile for all devices that receive this policy set. Users can then use the application to manage their work profile applications. If users delete the application, the work profile and all work profile applications are deleted from the device.

If you have Samsung Knox container configured for a device and you push the work profile policy to that same device, the container will be deleted and you will need to configure applications to the work profile.

To create a work profile policy set:

1. Log in to Admin Portal as an administrator.
2. Create a new policy set or update an existing one.
4. On the Enable Work Profiles page, select Yes from the drop down.
   
   Selecting Yes enables users to create a work profile on their devices.
5 On the **Exchange Settings** page, define the profile for Microsoft Exchange ActiveSync accounts in the Android for Work email application.

Configuring Microsoft Exchange ActiveSync automatically deploys the Gmail application to the specified users’ devices. Do not manually deploy another Gmail application to the same users because this can cause conflicting configurations.

**Note** For devices with Samsung service version 16.7 or older, configuring Microsoft Exchange ActiveSync deploys the Divide Productivity application. When you upgrade the Samsung service on both the device and cloud to 16.8 or newer, previously enrolled devices will have both the Divide Productivity and Gmail applications. Users can delete Divide Productivity when they are ready.

6 Use the **Certificate Profiles** option to distribute certificates to the devices.

Certificates can then be used by Wi-Fi providers or websites for authentication.

7 Update devices with the policy changes.

You can manually push policy changes or wait for the policy push delay or update interval you set in Device Policy Management on the Settings page in Admin Portal. See “**Updating device configuration policy changes**” on page 188.

If you do not see a domain, verify that you have created your Google account correctly and the Android for Work service was enabled. The “Your Primary Domain in Google Apps for Work” setting on the Google SAML app configuration page determines the available domain in this drop down.

8 Use the **System Apps** option to view, add, or delete system applications. The default system applications that will be available in the work profile are displayed.

9 Click **Save**.

### Configuring applications

You add and configure applications using Admin Portal so that users can access these applications on their devices as part of Android for Work (in work profile or on devices enrolled in device owner mode). Before configure applications, you need to create a Google Apps administrator account. You create the Google Android for Work account from the Google website.

You can only deploy Android app store applications. In-house Android applications are not supported with Android for Work. Only applications you deploy will be available in the user’s work Play Store.

Configuring applications that you want users to access via Android for Work is very similar to configuring applications for their personal profile. The differences are:

- For each application, you must choose one of the two “Install to Android for Work” options (on the Applications Settings page).
For applications with restrictions, you can set those restrictions.

When you save the configuration settings, you must accept the Android for Work permissions. If you do not accept the permissions, the applications will not be available to users.

See Deploying an Android Google Play application for detailed instructions.

**Enrolling devices in device owner mode**

A device in device owner mode provides the system administrator with full control of the device. You enroll company issued devices in device owner mode so that you can restrict activities and functions on the device using Admin Portal. Samsung SDS IAM & EMM is the administrator of devices in device owner mode. To place a device in device owner mode, you need a master device that is configured for NFC provisioning. You then use the master device to bump other devices (referred to as target devices) and initiate the enrollment.

**Device owner prerequisites**

To enroll devices in device owner mode, you need the following:

- Have both the master and target devices at hand. Bumping the devices requires that you have both devices with you.
- The master device should already be enrolled to the Samsung SDS IAM & EMM User Suite.
- The target devices must be set to factory reset.
- Both the master and target devices must have wi-fi access.

**Configure master device for NFC provisioning**

You must configure the master device for NFC provisioning to enroll target devices in device owner mode.

To configure the master device for NFC provisioning:

1. Log in to Admin Portal, click **Policies**, and select the policy set for the user associated with the master device.

2. Click **Mobile Device Policies**, **Android for Work Settings**, and **Device Owner**.

3. Select **Yes** in the Allow Provisioning mode drop down.

4. Click **Save**.

5. On the master device, go to the Settings page and tap **Start NFC Provisioning**. This action synchronizes the master device with Samsung service and gets the provisioning data.
6  (Optional) On the Provisioning Mode window, you can activate the **Send Username/Password** option to enter the user’s Samsung SDS IAM & EMM username/password. The typical scenario for providing username/password is if you are enrolling multiple devices and do not need to track individual device owners. In this case you would provide one username/password and bump multiple devices to this one account. For target devices of versions M (6.0) and newer, providing the credentials will initiate auto enrollment. Users of target devices that are older than version M (6.0) will need to finish the enrollment manually.

7  Bump the master device with the target device. You are now done with the master device. You either finish enrolling the target device yourself or ask the device owner to do it. See “Enrolling target devices” on page 145.

**Enrolling target devices**

You use the target device to finish enrolling it in device owner mode. The system administrator can either finish the enrollment on the target device or ask the device user to do it.

To finish enrolling the target device:

1  Connect the target device to an available wi-fi after NFC bump has been performed. After it is connected, the phone downloads Samsung SDS IAM & EMM Admin Portal and sets it as the device owner.

2  You may need to enter your Samsung SDS IAM & EMM credentials to finish installing Admin Portal, depending on how the system administrator configured the enrollment and your device version. If the system administrator has entered the user credentials and the device is of version M (6.0) or newer, then Admin Portal is automatically installed, the device is enrolled, and policies are synchronized.

3  On the Google account information screen, click **Accept** to get redirected to the Samsung SDS IAM & EMM log in screen.

4  Enter your Samsung SDS IAM & EMM credentials to complete the Google account setup.
Deploying web applications to Knox containers

This section is for administrators assigning web applications to Samsung Knox Workspace devices with a Knox container only.

Users open the Samsung SDS IAM & EMM WebApps application installed inside a Knox container to launch the web applications you assign to them. When you use the Samsung service for mobile device management, Samsung SDS IAM & EMM WebApps is automatically installed in the Knox container when users create the Knox container.

**Note** If you are using another mobile device management provider, users must install the Samsung SDS IAM & EMM WebApps application by some other means. In addition, Knox SSO service must be enabled and the Samsung SDS IAM & EMM WebApps application must be added to the Application SSO whitelist policy. Contact your mobile device management provider for the procedures.

You use the same procedure to assign web applications to Samsung SDS IAM & EMM WebApps that you use to assign applications to the Samsung SDS IAM & EMM client—see “Adding web applications by using Admin Portal” on page 131). How the web applications are displayed on the devices depends upon whether you are using the Samsung service for single sign-on alone or mobile device management and single sign-on.

- If you are using the Samsung service for single sign-on only, the applications are always displayed in Samsung SDS IAM & EMM WebApps. If users also install the Samsung SDS IAM & EMM client outside the container the web applications are listed on the Apps screen too.

- If you are using the Samsung service for mobile device management as well as single sign on, the web applications you assign are displayed in Samsung SDS IAM & EMM WebApps only.

  In this case, the Samsung SDS IAM & EMM client installed outside the container does not have a Web Apps screen.

**Note** By default, the Samsung service provides single sign-on for all SAML and user name password applications you assign to users. You can, however, disable single sign-on for one or more devices using the mobile device Disable SSO command (see “Using Active Directory Users and Computers to manage devices” on page 162 and “Using the device management commands” on page 165 for the details about the mobile device commands).
Deploying mobile applications to Knox containers

This section is for administrators deploying a mobile application to devices with a Samsung Knox container and are using the Samsung service for Samsung Knox device mobile device management.

In many ways, deploying a mobile applications for installation in a Samsung Knox container is the same as deploying a mobile application to any Android device. That is,
- You have the application’s binary .APK file,
- You use Admin Portal to upload the .APK file and select a role to select which users get the application.

You can configure the application for automatic or optional installation. If you select automatic, the application is installed without user prompting in the Knox container if the container has already been created. If it has not, the application is installed automatically right after the container is created. If the application is configured for optional installation, the user must install it from the Samsung SDS IAM & EMM client.

- The application is listed in the Samsung SDS IAM & EMM client.

Users can open the application either from the Samsung SDS IAM & EMM client in personal mode or by clicking the application’s icon from the Knox mode container.

For devices that have a Knox version 2 container, you use the procedures described in “Adding and deploying mobile applications using Admin Portal” on page 138 to deploy mobile applications for installation in the container. However, there are a couple of differences, especially if you are deploying applications to devices with Knox Version 1 containers:

- For Knox version 2 containers, you can configure Android in-house applications for installation in either in personal mode or in the Knox mode container.

  See “Deploying inhouse Android applications to KNOX 2 containers” on page 147 for the details.

- For Knox version 1 containers, mobile applications must be wrapped before they can be installed. If the application is not wrapped, it is installed in personal mode.

  See “Deploying wrapped mobile applications to KNOX version 1 containers” on page 148 for the details.

Applications that are downloaded from the Samsung Knox Apps store to a Knox version 1 container do not need to be wrapped separately (they are already wrapped).

Deploying inhouse Android applications to Knox 2 containers

For devices with Knox version 2 containers, you can specify whether an inhouse Android application is installed inside the Knox mode container or in personal mode. (This feature is not available for applications downloaded from Google Play.)
Note You must have a Knox Premium, Workspace, or EMM license to use this option. If you do not you can install the application on the device only and the other options are dimmed.

You specify the installation destination when you configure the application. You have the following options:

- Install in the Knox container based on Enable Knox container policy setting.
  
  Select **Deploy to Knox container if the “Enable Knox Container” policy is applied, otherwise deploy to device** to install the application in the container but only if container creation is enabled. Otherwise, install the application in personal mode. (See “Enabling the device to allow users to create an enterprise container” on page 176 to see how you set this policy.)

  **Note** If the “Enable Knox Container” policy is set but the user has not yet created the container, the application is not installed in personal mode. Instead, application installation is deferred until the container is created.

- Install in the Knox mode container.
  
  Select **Install to Knox container only** to install the application in the Knox 2 container only. If the user has not yet created the container, the application is not installed in personal mode. Instead, application installation is deferred until the container is created.

- Install in personal mode.
  
  Select **Install to Device only** to install the application in personal mode only.

If the license expires, the applications remain installed in the container, however the container is not accessible by the user. You can continue to deploy mobile applications to a device with an expired license, however, an error message indicates that the action cannot be completed until the proper license is installed.

### Deploying wrapped mobile applications to Knox version 1 containers

Deploying mobile applications to devices that have a Knox version 1 container there are some procedural differences for the application developer and Samsung service administrator:

For the application developer:

- Before the user can install an Android application in a Samsung Knox version 1 container, the application must be rebuilt by Samsung in a process referred to as “app wrapping.”

  To learn more about wrapping and get your application wrapped, go to [https://www.samsungknox.com/apps/app-wrapping](https://www.samsungknox.com/apps/app-wrapping).
• In order for a mobile application to use single sign-on (SSO) inside of a Samsung Knox container, the mobile application vendor uses the Centrify for Samsung Mobile Authentication Service (MAS) SDK to enable their mobile application for SSO.

For the Samsung service administrator:
• You cannot deploy an application from Google Play to a Knox version 1 container unless it has been wrapped.
• When deploying a Samsung Knox wrapped mobile application, use the Android InHouse application template in the Apps catalog in Admin Portal.
• When deploying a Samsung Knox wrapped mobile application that is also configured for SSO, you must also deploy a corresponding SAML web application to the same set of users.
• For every mobile application that uses the SSO capability, you must add the package name to the Application SSO whitelist policy (see “Adding mobile applications that use SSO to the Application SSO whitelist” on page 180). You get the package name from the application developer.

Note Mobile applications that use the SSO capability that you deploy from Admin Portal and the user installs from the Samsung SDS IAM & EMM client on their device do not need to be added to the Application SSO whitelist policy.

Use the following procedure to deploy a wrapped mobile application to devices with a Samsung Knox version 1 container. If your mobile application was developed to use Samsung Knox SSO go to “How to configure mobile applications that use KNOX SSO” on page 150 for additional deployment instructions.

To learn about application wrapping see “How developers prepare a mobile application for use in Samsung KNOX version 1 containers” on page 151.

To deploy a wrapped mobile application to a Knox version 1 container:

1 Open Admin Portal and select the Apps page.
2 Click Add Mobile Apps.
3 Click Add Custom App.
4 Select Android InHouse and click Add.
5 Click Yes to confirm.
6 Click Close to exit.

The Android InHouse application configuration page is opened.

7 Click Application Help underneath the application name. Use the instructions to configure the Application Settings and Description pages.
Note  Knox installation options (see “Deploying inhouse Android applications to KNOX 2 containers” on page 147) is not available for wrapped applications.

8  Click User Access and select all of the roles that should get this application.

   If you select Automatic Install (the default), the Samsung SDS IAM & EMM client automatically installs the wrapped application in the container. If you instead select Optional Install, the user must open the Samsung SDS IAM & EMM client and install the application manually.

9  Click Save.

How to configure mobile applications that use Knox SSO

Mobile applications that use the Knox SSO service to ask for a SAML token from inside of a Samsung Knox version 1 or version 2 container must have a paired web SAML application deployed from Admin Portal to authenticate the user. SAML provides a token-based method for single sign-on, and the paired web application provides the Samsung service connection to acquire the token.

Note  The Samsung SDS IAM & EMM WebApps application uses a SAML token for single sign-on, however, it is an exception to this rule. It does not need a paired web SAML application.

Deploying a mobile application that uses a SAML token to provide SSO:

1  In Admin Portal, deploy the wrapped application as described in “Deploying wrapped mobile applications to KNOX version 1 containers” on page 148.

2  Using either Admin Portal or the Active Directory Group Policy Management Editor, add the application’s package name to the Application SSO whitelist policy—see “Adding mobile applications that use SSO to the Application SSO whitelist” on page 180.

3  In Admin Portal, add, configure, and deploy a generic web SAML application for mobile application.

   You must deploy a SAML web application for every mobile application that uses Samsung Knox SSO installed in the Knox container. This includes all of the mobile applications you deploy and all mobile applications that use Knox SSO the user installs from the Samsung Knox Apps store.

   Depending upon the application, one of the following scenarios applies:
   •  Deploy the SAML application in the Add App catalog in Admin Portal that is preconfigured for Samsung Knox SSO.
   •  Deploy the SAML application in the Add App catalog in Admin Portal that you can configure for use with Samsung Knox SSO. For example, Box, Dropbox, and so forth.
If your SAML application isn’t already in the Add App catalog in Admin Portal, deploy and configure a generic SAML application profile. The mobile application developer provides the configuration parameters for the SAML application profile.

The following conditions apply to the web SAML application:

- The App ID has to be the same as the text string that is specified as the target in the getSecurityToken(target) code of the wrapped mobile application.
- There can only be one SAML application deployed using the name used by the wrapped mobile application. For example, you cannot have two Box SAML applications configured.

4 In the User Access tab of the Application Settings dialog box, assign the web SAML application to the same roles to which you assigned the mobile applications. (See “Assigning applications to and removing them from roles” on page 251.)

The Samsung service deploys the web SAML application to the role members. This web SAML application does not, however, appear in Samsung SDS IAM & EMM WebApps.

How developers prepare a mobile application for use in Samsung Knox version 1 containers

Mobile applications must be customized in a process called “app wrapping” before you can install them in the Samsung Knox version 1 container. To learn more about wrapping and get your application wrapped, go to https://www.samsungknox.com/apps/app-wrapping.

The customization consists of the following broad steps:

1 Configure for SSO (optional).

The mobile application developer uses the Centrify for Samsung Mobile Authentication Service (MAS) SDK to enable the mobile application for single sign-on. Not all applications are appropriate for SSO; for example, you don’t need SSO for an application that doesn’t require a login (such as a clock, for example).

In addition to providing the APK file you need the following information from the application developer to deploy a generic SAML web application for the mobile application. (See “How to configure mobile applications that use KNOX SSO” on page 150 for deploying applications that use the Knox SSO capability.)

- The text string that is specified as the target in the getSecurityToken(target) code of the mobile wrapped application. This text string must match the App ID in the Admin Portal application settings.
- The application package name. You’ll use the application package name if you need to add the application to Samsung Knox SSO whitelist.

2 Wrap the application’s APK file.
The mobile application developer produces the binary APK file. However, the APK file must be wrapped before it can be installed in the Samsung Knox container.

Wrapping is an automated service that unpacks the application's original APK file, extracts the certificate, and repackages the application into a new APK package with a digital signature and Knox container specific certificate. The service also provides QA testing to confirm device compatibility and inspects for malware and risk behaviors. To learn more about wrapping and get your application wrapped, go to https://www.samsungknox.com/apps/app-wrapping.

3 Distribute the wrapped binary.

You can use Admin Portal to distribute the wrapped application. the Samsung SDS IAM & EMM client automatically determines if the application is wrapped and installs it inside the Knox container, not outside with the other Android applications.
Managing devices

The Devices page lists all of the devices that have been enrolled in the Samsung service. This page is blank until devices are enrolled. You can use the column headers to sort the applications by name, type, description, and status.

**Note** Your role must have the Samsung service Devices Management administrative right to view and manage the devices.

You use Admin Portal to manage devices enrolled in the Samsung service. See “Supported devices” on page 90 for the list of mobile devices that can be enrolled in the Samsung service and their operating system requirements. The Devices page in Admin Portal lists the enrolled devices and provides you details about the device configuration, installed applications, and activity.

**Note** You can also install mobile device policies and mobile applications on enrolled devices. See “Managing device configuration policies” on page 221 and “Adding and deploying mobile applications using Admin Portal” on page 138 for the details.

If you are using Active Directory accounts for user authentication, you can also use Active Directory Users and Computers to perform many of the same management functions. The Devices page in Admin Portal lists the devices enrolled by all users. However, Active Directory Users and Computers lists only the devices enrolled by users with Active Directory accounts.

By default, the Samsung service is set to provide mobile device management. However, you can reset this option to provide just single sign-on for web applications. See “How to configure Mobile Device Management or single sign-on only” on page 18 to reset this option. When you configure the Samsung service for single sign-on only, Admin Portal page still lists the enrolled devices, however, your device management options are limited. For example, most of the commands are not available.

This chapter contains the following topics:

- “Enrolling a device” on page 154
- “Using Admin Portal to manage devices” on page 160
- “Using Active Directory Users and Computers to manage devices” on page 162
- “Using the device management commands” on page 165
- Managing policy compliance
- “Working with Samsung KNOX devices” on page 173
Enrolling a device

The Samsung service requires the device owners to enroll the device regardless of whether it is used for single sign-on or mobile device management.

Before they can enroll a device, however, the users’ account must have the enroll device permission. See “Enabling users to enroll devices” on page 22 for the details.

Users enroll their devices using the following methods:

- For Android devices: Users install the Samsung SDS IAM & EMM client for Android on the device.
  
  Users with Samsung Knox devices that have the Universal MDM Client (UMC) installed can enroll their devices by entering just their user name and password—see “Enabling Samsung KNOX UMC login suffix updates” on page 348 for an overview of the UMC.

- For iOS devices: Users install the Samsung SDS IAM & EMM client for iOS on the device.
  
  If your organization is using the Apple Device Enrollment Program, you can have the Samsung SDS IAM & EMM client installed automatically on the device. If you use this program, however, you cannot unenroll the device. See “Linking to the Apple Device Enrollment Program” on page 340 for the details.

Users can get the Samsung SDS IAM & EMM client from a number of places. For example:

- They can click Add Devices from the Samsung SDS IAM & EMM user portal. From the pop up window, users can use a QR reader to download the application from Google Play or the Apple App Store, send an SMS message to the device with a link that downloads the application, or get a link they can enter in the device’s browser to download the application.

- You can send them an SMS message using the SMS Invite command.

- You can email the same link or download the Samsung SDS IAM & EMM client and email it to your users.

Application installation is described in the user portal. See the user portal help for the Samsung CellWe EMM application installation and enrollment instructions for each device.

What happens when a device is enrolled

When the user enrolls a device, the Samsung service performs the following actions:

- The device is added to the Devices page in Admin Portal.
  
  If the user has an Active Directory account, the device is also added to the Active Directory organizational unit specified in the Device Enrollment Settings.

- The web applications assigned to the user are added to the Web Apps screen in the Samsung SDS IAM & EMM client or Samsung SDS IAM & EMM WebApps screen.
Note Samsung Knox Workspace devices that are enabled to have a Knox container do not have the Web Apps screen. Instead, the Samsung service lists the web applications to the Samsung SDS IAM & EMM WebApps application.

- The device is added to the user’s Devices page in the Samsung SDS IAM & EMM user portal.

- If the user enrolls multiple devices, the first is device enrolled is designated as the primary device. The primary device is the only device that can be used with the Mobile Authenticator (see “Authentication - Setting authentication policy controls” on page 193). The user can change the primary device designation in the user portal.

When you use the Samsung service for mobile device management, it also performs the following actions:

- The mobile applications are deployed to the devices.

  On Android devices, the mobile applications are added to the Apps screen in the Samsung SDS IAM & EMM client (see “Installing mobile applications on Android devices” on page 139).

  On iOS devices, the user is prompted to install the mobile applications set for Automatic Install (see “Installing mobile applications on iOS devices” on page 140).

- The mobile device policies defined in either the Samsung SDS IAM & EMM policy service policy set or the Windows group policy object are installed.

  Note You can use the policies to set Samsung and iOS devices into kiosk—single application—mode. After this policy and the application are installed, the device always opens into the specified application and that’s the only application that can be run. See “Using the Samsung KNOX Device Settings” on page 231 and “Using iOS settings” on page 229 for more information about kiosk mode.

- If you created a wi-fi, VPN, or Exchange profile that uses a certificate for authentication, one or more certificates are automatically installed.

  If you are using the Samsung SDS IAM & EMM policy service for device policy management, a certificate is automatically issued by the Samsung SDS IAM & EMM CA and installed in the device by the Samsung service. If you are using Active Directory group policy, the certificates (user and/or computer) are automatically issued by your designated Active Directory certification authority (see “Using Active Directory certificates in devices for authentication” on page 365) and installed in the device by the Samsung service.

### Enabling invitation-based device enrollment

You can enable smart card users to enroll their mobile devices to the Samsung service. This enrollment process is different from the standard enrollment because smart card users do not have passwords.
Both Android and iOS devices are supported.

To enable smart card users to enroll mobile devices:

1. Log in to Admin Portal.
2. Click Roles.
3. Create a new role or select an existing role.
4. Click Members > Add.
5. On the Add Members window:
   a. Enter the first few letters of the user, role, or Active Directory/LDAP account/group you want to add and click the search icon.
   b. Select the relevant user, role, or Active Directory/LDAP account/group and click Add.
6. Click Save to save the changes.
7. Click Policies and either click Add Policy Set or select an existing policy.
8. Click Mobile Device Policies > Device Enrollment Settings.
9. Select Yes in the Permit device enrollment policy.
10. Select Yes in the Enable invite based enrollment policy.
11. Select the length of time (in minutes) that the invitation will remain valid in the Invite based enrollment link expiration (default 60 minutes) policy.
12. Configure the other policies as necessary.
13. Click Save.
14 Click Policy Settings > Apply policy to specified roles and select the role you created or selected in Step 3.

15 Click Save.

16 Click Users, select the relevant users, go to Actions, and select either Send SMS invite for device enrollment or Send email invite for user portal setup to have the Samsung service send a text or email message with the enrollment link.

The selected users can now open either the email or SMS message to enroll their devices.

**Device status**

Admin Portal shows the device status for all devices that have been enrolled in the Samsung service on the Devices page.

*Note* You can also see the state of devices enrolled by users with Active Directory/LDAP accounts in Active Directory Users and Computers. See “Using Active Directory Users and Computers to manage devices” on page 162 for the details.

There are four status values:

- Enrolled: The device has been successfully enrolled by the user
- Enrolling: The device is in the process of enrolling
- Unreachable: The device has not been in contact with the Samsung service for an administrator-defined number of days (see “General device management settings” on page 189).
  
  If the device is labelled “unreachable,” it returns to “Enrolled” the next time a user opens the Samsung SDS IAM & EMM client on the device. A device that is unreachable is not unenrolled.

- Unenrolled: The device has been unenrolled either by an administrator or the user.

The device listing remains in Admin Portal, the Samsung SDS IAM & EMM user portal, and Active Directory (for devices enrolled by users with Active Directory accounts only) after it is unenrolled or unreachable and remains listed until the device is manually deleted by a Samsung service administrator or the user.

**Location tracking**

If location tracking is enabled, the device’s location is displayed for users on the Devices screen in the user portal. Additionally, you have the option to enforce mandatory sharing of device location with systems administrators (Force option) or allow users to control sharing of their device locations (Opt-In option). You can enable/disable location tracking using the “Report mobile device location” mobile device policy in Policies > Mobile Device Policies > Common Mobile Settings > Restrictions Settings.
Users can turn location tracking on and off in the Settings menu in the user portal. However, if you select **Force** in the Enable Device Location Tracking by Administrator dropdown, location tracking is enabled for both the user and systems administrator regardless of the user selection.

You can use Active Directory Users and Computers to configure device location reporting. To enable that setting, go to the Group Policy in your active directory that applies to the devices: Computer Configuration > Policies > Samsung SDS IAM & EMM Cloud Management Settings > Common Mobile Settings > Restrictions Settings > Report mobile device location.

However, the Enable Device Location Tracking by Administrator option is only available for Samsung service managed devices.

In iOS devices, the Samsung SDS IAM & EMM client does not use GPS location tracking. Using GPS hardware is very battery-intensive. Instead, it uses the device’s significant-change location service. This produces updates only when there has been a significant change in the device’s location, for example 500 meters or more. In addition, significant-change location tracking is event-based -- the application sleeps until there is a significant location change. Consequently, location tracking does not have any significant impact on battery consumption.

**Note** The Apple Location icon shown on the top status bar or in the Privacy > Location Settings does not differentiate between GPS and significant-change location tracking.

In Android devices, the Samsung SDS IAM & EMM client is configured for low power consumption. To confirm, open the device’s Settings > Location. The Samsung SDS IAM & EMM client listing shows “Low battery use.”

### Managing enrollment of Android devices with Google services SafetyNet check

The SafetyNet API provides access to Google services that help you assess the health and safety of Android devices. The Samsung service uses the Google services in conjunction with an enrollment setting to let you control device enrollment. You must select **No** for the "Permit noncompliant devices to enroll" policy setting to prevent Android devices that fail the Google services SafetyNet check from enrolling to the Samsung service. If you have the "Permit noncompliant devices to enroll" policy setting set to **Yes**, then Android devices can...
enroll regardless of the Google services SafetyNet check result. The policy setting is located in Admin Portal > Policies > Mobile Device Policies > Device Enrollment Settings.

Note: Only Google services 8.4 and above supports SafetyNet.
Using Admin Portal to manage devices

Admin Portal lists all of the devices that have been enrolled in the Samsung service on the Devices page. You can use the drop down menu (“All Devices” in the picture) to select devices of a specific type. You can click the column header to sort the listed devices. You use this page to view the device properties and issue commands to one or more devices. This page is empty until users enroll their mobile devices.

The following figure illustrates a sample Devices page populated with devices with different status.

You can see the location of all devices whose location is available by toggling to the map view. Select a device to see the device details and the following information if you are using the Samsung service for mobile device management:

- **Device Activity**: Activities performed on the device.
- **Device Applications**: Shows the applications that are targeted for this device, the application version, the installation type (automatic or optional), and the application statuses (Installed or Not Installed). You can export the information to CSV and Excel.
- **Device Location**: Shows the device location.
- **Policy Summary**: Shows the policies applied to the device.

If you are using another service for mobile device management, the Device Applications and Device Activity pages are blank.

To search for a device or devices, enter the first few characters of the information from any field. Admin Portal automatically filters the list for the matching devices. For example, you can enter the first few characters of the user’s name, serial number, or model to select a device.

Sending commands from Admin Portal

Admin Portal provides commands you can send to an enrolled device. (If the device is unenrolled you can just delete it.) You can display the commands using any of three methods:
Right-click the device on the Devices page.
Admin Portal displays a pop up menu with the commands. Use this method to send a command to one device at a time.

Click the check box of one or more devices on the Devices page.
Admin Portal displays a pop-up **Actions** menu with the commands.

Click the device.
Admin Portal opens the device details page. The commands are provided in the **Actions** menu.

See “Using the device management commands” on page 165 for the command descriptions. Some commands are available for specific types of devices only.

**Note** To run these commands you must be a member of an Admin Portal role that has Device Management rights. Members of the sysadmin role have this permission. If you are not a sysadmin, go to the Users page in Admin Portal and open your account to see your roles. Then open the Roles page and select your role or roles to see the rights assigned to you.

To send a command from the Devices page to a single device:

1. Log in to Admin Portal.
2. Click **Devices**.
3. Right-click the device.
   Admin Portal overlays a pop up window with the commands.
4. Click the command.
   Admin Portal displays a drop down message indicating that the command has been issued.

To send a command from the device details page:

1. Log in to Admin Portal.
2. Click **Devices**.
3. Select a device.
   Click the **Actions** menu. See “Using the device management commands” on page 165 for the command descriptions.
4. Click the command.
   Admin Portal displays a drop down message indicating that the command has been issued.
Using Active Directory Users and Computers to manage devices

If you are using Active Directory group policy for device policy management, you can use Active Directory Users and Computers to manage enrolled devices. The Samsung service stores a record of each enrolled device in the Active Directory organizational unit you specified in the Device Enrollment Settings—see “Enabling users to enroll devices” on page 22.

The device’s Properties window has the following additional tabs:

- IAM & EMM Mobile: Displays the device properties, state, logging settings, and network traffic and phone record.

- Installed Applications: For Android devices, all of the mobile applications installed on the device are listed. For iOS devices only the mobile applications installed using the Samsung service are listed.

In addition, the user’s Properties window has the IAM & EMM Mobile tab which lists the devices enrolled by that user.

Note These tabs are only added to the device and user Properties when you use Active Directory group policy for device policy management and you installed the Active Directory Users and Computers Console Extension when you installed the Samsung SDS IAM & EMM Management Suite software. If you do not see these tabs, see “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355.

Viewing the enrolled device records

When an Active Directory user enrolls a device, the Samsung service creates a device record for it in the organizational unit specified in the Device Enrollment Settings in the policy set assigned to the user’s role. See “Enabling users to enroll devices” on page 22 to see how you specify the organizational unit.

To view a list of all devices enrolled by a role’s members, open the Active Directory organizational unit assigned in that role’s policy set. Any devices that have an icon with a down arrow were but at that moment are not enrolled.

Using the IAM & EMM Mobile tab

To see a device’s mobile properties, double-click the device in Active Directory Users and Computers and then select the IAM & EMM Mobile tab. The following table describes the
Using Active Directory Users and Computers to manage devices

Chapter 19 • Managing devices

General Information and State fields in this tab. The same information is available in the device details page in Admin Portal.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Information</strong></td>
<td></td>
</tr>
<tr>
<td>Device type</td>
<td>The device’s model name and number.</td>
</tr>
<tr>
<td>OS version</td>
<td>The version number of the operating system in the device.</td>
</tr>
<tr>
<td>Phone number</td>
<td>If applicable, the phone number of the device.</td>
</tr>
<tr>
<td>Serial number</td>
<td>The serial number of the device.</td>
</tr>
<tr>
<td>IMEI number</td>
<td>The International Mobile Equipment Identity value for the device.</td>
</tr>
<tr>
<td>Push Notification Token</td>
<td>Indicates whether a Push Notification Token exists for this device.</td>
</tr>
<tr>
<td>Carrier name</td>
<td>If applicable, the wireless carrier to which the device is subscribed.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td></td>
</tr>
<tr>
<td>Device State</td>
<td>See “Device status” on page 157</td>
</tr>
<tr>
<td>Last seen date</td>
<td>The date and time when the device last contacted the Samsung service.</td>
</tr>
<tr>
<td>User name</td>
<td>The Active Directory user account name of the device's owner.</td>
</tr>
<tr>
<td>Customer ID</td>
<td>The customer ID used to enroll the device.</td>
</tr>
</tbody>
</table>

In addition, the IAM & EMM Mobile tab provides vendor-specific information. For example, the IAM & EMM Mobile tab for an iOS device also displays iOS settings and carrier and network properties while on Android devices it displays logging settings and network traffic and carrier network data.

**Sending commands to a device**

You can use Active Directory Users and Computers to send commands to devices. Right-click the device listing and select All Tasks to display the commands available. You can select multiple devices using Shift-click and Ctrl-click. If the commands are dimmed, the device is unenrolled.

The Samsung service commands available in All Tasks depend upon the type of device and whether you are using the Samsung service for single sign-on or mobile device management). See “Using the device management commands” on page 165 for the command descriptions.

To send Samsung service commands from the device listing:

1. Open Active Directory Users and Computers on the server upon which you installed the connector or another computer in which installed just the Active Directory/LDAP and group policy extensions.
2 Select the organizational unit with the mobile device accounts.

   The list of devices appears in the right pane.

3 Right-click the device or select multiple devices and right-click.

4 Expand the All Tasks menu to view the commands and click the command.

Managing mobile devices from the user Properties

You can see a list of just the devices enrolled by a specific user by opening the user’s Properties and selecting the IAM & EMM Mobile tab.

This tab also has buttons for the commands available when you use the Samsung service for mobile device management. Some devices provide additional commands. Right-click the device to see the complete set of commands.

Devices with the red circle and “x” are unenrolled. When the device is unenrolled the commands are dimmed.

To view devices and issue commands from an Active Directory user account:

1 Open Active Directory Users and Computers on the server upon which you installed the connector or another computer in which installed just the Active Directory and group policy extensions.

2 Select the container with your mobile users’ accounts.

3 Double-click the device owner’s account.

4 Click the IAM & EMM Mobile tab.

   The user’s enrolled devices are listed in the window.

5 Click a device or use Shift-click or Ctrl-click to select multiple devices and then right-click.

   The command sets available for the devices selected are displayed in a pop-up window.

6 Click the command.

   See “Using the device management commands” on page 165 for the command descriptions.
Using the device management commands

The following tables list the commands you can send to devices from Admin Portal and Active Directory Users and Computers. The commands available vary depending upon the device type, your Device Management permissions (see “Admin Portal administrative rights” on page 252), and the device’s state (enrolled, unenrolled, unreachable). For example, there are more commands available for Samsung Knox devices than other Android and iOS devices, and the only command available for unenrolled devices is “Delete.” In addition, if you are using the Samsung service for single sign-on only, the only commands available are Delete, SSO Enable, and SSO Disable.

You can issue the commands from the device and user properties in Active Directory Users and Computers when you use Active Directory Group Policy Management for device policy management (see “Selecting the policy service for device policy management” on page 345). If you are using Samsung SDS IAM & EMM policy service, you can invoke the commands from Admin Portal alone.

**Note** If you are using Active Directory Group Policy Management for device policy management, you can also use the Active Directory Disable Account command to unenroll a device.

Users can invoke many of the same commands from the user portal. The Availability column in the following tables indicates on which devices the commands are available and where they can be called from.

<table>
<thead>
<tr>
<th>Device Management</th>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Lock</td>
<td>Admin Portal and Samsung Knox Workspace devices</td>
<td>Locks the Samsung SDS IAM &amp; EMM client on the device and only the administrator can unlock it. Users can not access any functionality on the Samsung SDS IAM &amp; EMM client on the device.</td>
</tr>
<tr>
<td>Delete</td>
<td>All devices</td>
<td>Delete the device record from the Samsung service, Active Directory Users and Computers, Admin Portal, and Samsung SDS IAM &amp; EMM directory. This removes the device listing from Admin Portal and the user portal too.</td>
</tr>
</tbody>
</table>

**Notes**
- If you delete an enrolled device, the device is unenrolled. The user is prompted to enter his credentials the next time he opens the Samsung SDS IAM & EMM client to re-enroll the device.
- In Active Directory Users and Computers, the Delete command is offered separately from the All Tasks commands.
<table>
<thead>
<tr>
<th>Device Management</th>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fetch Device Log</td>
<td>Samsung Knox Workspace and Android devices only</td>
<td>Send the audit log file in the device to an email address.</td>
</tr>
<tr>
<td></td>
<td>Admin Portal only</td>
<td><strong>Note:</strong> Set the Common Mobile Settings &gt; Enable debug logging policy to get richer debug information. You specify the email address when you click the command. You can also set an option to send the log file when the device is on Wi-Fi only.</td>
</tr>
<tr>
<td>Fetch Audit Log</td>
<td>Samsung Knox Workspace and Android devices only</td>
<td>Send the audit log file from the device to an email address.</td>
</tr>
<tr>
<td></td>
<td>Active Directory Users and Computers only</td>
<td><strong>Note:</strong> Set the Common Mobile Settings &gt; Enable debug logging policy to get richer debug information. You specify the email address when you click the command. You can also set an option to send the log file when the device is on Wi-Fi only.</td>
</tr>
<tr>
<td>Force Password Change</td>
<td>Samsung Knox Workspace devices</td>
<td>Force user to create a new password. Users are first prompted to enter their current password. If this fails, the user cannot create a new password. If the device is on, the prompt is displayed as soon as the command is received. If the device is off, the prompt is displayed the next time it’s turned on.</td>
</tr>
<tr>
<td></td>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
<tr>
<td>Lock Screen</td>
<td>All devices</td>
<td>Closes the screen. To restore the screen, the user must enter the passcode.</td>
</tr>
<tr>
<td></td>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
<tr>
<td>Device Lockout</td>
<td>Samsung Knox Workspace devices only</td>
<td>Lock down the device. This command lets you define a passcode that must be entered to unlock the device. In addition, the command lets you specify a lockout message that is displayed on the device.</td>
</tr>
<tr>
<td></td>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
<tr>
<td>Device Management</td>
<td>Availability</td>
<td>To do this</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lock Client App</td>
<td>iOS and Android devices only Admin Portal and Samsung SDS IAM &amp; EMM user portal</td>
<td>Locks the Samsung SDS IAM &amp; EMM client on the device.</td>
</tr>
<tr>
<td>Reset Client App PIN</td>
<td>iOS and Android devices only Active Directory Users and Computers, Admin Portal, and Samsung SDS IAM &amp; EMM user portal</td>
<td>Resets the passcode for the client application on the device. This command is useful when users forget their passcodes.</td>
</tr>
</tbody>
</table>
| Ping                       | All devices Active Directory Users and Computers and Admin Portal only         | Send a message to the device and update the device’s “last seen” timestamp. Use this command to determine if an enrolled device in the Unreachable state is back in communication with the Samsung service. If the device acknowledges the message, the Samsung service updates the timestamp used to determine whether or not the device is still in use.  
**Note:** After you send the ping command, refresh the browser page to update the device’s status.             |
| Power Off Device           | Samsung Knox Workspace devices only Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM & EMM user portal | Turn off the device.                                                                                                                     |
| Reapply Policies           | All devices Active Directory Users and Computers and Admin Portal only       | Install all of the current group policy profiles (rather than only the updated policies) on the device.  
**Note:** Group policies are not installed on devices for users with accounts in Samsung SDS IAM & EMM directory alone. |
<p>| Reboot Device              | Samsung Knox Workspace devices only Active Directory Users and Computers only | Force the device to reboot.                                                                                                             |</p>
<table>
<thead>
<tr>
<th>Device Management</th>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
</table>
| Reset Password           | All devices                                                                  | Force user to create a new passcode. This command just prompts the user to create a new password. (Use Force password change if you want to authenticate the user before the passcode can be changed.)  
If the device is on, the prompt is displayed as soon as the command is received. If the device is off, the prompt is displayed the next time it’s turned on.  
Note: This command does not undo a lock command                                                                 |
| Unenroll Device          | All devices                                                                  | Suspend the device from the Samsung service. This removes all mobile device policy profiles installed on the device. It does not, however, remove the Samsung SDS IAM & EMM client.  
To use the Samsung service again, the user must enroll the device again.  
Note: You can set a policy that prevents users from unenrolling a device. See “Using the Common Mobile Settings” on page 228. |
| Update Policies          | All devices                                                                  | Push the current mobile device policies for installation on the device. This command ensures that the device has the latest mobile device policy settings.                                                                                                                                         |
| Wipe Device              | All devices                                                                  | Remove all user data and restore the device to its shipping default state.  
**Note:** You can set a policy that prevents users from wiping a device. See “Using the Common Mobile Settings” on page 228.                                                                 |
| Show FileVault Recovery  | OS X devices (10.9 or later)                                                 | Retrieve a device’s FileVault recovery key. FileVault recovery keys are only available after the FileVault policy is pushed to a device and applied (triggered by an administrator login after the policy is pushed).  
This key is stored permanently in Admin Portal, even if the FileVault encryption policy is disabled in the Policy tab, or the device is unenrolled. |

---

**Admin Portal user’s guide**
Using the device management commands

### SSO Management

<table>
<thead>
<tr>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>All devices</td>
<td>Disable single sign-on for web applications listed in the Samsung SDS IAM &amp; EMM client and, on Knox devices, in Samsung SDS IAM &amp; EMM WebApps and the mobile applications that use the Samsung Knox SSO service. You would use this command, for example, if the device is misplaced or stolen. After this command is sent, an error message is displayed when the user opens the application indicating that SSO is disabled. The user cannot open any application on the selected device that uses SSO until the Enable SSO command is sent.</td>
</tr>
<tr>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
</tbody>
</table>

### Enable SSO

<table>
<thead>
<tr>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>All devices</td>
<td>Enable single sign-on for the web applications listed in the Samsung SDS IAM &amp; EMM client and, for Knox devices, in Samsung SDS IAM &amp; EMM WebApps, and the mobile applications that use the Samsung Knox SSO service. By default SSO is enabled. This command is provided so you can enable single sign-on again for a device that previously had it disabled.</td>
</tr>
<tr>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
</tbody>
</table>

### Call Log Management

<table>
<thead>
<tr>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Knox Workspace devices only</td>
<td>Reset the call counts.</td>
</tr>
<tr>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Knox Workspace devices only</td>
<td>Reset the count of cellular data network bytes received and sent.</td>
</tr>
<tr>
<td>Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td></td>
</tr>
<tr>
<td>Container Management</td>
<td>Availability</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Create Container         | Samsung Knox Workspace devices only  
Active Directory Users and Computer and Admin Portal  
(not available from the Samsung SDS IAM & EMM user portal) | Enable the user to create a Samsung Knox enterprise container after enrolling the device.  
When you use this command, the Samsung SDS IAM & EMM client adds the Create Knox container option to the Setup screen. |
| Disable Container        | Samsung Knox Workspace devices only  
Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM & EMM user portal | Lock the Knox enterprise container.  
Users cannot open the container until an Enable Container command is sent to the device. |
| Enable Container         | Samsung Knox Workspace devices only  
Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM & EMM user portal | Unlock the Knox enterprise container.  
If the device is locked using the Disable container command, the user cannot open it until this command is sent to the device. |
| Re-Authenticate SSO      | Samsung Knox Workspace devices only  
Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM & EMM user portal | Force the user to enter his credentials the next time he logs in to an application configured for single sign-on.  
Normally, the user does not need to log in to any applications configured for single sign-on.  
After you issue this command, they next time the user opens any mobile application installed in the Samsung Knox container that uses the single sign-on interface she is prompted to enter her credentials. The user is prompted just once. |
<table>
<thead>
<tr>
<th>Container Management</th>
<th>Availability</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove Container</td>
<td>Samsung Knox Workspace devices only Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal This command is not available to administrators with the Device Management (Limited) role permission.</td>
<td>Remove the Knox enterprise container. This command does not remove a Knox personal container.</td>
</tr>
<tr>
<td>Reset Container Password</td>
<td>Samsung Knox Workspace devices only Active Directory Users and Computers, Admin Portal, and the Samsung SDS IAM &amp; EMM user portal</td>
<td>Force the user to create a new password for the enterprise container. If the user is inside the container when the command is sent, the user is prompted to change the password the next time he tries to re-enter.</td>
</tr>
</tbody>
</table>
Managing policy compliance

System administrators can track the policy compliance of all enrolled devices. A compliant device means it has received all assigned policies and the user has applied all relevant policies (some policies require user configurations).

You control policy compliance tracking at the policy set level. If you enable policy compliance tracking for a specific policy set, then all policies listed on the Policy Summary page will be checked for compliance.

You can see the compliance status of each enrolled device from the Devices page and on the Device Details page for each device. A device’s overall compliance status is determined by the policy sets applied to the user. If all policies within those policy sets are in compliance, then the device receives a Compliant status. If even one policy is out of compliance, then the device receives a Non Compliant status. If there are conflicting compliance responses because you have multiple policy sets, then the top-most policy set (as configured on the Policies page using drag/drop) is applied for compliance tracking. See Using hierarchical policy sets. For example, the Policy Setting page (shown above) shows this device has two policy sets applied (Migrated MDM Configuration and dianaCloud policy). Any conflicting compliance responses are resolved based on the hierarchy of the two policy sets.
Working with Samsung Knox devices

Samsung Knox devices are similar to other Android devices in several ways; for example, users install the same Samsung SDS IAM & EMM client and can send the same device commands to update policies, reset the password, etc. However, if you are using the Samsung service for mobile device management, you have many more commands you can send to the Knox Workspace devices, and there are many more mobile device policies you can set. The commands are described earlier in this chapter (see “Using the device management commands” on page 165). The mobile policies are introduced in “Using the Samsung KNOX Device Settings” on page 231 and “Using the Samsung KNOX Workspace Settings” on page 235.

In addition, users with Samsung Workspace devices can create a Samsung Knox mode container. A Knox mode container is a password-protected area in which users can manage, maintain and protect information separate from the applications and files on the device. You can also purchase licenses to deploy mobile and web applications that are available to the user from the container only.

This section describes working with Samsung Knox devices and containers when you are using the Samsung service for mobile device management. If you are using another service for mobile device management, these topics do not apply to you, and you can skip to “Using KNOX Workspace devices in a single sign-on configuration” on page 181.

This section contains the following topics:

- “KNOX Workspace device properties” on page 174
- “Enterprise versus personal KNOX containers” on page 175
- “Enabling the device to allow users to create an enterprise container” on page 176
- “Determining the KNOX container version” on page 177
- “Deploying a system wide VPN client to KNOX Workspace devices” on page 178
- “Working with UMC supported KNOX devices” on page 179
- “Bulk enrollment” on page 179
- “Moving files and data between the container and device” on page 179
- “Enabling enterprise billing” on page 180
- “Adding mobile applications that use SSO to the Application SSO whitelist” on page 180
- “Using KNOX Workspace devices in a single sign-on configuration” on page 181
Knox Workspace device properties

If you are managing Samsung Knox Workspace devices, the device details screen adds the following fields under Operating System Settings which can be useful for device management:

<table>
<thead>
<tr>
<th>Operating System Setting</th>
<th>Indicates this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit log</td>
<td>Indicates if the audit log is enabled or disabled. The device can record an audit log of user activities that you can fetch in Admin Portal (see “Using the device management commands” on page 165)</td>
</tr>
<tr>
<td></td>
<td>To enable the audit log, set the Samsung Knox Workspace Settings &gt; Device Settings &gt; Enable audit log policy in either Active Directory or the Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td>Knox Attestation State</td>
<td>Indicates if software attestation is enabled. Attestation state indicates whether the device’s boot loader, kernel, and system software have been modified. Attestation is confirmed when the user enrolls the device and periodically after that by the MDM provider.</td>
</tr>
<tr>
<td></td>
<td>By default, this policy is not enabled. To enable attestation, set the Samsung Knox Workspace Settings &gt; Require attestation verification policy in either Active Directory or the Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td>Knox Container</td>
<td>Indicates the status of the Knox container as follows:</td>
</tr>
<tr>
<td></td>
<td>• Active: The user has created a Knox enterprise container, and the Samsung service is the mobile device management provider</td>
</tr>
<tr>
<td></td>
<td>• Creation in progress: A Knox container is being created on the device.</td>
</tr>
<tr>
<td></td>
<td>• Does not exist: A Knox enterprise container has not been created on the device.</td>
</tr>
<tr>
<td></td>
<td>• Lock: The Knox enterprise container has been locked.</td>
</tr>
<tr>
<td></td>
<td>• Removal in progress: The Knox container is being removed from the device.</td>
</tr>
<tr>
<td></td>
<td>• Unmanaged: There is a Knox container on the device, however, it is a personal container or an enterprise container managed by another mobile device management provider.</td>
</tr>
<tr>
<td>Knox Device SDK Version</td>
<td>Indicates the device’s MDM software version. The MDM version determines which mobile device policies are available to you in the Active Directory Group Policy Management Editor and Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td>Knox Workspace SDK version</td>
<td>Indicates the device’s Knox container version. This affects several aspects of container usage. See “Determining the KNOX container version” on page 177 for the details.</td>
</tr>
</tbody>
</table>
Enterprise versus personal Knox containers

All Samsung Knox Workspace devices allow users to create a Knox enterprise container when the licenses have been procured and you have enabled the device to allow the user to create a container. Some Knox Workspace devices let users create a personal container. A personal container provides many of the same features as the enterprise container—that is, the personal container is also a password-protected, private workspace with its own set of applications and file folders. You do not need to set a policy to enable users to create a personal container.

Devices can have only one container—either a personal or an enterprise container—on a device. If the user creates a personal container and then creates an enterprise container, the personal container and all of its files are deleted and the mobile applications in the container are uninstalled.

When you use the Samsung service for mobile device management, the Samsung SDS IAM & EMM client automatically installs Samsung SDS IAM & EMM WebApps in an enterprise container. However, users with personal containers must download and install the application themselves. The instructions are provided in the user portal online help. When they do, Samsung SDS IAM & EMM WebApps lists all of the web applications you assign in Admin Portal and provides single sign-on to those applications.

There are several operational differences that distinguish personal from enterprise containers:

- Single sign-on to Samsung SDS IAM & EMM WebApps is not supported when it is installed in the personal container. Users must enter their credentials every time they open Samsung SDS IAM & EMM WebApps. (However, they are not prompted to enter their credentials when they open the web applications.)

- If users with personal Knox containers don't install the Samsung SDS IAM & EMM client on their devices, the devices do not appear in the Devices screen in Admin Portal and do not appear in users' Devices screen in the Samsung SDS IAM & EMM user portal.

<table>
<thead>
<tr>
<th>Operating System Setting</th>
<th>Indicates this setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Successful Knox Attestation Check</td>
<td>Indicates the last time attestation was performed to confirm that the devices's boot loader, kernel, and system software have not been modified.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This setting is displayed only when the “Require attestation verification” Samsung Knox Workspace policy is set.</td>
</tr>
<tr>
<td>Log SMS</td>
<td>Indicates if short message service logging is enabled or disabled. By default, SMS logging is disabled. To enable this SMS logging, set the Samsung Knox Device Settings &gt; Device Inventory Settings &gt; Enable logging of SMS policy in either Active Directory or the Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
</tbody>
</table>
After the user creates an enterprise container, the mobile device policies are installed, Samsung SDS IAM & EMM WebApps is installed, and the Knox SSO service is updated and enabled. This takes a minute or two to complete. Users can then open Samsung SDS IAM & EMM WebApps to launch the web applications you assign to them. If you deployed any mobile applications for automatic installation, they are installed on the device right after the device is enrolled too.

---

**Notes**

- When you set the “Enable Knox container” policy, the Samsung SDS IAM & EMM client does not include the Web Apps screen on Knox 2 devices. However, on Knox 1 devices, the Samsung SDS IAM & EMM client contains the Web Apps screen until the user runs the “Enable Samsung Knox Workspace mode” command.

- On Verizon devices only, the Chrome browser is automatically installed in the container. To prevent Chrome from being installed use the Samsung Knox Workspace Settings > Application Management > Applications that can be installed policy.

---

**Enabling the device to allow users to create an enterprise container**

Users cannot create a Knox enterprise container until you set the “Enable Knox container” policy (see “Using the Samsung KNOX Workspace Settings” on page 235) in a Samsung SDS IAM & EMM policy service policy set or Active Directory group policy object.

On Knox version 1 devices, this results in two commands being added to the SETUP REQUIRED screen in the Samsung SDS IAM & EMM client:

- **Enable Samsung Knox Workspace mode:** This command confirms that you have a sufficient license key to create a container and activates one of your licenses.

- **Create Knox container:** This command launches the container creation procedure.

On Knox version 2 devices, the license validation and activation is done transparently and the container creation process is launched immediately at the end of device enrollment when you set this policy.

The instructions for creating the Knox container are in the user portal.

To enable a user to create a Knox enterprise container by using the Samsung SDS IAM & EMM policy service:

1. Open Admin Portal and select the policy set applied to the users’ role.
2. Expand **Policies**, **Mobile**, and **Samsung Knox Workspace Settings**.
3. Click **Enable Knox container** and then use the drop-down list to select **Yes**.
4. Click **Save**.
To enable a user to create a Knox enterprise container by using the Group Policy Management Editor:

1. Open the Group Policy Management Editor and select the group policy object you have linked to the Active Directory container with the Samsung Knox devices.
2. Expand Samsung SDS IAM & EMM Management Settings and select Samsung Knox Workspace Settings.
3. Double-click Enable Knox container.
4. Select Policy enabled and click OK. (The policy is set “True” by default.)

**Determining the Knox container version**

There are two versions of Samsung Knox Workspace devices extant in the marketplace. There are differences in some device behaviors and user procedures for devices that have a Knox version 1 versus a version 2 container. In addition, some policies are only available on Knox version 2 containers (for example, moving files between personal space and the container.) The Knox container version number depends upon the Knox Workspace SDK version installed in the device.

The following procedure describes how you determine the Knox container version from the Knox Workspace SDK version. The device must be enrolled to perform this procedure.

To determine the device’s Knox container version:

1. Open Admin Portal and click the Devices tab.
2. Click the Knox Workspace device and then click Details.
3. Scroll down through the Operating System Settings to Knox Workspace SDK Version.

The field value indicates the Knox container version number as follows:

<table>
<thead>
<tr>
<th>Entry</th>
<th>Knox Container version number</th>
</tr>
</thead>
<tbody>
<tr>
<td>KNOX_ENTERPRISE_SDK_VERSION_1_x_x</td>
<td>1</td>
</tr>
<tr>
<td>KNOX_ENTERPRISE_SDK_VERSION_2_x</td>
<td>2</td>
</tr>
</tbody>
</table>

*Note* Users can perform a similar procedure from the user portal.

**Deploying a system wide VPN client to Knox Workspace devices**

If you are configuring a system wide VPN client policy (that is, a VPN client that will be used from both the device and the container), you should deploy the VPN client binary from Admin Portal.
You can deploy the binary from Google Play. Alternatively, if you have the binary, use the Android InHouse template to deploy the client. You deploy the VPN client in the same manner you would deploy any mobile application from Google Play to Android devices. See “Adding and deploying mobile applications using Admin Portal” on page 138 for the details.

For Knox version 2 devices, the Samsung SDS IAM & EMM client automatically installs the VPN client on the device and in the container. On Knox version 1 containers, the VPN client is only installed on the device. You do not need to install it in the container.

The following VPN clients packages are currently supported:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Client software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jupiter</td>
<td>Junos Pulse (do not use the Junos Pulse for Samsung version)</td>
</tr>
<tr>
<td></td>
<td>You can get this client from Google Play.</td>
</tr>
<tr>
<td>F5</td>
<td>F5 BIG-IP Edge Client</td>
</tr>
<tr>
<td></td>
<td>You can get this client from Google Play.</td>
</tr>
<tr>
<td>Mocana</td>
<td>This VPN client is only available from the Samsung Knox web site and you must</td>
</tr>
<tr>
<td></td>
<td>have an account to download it. Go to <a href="https://www.samsungknox.com">https://www.samsungknox.com</a>, log in to your account, click Download Knox VPN Client, and follow the instructions to download the binary file. Then, open Admin Portal and open the Apps page. Click Add Mobile Apps, click the Add Custom App tab, and click the Add button for Android InHouse to upload the binary. See “Adding and deploying mobile applications using Admin Portal” on page 138 for more details.</td>
</tr>
</tbody>
</table>

If you are using the Jupiter Junos Pulse client, the user must accept the end user license agreement (EULA) before the VPN profile can be configured. Users gets an outstanding item in the Setup item in the Samsung SDS IAM & EMM client screen menu and an error message when they open the VPN profile in the SETUP REQUIRED screen.

To complete the configuration, users exit the Samsung SDS IAM & EMM client application, open the Junos Pulse application on the device, and accept the EULA. Users can then close the Junos Pulse application, open the Samsung SDS IAM & EMM client, open the Setup screen and tap the Junos Pulse client to complete the installation.

On Knox version 2 containers, if you are configuring the VPN for system-wide use—that is, the same VPN is used for all applications—the user must accept the EULA for the Junos Pulse client installed on the device and in the container. If you are configuring the VPN client for per-app use, the user needs to accept the EULA in the Junos Pulse client installed on the device only.

The Junos Pulse configuration instructions are provided in the user portal help in the section that describes creating a Knox container.
Working with UMC supported Knox devices

Some Samsung Knox devices are equipped with the Universal Mobile Device Management Client (UMC). Users with UMC supported devices can simply enter their Samsung service user name and password to install the Samsung SDS IAM & EMM client on their device and enroll it to the Samsung service. These users do not need to get the Samsung SDS IAM & EMM client from Google Play and install it manually.

When the user opens the UMC, the software contacts the Samsung Enterprise Gateway, a different service containing records of which account login suffixes are associated with which mobile device management services. The Samsung Enterprise Gateway receives the enrollment request from the UMC, parses the account name in the request to extract the login suffix, and uses that to contact the MDM provider that has previously registered that login suffix in the gateway. The MDM provider then installs its client software in the device.

To automate installation of the Samsung SDS IAM & EMM client using UMC, however, you must enable the policy that automatically updates the Samsung Enterprise Gateway every time you make a login suffix change. See “Enabling Samsung KNOX UMC login suffix updates” on page 348 for the details.

Bulk enrollment

System administrators with a Samsung account can use the Samsung Knox Mobile Enrollment user interface to bulk enroll devices. Accounts can be created from https://www.samsungknox.com/me.

As part of the configuration, you will need to enter your tenant URL followed by /umdm. For example, https://test.my-company.com/umdm.

Also note that we are only supporting mandatory authentication.

Specific instructions for configuring bulk enrollment are covered in the Samsung documentation.

Moving files and data between the container and device

You can set policies that control whether users can move files between the device and the container. In addition, you can set a policy that synchronizes the data in applications with instances installed inside and outside of the container.

Note These policies are only available for Knox version 2 containers.

See “Restriction Settings” on page 402 for the policies that let you control whether users can move data out of or into the container. The user opens the My Files app in the device or container to select and the move the files. Users cannot copy the files, they can only move them.
See “Application Management” on page 398 for the policy that synchronizes the data. You use the policy to specify the application and the direction of the data (to or from the container and the device). You can specify multiple applications.

**Enabling enterprise billing**

Enterprise billing allows separate bill generation for personal and enterprise data usage. You enable it using the Enable Enterprise Billing (if you are using Active Directory/LDAP group policy for device policy management) or the Enterprise Billing (if you are using the Samsung SDS IAM & EMM policy service) in the Samsung Knox Workspace Settings.

*Note*  This feature is only available for devices that have Knox 2.1.

You would enable this policy for employees who bring their own devices to work. The policy lets you to have two different Access Point Names (APNs) that separates data usage over mobile internet (2G/3G/4G) connections. The default APN is used for routing personal data connections and the second, enterprise APN is used for the following:

- All data traffic from a Knox container
- All data traffic from the Samsung SDS IAM & EMM client

Before you can use this policy you need to work with your mobile network operator for the following:

- The mobile network operator must create a separate, enterprise APN for you. This is the APN that will be used for enterprise data. You specify this APN in the policy.
- The mobile operator must record the transactions over the enterprise APN separately so that enterprise data can be billed separately.

When you configure the policy, you also need to enter the mobile country code and the mobile network code.

**Adding mobile applications that use SSO to the Application SSO whitelist**

The Knox container has a Knox SSO Service which provides single sign-on for mobile applications installed in the container. All applications that you deploy or users install in the Knox container that use the Knox SSO Service must be added to the device’s Application SSO whitelist before the user can open the application. In addition, the device must have a valid Samsung Knox SSO license.

You add an application to the device’s SSO whitelist by adding the application’s package name to the Application SSO whitelist policy in the group policy object or policy set.

*Note*  Samsung SDS IAM & EMM WebApps uses the Samsung Knox SSO Service. However, it is automatically added to the device’s Application SSO whitelist when the user creates the Knox container using the Samsung SDS IAM & EMM client. (It will not be listed in the Application SSO whitelist policy.)
The following procedures describe how to add applications to the Application SSO whitelist policy using the Samsung SDS IAM & EMM policy service and the Group Policy Management Editor.

To add a mobile Android app to the Application SSO whitelist using the Samsung SDS IAM & EMM policy service:

1. Open Admin Portal and select the policy set.
2. Expand Policies, Mobile, Samsung Knox Settings, and Container Settings.
3. Click Applications Settings and click the Application SSO Whitelist Add button.
4. Enter the application’s package name.
   
   **Note** The package name is not the application name.
5. Click Save.

To add a mobile Android app to the Application SSO whitelist using the Group Policy Management Editor:

1. Open the Group Policy Management Editor and select the group policy object you have linked to the organization unit with the Samsung Knox devices.
2. Click Samsung SDS IAM & EMM Management Settings > Samsung Knox Workspace Settings > Container Settings > Application Management.
3. Double-click Application SSO whitelist.
4. Click Policy enabled and the Add button.
5. Enter the application’s package name and click OK.
   
   **Note** The package name is not the application name.
6. Click OK to exit the dialog box.

**Using Knox Workspace devices in a single sign-on configuration**

If you are not using the Samsung service for mobile device management, you can still use it for single sign-on to web applications. (See “How to configure Mobile Device Management or single sign-on only” on page 18 to select the Samsung service for mobile device management or opt out.) When you do not use the Samsung service for mobile device management, users install the Samsung SDS IAM & EMM client on the device to enroll just their account in the Samsung service. This provides single sign-on to the web applications you assign to them in Admin Portal. However, the Samsung service does not enroll the device in the Samsung service.

If your users are creating Knox mode containers, they can also install Samsung SDS IAM & EMM WebApps in the container to launch the web applications you assign to them from
inside the container. However, in this case Samsung SDS IAM & EMM WebApps is not automatically installed in the container. Instead, you use the mobile device management provider’s procedures to configure the container. There are two parts to the configuration:

- Installing the application
- Enabling single sign-on

**Deploying Samsung SDS IAM & EMM WebApps**

You will need to work with your mobile device management provider to deploy the Samsung SDS IAM & EMM WebApps mobile application to the users and install it in the container.

Use the following URLs to download the Samsung SDS IAM & EMM WebApps binary apk file. There are two version: one for Knox version 1 containers (this version is wrapped) and one for Knox version 2 containers (this version is not wrapped).

*Note* In all of the following URLs, you replace `vv_r-bbb` with the file’s version, revision and build number. Contact Support to get the correct numbers for your account.

- Sample URL for Knox version 1 containers:
  

- Sample URL for Knox version 2 containers:
  

**Enabling single sign-on in a Knox mode container**

There are two aspects to enabling single sign-on in a Knox mode container:

- Turn on the Knox SSO Service.
  
  On Samsung Workspace devices, single sign-on in a Knox mode container is provided through the Knox SSO Service. When you use the Samsung service for mobile device management, the Knox SSO Service is installed and enabled automatically. When you have another mobile device management provider, it is their responsibility to either enable the pre-loaded SSO service or install and enable a replacement.

- Specify the applications that can use the Knox SSO Service.
  
  Samsung Knox Workspace devices restrict access to the Knox SSO Service to mobile applications that have been listed on a SSO whitelist in the device. When you are using the Samsung SDS IAM & EMM policy service to manage devices, for example, you use the Application SSO whitelist policy to specify the applications. However, how you add applications to the device’s SSO whitelist will vary with each mobile device management provider.
You must add Samsung SDS IAM & EMM WebApps to the SSO whitelist to provide single sign-on to the web applications. In many cases, to add the application you are required to provide its package name. If your mobile device management provider requires you to specify the package name for Samsung SDS IAM & EMM WebApps use the following: com.samsungemm.sso.myapps.
Working with Samsung Knox devices
Managing policies

You use the Policies tab in Admin Portal to create policy sets for roles. A policy set lets you configure the following categories of policies:

- **Mobile Device Policies**
  
  Use to set device management settings (for example, time periods for device information updates and unresponsive devices) and device enrollment settings (for example, whether users can enroll devices and the number and types of devices they can enroll).

  The Mobile Device Policies are only available if you use the Samsung service for mobile device management. (See “How to configure Mobile Device Management or single sign-on only” on page 18.) If you are using the Samsung service for single sign-on only, the Mobile Device Policies are not included.

  If you are using Samsung service for device policy management (see “Selecting the policy service for device policy management” on page 345), the set of Mobile Device Policies also includes configuration policies for Android, Samsung, and iOS devices.

  If you have selected Active Directory group policy for device policy management rather than the Samsung SDS IAM & EMM policy service, then you use Active Directory Group Management Editor to configure the device policies.

- **Account Security Policies**:
  
  You can use account security policies to set and configure policies for multifactor authentication, user self-service controls, and the password requirements for Samsung SDS IAM & EMM directory accounts.

- **Application Policies**
  
  You can use the application policy to prevent users from adding web applications from their user portal and allow users to view/copy their personal passwords. By default, users can add web applications on their portal.

Information relevant to policies:

- “Using policy sets” on page 187
- “General device management settings” on page 189
- “Authentication - Setting authentication policy controls” on page 193
- “Setting password controls” on page 199
- “Managing Application policies” on page 220
- “Managing device configuration policies” on page 221
“Mobile device configuration policies overview” on page 227
“Configuring OATH OTP” on page 201
“Configuring derived credentials” on page 202
Using policy sets

Policy settings are installed initially when the user enrolls the device. They are updated automatically according to the policy push delay or update interval you set. See “Selecting the policy service for device policy management” on page 345 for the details. You can also update the policies in real time—see “Updating device configuration policy changes” on page 188 for the details. To apply the policy set to users, you apply the policy set to one or more roles.

You can set up hierarchical policy sets so that, for example, a base policy set can be applied to all users and then other policy sets can be applied to smaller sets of users (for example, the sales and support departments). See “Using hierarchical policy sets” on page 187 for the details.

You can see your current policy settings by clicking Summary. Click the link to open the category if you want to make changes.

Using hierarchical policy sets

You can apply multiple policy sets to the same role. For example, you might create a global policy set to define basic policies for all users and then create more policy sets for a subset of those users.

The Samsung service reads the policy sets from bottom to top on the Policy page when it installs the policies in a device. If the same policy has different settings in different policy sets, the setting in the last policy set read—the top-most—is applied.

The same bottom-to-top process is applied to mobile device policies. See “Managing device configuration policies” on page 221 for more information on using mobile device policies in hierarchical policy sets.

For users in multiple roles, the Samsung service first determines which policy sets apply to the user and then reads those policy sets from bottom to top to apply the policies. The hierarchical order of the roles has no effect upon the order in which the policy sets are read.

If you want one policy setting to be enforced over another one, drag that policy set up in the list.

Editing a policy set

To change policies in a policy set, select the policy set from the Policies page. You can see the current setting for the policies you have set previously by clicking Summary. The Summary page does not show the default value for policies you have not modified.

Changes to device management and enrollment settings, account security policies, and applications policies are implemented immediately. Changes to the device configuration policies are deployed to the devices according to your configuration. See “Updating device configuration policy changes” on page 188.
Updating device configuration policy changes

After you change a device configuration policy, the Samsung service automatically updates the devices according to the policy push delay or update interval you set in Device Policy Management on the Settings page in Admin Portal (see “Selecting the policy service for device policy management” on page 345).

If you are using Active Directory Group Policy Management to define policies, you update user with policy changes using Active Directory Users and Computers.

To update all devices when you use the Samsung SDS IAM & EMM policy service:

1. In Admin Portal, click the Policy tab.
2. Click Push Policy.
3. Click Yes in the pop up window.

To push policy set changes to individual devices:

1. In Admin Portal, click the Devices tab.
2. Right click the device listing.
3. Click Update Policies.

To push a group policy object changes to individual devices:

1. Open Active Director Users and Computers
2. Open the organizational unit with the devices.
3. Select the devices.
4. Right-click and expand All Tasks and then Device Management.
5. Click Update Policies.
General device management settings

The Samsung SDS IAM & EMM identity platform provides numerous device policy controls for device management. This table lists the general device policy controls and their location on the Admin Portal.

The Common Mobile Settings policies are available to Knox Express for IT and Knox Premium licenses. Note, however, that to set policies using the Active Directory Group Policy Management Editor, you must have a Knox Premium license. Otherwise, you can set policies through the Samsung SDS IAM & EMM policy service only.

<table>
<thead>
<tr>
<th>Policy Setting Name</th>
<th>What it does</th>
<th>Location on Admin Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the Samsung service service for mobile device management (default yes)</td>
<td>Configure the Samsung SDS IAM &amp; EMM identity platform for mobile device management or single-sign-on only. See <a href="#">How to configure Mobile Device Management or single sign-on only</a> for more information on this policy setting.</td>
<td>Policies &gt; Mobile Device Policies &gt; Device Management Settings</td>
</tr>
<tr>
<td>Update device information frequency (default 12 hours)</td>
<td>Defines the frequency in which the Samsung service pings the device -- also known as device polling. If the device does not respond, it pings it again after 90 minutes. Each ping requests the current information on device properties, installed applications, and installed mobile device policies. The Samsung service uses this information to update the device properties displayed in Admin Portal and the Samsung SDS IAM &amp; EMM user portal.</td>
<td>Policies &gt; Mobile Device Policies &gt; Device Management Settings</td>
</tr>
<tr>
<td>Mark unresponsive devices as “Unreachable” threshold (default 14 days)</td>
<td>A device is designated “unreachable” if the Samsung service does not get a ping response or the user does not open the Samsung SDS IAM &amp; EMM client on the device during the period you set. The device remains enrolled after the status is changed to “Unreachable.” If the device responds to a ping or the user opens the Samsung SDS IAM &amp; EMM client client, the status is changed back to reachable.</td>
<td>Policies &gt; Mobile Device Policies &gt; Device Management Settings</td>
</tr>
<tr>
<td>Enable Derived Credentials Issuance (default no)</td>
<td>Allows derived credentials to be issued to enrolled devices as part of configuring mobile devices to use smart card authentication. See <a href="#">Configuring derived credentials</a> for more information about the feature.</td>
<td>Policies &gt; Mobile Device Policies &gt; Device Management Settings</td>
</tr>
<tr>
<td>Allow authentication notification on multiple devices</td>
<td>Allows authentication notifications to be sent to multiple enrolled devices. Selecting “No” sends notifications to the primary device only. Default setting is “No”.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Common</td>
</tr>
<tr>
<td>Policy Setting Name</td>
<td>What it does</td>
<td>Location on Admin Portal</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable debug logging</td>
<td>Turns on the debug logging mode on the device. The Samsung SDS IAM &amp; EMM application supports two logging modes: regular and debugging. Only limited logs are collected in regular mode. You set this policy to collect the full range of logs supported. By default regular mode is enabled.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Common</td>
</tr>
<tr>
<td>Encrypt internal onboard storage</td>
<td>Encrypts the storage system on Android devices. Select Yes to prompt the user to encrypt the secure (application data) storage area, No to allow the storage area to allow devices to back up without using encryption. For some Samsung devices, this policy is automatically set when you enable Common Criteria mode, however, the setting is not shown in the policy. This allows you to set a different value for this policy for other devices. This policy applies to Android devices version 3.0 or later and is not supported on iOS and OS X devices.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Common</td>
</tr>
<tr>
<td>Permit camera use</td>
<td>Sets the ability for device owner to use the camera. See the bubble help associated with this setting for more information. <strong>Important:</strong> A &quot;No&quot; configuration will override any configurations made to the same setting in the Knox container. This means that a &quot;No&quot; configuration will disable camera use on both the device and Knox container.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Restriction Settings</td>
</tr>
<tr>
<td>Permit user to enroll devices</td>
<td>Allows users to enroll their devices to the Samsung service.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Restriction Settings</td>
</tr>
<tr>
<td>Permit user to wipe devices</td>
<td>Allows users to wipe their devices. For iOS devices, this policy applies only to devices with iOS 8 or later that are configured as &quot;supervised&quot; in Apple Configurator. For Android devices, this policy applies only to devices that are configured for Android for Work device owner mode and support Samsung Knox Device SDK version 4.0 or later.</td>
<td>Policies &gt; Mobile Device Policies &gt; Common Mobile Settings &gt; Restriction Settings</td>
</tr>
</tbody>
</table>
### Policy Setting Name: Report mobile device location
- **What it does:** Allows devices to report their locations. If you select “Yes” or “--”, you need to configure the related policy setting (Enable admin location sharing).
- **Location on Admin Portal:** Policies > Mobile Device Policies > Common Mobile Settings > Restriction Settings
- **Details:** Selecting “Yes” or “--” and “Disable” for the “Enable admin location sharing” policy setting means the device location is only available to the user.

### Policy Setting Name: Enable admin location sharing
- **What it does:** Defines if system administrators can see device locations.
- **Location on Admin Portal:** Policies > Mobile Device Policies > Common Mobile Settings > Restriction Settings
- **Details:** Selecting “Disable” means the device location is only available to the user. Selecting “Opt-In” means users are prompted with an allow/deny action and have the ability to change their selection in the device Advanced Settings area. Selecting “Force” means users cannot opt out or access the device location sharing setting.
- **Additional Info:** If users set the “Do not track my device location” option in the user portal (user portal > user account name dropdown > Settings) and you select “Force” for this policy setting, then your configuration overrides the user selection.

### Policy Setting Name: Require client application passcode on device
- **What it does:** Sets the requirement for users to enter a passcode to open Samsung SDS IAM & EMM application on devices.
- **Location on Admin Portal:** Policies > Mobile Device Policies > Common Mobile Settings > Security Settings
- **Details:** Select yes to configure the following related policy settings:
  - **Auto-Lock (minutes)** -- Sets the number of minutes of inactivity before the client application is locked.
  - **Lock on exit** -- Sets the requirement for a passcode to open the client application after the client has been closed.
## General device management settings

<table>
<thead>
<tr>
<th>Policy Setting Name</th>
<th>What it does</th>
<th>Location on Admin Portal</th>
</tr>
</thead>
</table>
| Require passcode on device  | Sets the requirement for users to enter a passcode to access the mobile device. Select yes to configure the following related policy settings:  
• Permit simple value  
• Auto-lock (minutes)  
• Maximum number of failed attempts  
• Grace period for device lock  
• Passcode history  
• Maximum passcode age (days)  
• Minimum number of complex characters  
• Minimum passcode length  
• Require alphanumeric value  
See the bubble help associated with these setting for more information. | Policies > Mobile Device  
Policies > Common Mobile Settings > Security Settings                                                                                                                                 |
| Wi-Fi Settings              | Configure Wi-Fi profiles—Wi-Fi SSID and connection parameters—for iOS, Android, and OS X devices.  
See the bubble help associated with this setting for more information.                                                                                                                                 | Policies > Mobile Device  
Policies > Common Mobile Settings > Wi-Fi Settings                                                                                                                                 |
Authentication - Setting authentication policy controls

You can specify what authentication mechanisms your users need to provide to access the service, as well as if and when multifactor authentication is required. For example, you can create a rule to require that users provide a password and text message confirmation code if they are coming from an IP address that is outside of your corporate IP range. To specify this requirement, you need to create a rule and associate it with an authentication profile.

**Note** You must have a Samsung SDS IAM & EMM+ license key and licenses to use multifactor authentication.

This section contains the following topics:
- “Setting up smart card authentication” on page 193
- “Exempting users without valid authentication methods” on page 194
- “Limiting multifactor authentication from the same device” on page 195
- “Authentication mechanisms” on page 195
- “What you need for each authentication mechanism” on page 197
- “Temporarily suspending multifactor authentication” on page 198
- “Browser cookies associated with authentication policy controls” on page 198

**Setting up smart card authentication**

Smart card log in is a certificate-based log in. The certificate is supplied by the smart card and used by Samsung SDS IAM & EMM to authenticate users. To use smart card authentication with Samsung SDS IAM & EMM identity platform, your users must already be configured for smart card log in.

**Note:** Smart card authentication is a premium feature.

If you need to set up derived credentials for secure mobile access to applications, websites and services that require smart card authentication, see “Configuring derived credentials” on page 202.

To set up smart card authentication:

1. Log in to the Admin Portal, navigate to **Policies**, select the relevant policy or create a new one, select **User Security Policies**, and select **Login Authentication**.

2. Confirm that "Use certificates for authentication" (in the Other Settings section) is enabled (default).

   You must have this option enabled to use smart card authentication. This option allows Samsung SDS IAM & EMM to use the smart card generated certificate to authenticate users to the cloud.
3 (Optional) Enable the "Set identity cookie for connections using certificate authentication" option only if you have a hybrid system where users are logging in using smart cards and another authentication method.

Enabling this option will allow the Samsung SDS IAM & EMM identity platform to write cookies in the browser after a successful log-in. Samsung SDS IAM & EMM will then check the browser for this cookie upon subsequent log ins and take action based on any identity cookie authentication rules you have configured. See “Creating authentication rules” on page 28.

4 Upload your certificate authority chain.
   a Log in to Admin Portal.
   b Click **Settings > Authentication > Certificate Authorities**.
   c Provide a unique name for the trusted certificate authority.
   d Specify the field to use for extracting the user login name from the certificate.
      Select the same field for all certificates in the chain.
   e Click **Browse** to select certificate authority chain for uploading.
      The uploaded chain must contain all certificates for chain validation, starting from intermediate CA trusting to a root certificate authority.
   f (Optional) Select the **Enable Client Certificate Revocation Check** checkbox to allow Samsung SDS IAM & EMM identity service to verify that the smart card certificate has not been revoked.
      If the third party certificate server responses with a revocation URL, then smart card login will be denied. If the Online Certificate Signing Protocol (OCSP) and CRL Distribution Point (CDP) endpoints are reachable via the cloud for some test environments, do not enable this option.
      **Note:** This revocation check is specific to smart card logins. After derived credentials are securely stored on enrolled devices, this check does not impact the derived credentials.
   g Click **Save**.

**Exempting users without valid authentication methods**

The Samsung service looks into the user’s Active Directory/LDAP or Samsung SDS IAM & EMM directory account for the mobile phone number or email address used for multifactor authentication. Normally, users without a mobile phone number or email address cannot log in to the user or administrator portals when you enable authentication policy controls.

Set **Allow users without a valid authentication factor to log in** option to exempt users from multifactor authentication when their account does not have a mobile phone number and email address.
Limiting multifactor authentication from the same device

You can limit the authentication mechanisms available to users when they use the same mobile device for authentication and accessing the user portal. Only the following authentication methods will be available from the same mobile device: email, security question, and password. For example, if a user is accessing the user portal from her mobile phone, then she cannot use that same phone to authenticate via text message, phone call, mobile authentication, or scanning a Samsung SDS IAM & EMM generated QR code.

This policy is intended for government agencies needing to fulfill NIST compliance and is disabled by default.

To limit multifactor authentication from the same device:

1. Log in to the Admin Portal, navigate to Policies, select the relevant policy or create a new one, select User Security Policies, and select Login Authentication.

2. In the Other Settings section, uncheck the Allow additional authentication from same device setting.

3. Click Save.

Authentication mechanisms

You can select the authentication mechanisms that will be available to users. However, the mechanisms ultimately offered to users on the login prompt depend on the account’s properties. For example, if you select all of the mechanisms but a user account has only a user name and email address, then the login prompt will only offer the user-defined security question and email confirmation code options.

To set the authentication mechanisms, see “Creating authentication profiles” on page 30.

The following mechanisms are available:

- **Password**

  When you select this option, users are prompted for either their Active Directory or Samsung service user password when logging in to the Samsung SDS IAM & EMM user portal.

- **Samsung SDS IAM & EMM Mobile Authenticator**

  When you select this option, users authenticate using a one-time passcode displayed by the Samsung SDS IAM & EMM client installed on their mobile devices.

  If devices are connected via the cell network or a wi-fi connection, users can send the passcodes from the devices. If the devices are not connected, users must manually enter the passcodes into the Admin Portal or Samsung SDS IAM & EMM user portal login prompt.
Note  This option requires users to have the Samsung SDS IAM & EMM client installed on their devices and those devices must be enrolled in the Samsung service.

- **Phone call**
  When you select this option, the Samsung service calls the user using the stored mobile phone number and describes an action the user must perform to complete the authentication. The user completes the action from the device to log in.

- **Text message (SMS) confirmation code**
  When you select this option, the Samsung service sends a text message to the user’s mobile phone with a one-time confirmation code and/or an authentication link. Depending on the language setting, some languages display only the confirmation code while others display the confirmation code and link.

  Users who are connected to the Internet can click/tap the link. Otherwise, they need to enter the confirmation code in the login prompt.

  The link and confirmation code are valid for 20 minutes. If a user does not respond within this time period, the Samsung service cancels the login attempt.

- **Email confirmation code**
  When you select this option, the Samsung service sends a confirmation code and a link to the user’s email address.

  Users who are connected to the Internet can click/tap the link. Otherwise, they need to enter the confirmation code in the login prompt.

  The link and confirmation code are valid for 20 minutes. If a user does not respond within this time period, the Samsung service cancels the login attempt.

- **User-defined Security Question**
  When you select this option, users are prompted to answer their security question. If they have not created a security question, they are prompted to do so. Users create or change the question and answer from their Account page in the user portal.

- **OATH OTP Client**
  This text string is configurable and reflects what you entered during the OATH OTP configuration. When you select this option, users can use a third party authenticator (like Google Authenticator) to scan a Samsung SDS IAM & EMM generated QR code and get a one-time-passcode (OTP). This authentication mechanism requires additional configurations. See “Configuring OATH OTP” on page 201.

- **3rd Party RADIUS Authentication**
  When you select this option, the Samsung service communicates with your RADIUS server to allow for user authentication into Samsung SDS IAM & EMM. See Configuring the Samsung SDS IAM & EMM connector for use as a RADIUS client.
What you need for each authentication mechanism

The following table lists the authentication mechanism and the associated Active Directory, LDAP, and Samsung SDS IAM & EMM directory account properties that must be set correctly. If a property is not set correctly, the user may not be able to log in.

<table>
<thead>
<tr>
<th>Authentication mechanism</th>
<th>Required user account property</th>
<th>Active Directory/LDAP Properties tab</th>
<th>Samsung SDS IAM &amp; EMM directory Profile property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Login Name and Suffix</td>
<td>User logon name on the Account tab</td>
<td>NA</td>
</tr>
<tr>
<td>Samsung SDS IAM &amp; EMM Mobile Authenticator</td>
<td>Enrolled device</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Phone call</td>
<td>Mobile phone number</td>
<td>Open the Telephones tab and set the Mobile field</td>
<td>Set the Mobile Number field</td>
</tr>
<tr>
<td>Text message (SMS) confirmation code</td>
<td>Mobile phone number</td>
<td>Open the Telephones tab and set the Mobile field</td>
<td>Set the Mobile Number field</td>
</tr>
<tr>
<td>Email confirmation code</td>
<td>Any valid email address</td>
<td>Open the General tab and set the E-mail field</td>
<td>Set the Email address field</td>
</tr>
<tr>
<td>User-defined security question</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>OATH OTP client</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

Before you enable a specific authentication factor, confirm that each account has current contact information or a currently enrolled device—and make account changes a day before you enable the authentication policy for the accounts. If the information needed for a user’s authentication is not current in the Samsung service, the user will not be able to log in.

If you need to modify a user’s Active Directory or LDAP account, any changes you make are not immediately updated in the Samsung service. For example, it can take up to 24 hours for changes made in Active Directory Users and Computers to be incorporated into the Samsung service.

By contrast, updates made to Samsung SDS IAM & EMM directory accounts go into effect immediately.

**Note** Users can set their Active Directory or LDAP account’s mobile phone number from the user portal. When users change their Active Directory or LDAP account’s mobile phone number using the user portal, the change goes into effect immediately.
Temporarily suspending multifactor authentication

If the user’s account information required for multifactor authentication is not set properly and it prevents the user from logging in, you can use the MFA Unlock command in Admin Portal to suspend multifactor authentication for 10 minutes—see “User Management commands” on page 106. The user must still enter the correct user name and password and is still prompted to enter the additional authentication factor, however, the Samsung service does not validate anything beyond the user name and password. Consequently, the user can, for example, enter any string of characters to fulfill the SMS confirmation code, and the Samsung service accepts the entry.

To temporarily suspend multifactor authentication for a user:
1. Open Admin Portal and select the Users page.
2. Right-click the account for the user who is locked out.
3. Select MFA Unlock.
   
   The user has 10 minutes to log in.

Browser cookies associated with authentication policy controls

When you enable authentication policy controls, the Samsung service leaves the following identity cookies in your users’ browsers:

- After multifactor authentication: The Samsung service leaves a cookie in the current browser after the user has successfully logged in to Admin Portal or the Samsung SDS IAM & EMM user portal by using a multifactor authentication method.
  
  When the Samsung service finds this cookie, it does not prompt the user to provide an additional authentication method for subsequent logins (the user is still required to enter a user name and password) unless the policy is set to always require additional authentication.

- After IWA Authentication: The Samsung service leaves a cookie in the current browser when the user has successfully logged in to Admin Portal or the user portal using Integrated Windows Authentication.
  
  When the Samsung service finds this cookie, it ignores the multifactor authentication requirements and lets a user open a web application from the user portal that is set with the “Restrict app to clients within the Corporate IP range” policy regardless of their IP address (see “Removing an application” on page 130).

Users are required to provide multifactor authentication if the cookies are deleted or they use a different browser to log in.
Setting password controls

You have many options for restricting user password requirements. Use the Password Settings options to set your configurations. In general, you can configure the following:

- To modify the default password policy for Samsung SDS IAM & EMM directory accounts—see “Modifying the default Samsung SDS IAM & EMM directory password policy” on page 199.

- To enable users with Samsung SDS IAM & EMM directory or Active Directory accounts to change their password from the user portal—see “Enabling users to change their password” on page 200.

Modifying the default Samsung SDS IAM & EMM directory password policy

The default setting for each password property is shown in parenthesis; for example the default minimum password length is 8 characters and requirement for a least one digit is Yes.

Notes

- Maximum password age:

  If users do not reset their password before the Maximum password age period expires, they are automatically prompted to reset it the next time they log in. Users must have the “Enable users to change their passwords” policy set to Yes to reset their password.

  If you have multifactor authentication enabled, users are prompted to create a new password after they have fulfilled the multifactor authentication method.

  Enter 0 (zero) if you don’t want to set a password expiration period.

- Password history: Select 0 (zero) to let users use the same password.

To change the default password requirements for Samsung SDS IAM & EMM directory accounts:

1. Open Admin Portal and click Policies, and select a policy set.
3. Use the drop-down lists and text boxes to modify the default setting.
4. Click Save.
Enabling users to change their password

When you enable this policy, the Account page in the user portal displays an option that lets users change their password. If you set this policy to No, the option is not displayed. This policy applies to users with Samsung SDS IAM & EMM directory and Active Directory accounts.

The default setting for this policy is Yes.

Notes

- If this policy is set to No and you use the Maximum password age policy to set an expiration date for the password, users will not be able to reset their password. Instead, an administrator will have to reset the password for them.

- This policy effects the display of the Change Password option on the user portal Account page only. Separately, you can set a policy that enables users to reset their password from the user portal login prompt (for example, if they have forgotten their password). See “Configure password reset self-service options” on page 44.

To prevent users from changing their password:

1. Open Admin Portal and click Policies, and select a policy set.


3. Click the drop-down list for Enable users to change their passwords and select No.

4. Click Save.
Configuring OATH OTP

You can enable users to use a third party authenticator application to authenticate to the Samsung SDS IAM & EMM Identity Service. When you enable this policy, users will have the following option:

- Use a third party authenticators to scan a Samsung SDS IAM & EMM generated QR code. The third party authenticator will then return a one-time-passcode (OTP) for users to log in to the user portal. You can direct users to Using a third party authenticator application.

- Use the one-time passcode that was generated when the system administrator uploaded existing OATH tokens. See “Importing OATH tokens in bulk” on page 353.

To enable the third party OTP policy:

1. Log in to Admin Portal, click Policies, and select a policy set or create a new one.
2. Click User Security Policies, OATH OTP.
3. Select Yes in the Allow OATH OTP Integration drop down.
4. In the OATH OTP Display Name text box, enter text that reflects the name of the third party authenticator for which you are configuring.
   This text will be displayed on the Authentication Profiles page and in the user portal when users scan the QR code.
5. Click Save.
6. Click Settings and Authentication.
7. On the Authentication Profiles page, select the relevant authentication profile or add a new profile.
8. Enable the OATH OTP Client mechanism (name of the mechanism reflects the name you entered in the User Security Policies section) for either Challenge 1 or Challenge 2. See “Creating authentication profiles” on page 30 for more information on authentication profiles.
9. Click OK.
Configuring derived credentials

Smart cards contain cryptographic credentials that allow users to authenticate without usernames and passwords. However, the physical cards require a dedicated reader and attempting to use smart cards with mobile devices is a real challenge. With derived credentials, the cryptographic credential is stored securely on a mobile device, in compliance with current smart card regulations. This means no need for a dedicated reader for mobile devices, and much more flexibility for users. Our derived credential solution allows mobile devices to be used for secure mobile access to applications, websites and services that require smart card authentication. This new capability extends Samsung SDS IAM & EMM's integration of identity-based security to mobility, offering secure single sign-on (SSO) in even the most highly regulated environments.

You can configure derived credentials to use either Simple Certificate Enrollment Protocol (SCEP) with Microsoft's Network Device Enrollment Service (NDES) or Windows Enterprise certificate authority.

The following legend applies to both the Windows Enterprise certificate authority diagram and the SCEP diagram:

- CA -- Certificate Authority
- CSR -- Certificate Signing Request
- DC -- Derived Credential(s)
- OCSP -- Online Certificate Status Protocol

This diagram shows the workflow (for Windows Enterprise certificate authority) starting when the end users request the provisioning of the derived credentials to their mobile devices.
This diagram shows the workflow (for SCEP server) starting when the end users request the provisioning of the derived credentials to their mobile devices.
Prerequisites

Before you start configuring devices for derived credentials, confirm the following:

- You have set up smart card authentication with the Samsung SDS IAM & EMM identity platform. See “Setting up smart card authentication” on page 193.

- The Enable Knox container policy in Admin Portal > Policies > Mobile Device Policies > Samsung Knox Workspace Settings is set to false. It is set to false by default.

- Enrolled devices using device credentials must be iOS 8 and newer or Android 6.0 and newer.
High level configuration procedure

At a high level, the systems administrator must do the following to set up and configure derived credentials:

1. Windows Enterprise CA -- Creating templates or SCEP using NDES -- Creating user template & editing registry
2. Windows Enterprise CA -- Creating the derived credentials or SCEP using NDES -- Creating the derived credentials
3. “Enabling the derived credential policy” on page 219
4. “Enabling applications for derived credentials” on page 219

Windows Enterprise CA -- Creating templates

Samsung SDS IAM & EMM identity service integrates with Enterprise Windows Certification Authority (CA) for provisioning derived credentials to enrolled mobile devices. To enable provisioning of derived credentials, you must configure additional parameters on Windows CA.

Issuing derived credentials require mobile devices to send the Certificate Signing Request (CSR) after they generate a key pair. The private key never leaves the devices and is securely stored in a trusted area of the device. The systems administrator must configure the following CSR generation parameters:

- Certificate key size
- Asymmetric certificate key
- Hashing algorithm

To submit a CSR and get a signed CSR response from Windows Enterprise Certificate Authority, the systems administrator must create and configure a derived credential certificate template and specify the template name in the Samsung SDS IAM & EMM identity service.

For security purposes, we recommend that you delegate the capability of submitting CSR for derived credentials to only a few users or machine principals. The standard delegation method is to use Certificate Request Agent, which enables "enroll on behalf of" capability for users of devices. When issuing a derived credential, the Samsung SDS IAM & EMM connector requests an enrollment agent certificate, signs the CSR sent by the device, and submits this to Windows CA. Systems administrators must create and configure certificate agent template for the connector to request an enrollment agent certificate.

On a Windows Certificate Authority machine, do the following:

1. “(Optional) Granting Samsung SDS IAM & EMM connector permissions to revoke certificates” on page 206
2. “Setting up a template for enrollment agent” on page 206
(Optional) Granting Samsung SDS IAM & EMM connector permissions to revoke certificates

If you want users to have the ability to revoke the derived credential certificates, you must grant the appropriate permissions on the Samsung SDS IAM & EMM connector(s).

To grant Samsung SDS IAM & EMM connector permissions to revoke certificates:

1. Log in to a Windows Certificate Authority machine and navigate to the elevated command prompt.

2. Type certsrv.msc to open Certificate Authority.

3. Grant the user or machine account that runs the connector permission to manage certificates.

   If this permission is not granted, users cannot revoke certificates. In production environments, the connector runs as local system account and you should add the machine account on which the connector runs. In multi connector environments, you must add all connector machine names.

4. Click OK.

Setting up a template for enrollment agent

When issuing a derived credential, the Samsung SDS IAM & EMM connector requests an enrollment agent certificate, signs the CSR sent by the device, and submits this to Windows Certificate Authority (CA). Systems administrators must create and configure a certificate agent template for the connector to request an enrollment agent certificate.

To set up a template for enrollment agent:
1 Log in to a Windows Certificate Authority machine and navigate to the elevated command prompt.

2 Type `certtmpl.msc` to manage certificate templates that are available for the CA.

3 Duplicate the Enrollment Agent (Computer) certificate template and provide a name, for example "DerivedCreds_Enrollment_Agent_Computers".

The enrollment agent signs the PKCS10 request submitted by the device or Samsung service and creates a PKCS7 message.

**Note** If the connector service resides under a user account, select "Enrollment Agent" and use the user account instead of local system account.

4 Click **Properties** in the duplicated enrollment agent template and configure the following:
   a. Select **Allow private key to be exported** on the Request handling tab.
   b. Set the minimum key size to 2048 on the Cryptography tab
   c. Select **Build from this Active Directory information** on the Subject Name tab and enable DNS name to be included in the alternate subject name.
   d. Grant the account that runs the Samsung SDS IAM & EMM connector with **Enroll** and **Read** permissions on the Security tab.

5 Click **Apply > OK**.
**Setting up a template for issuing derived credentials**

To submit a Certificate Signing Request (CSR) and get a signed CSR response from Windows Enterprise Certificate Authority, you must create and configure a derived credential certificate template and add it to the Samsung SDS IAM & EMM identity service.

To create and configure a derived credential certificate template:

1. Log in to a Windows Certificate Authority machine and navigate to the elevated command prompt.
2. Duplicate the User template and name it, for example "DerivedCreds_UserCert_Template".
3. Click **Properties** on the duplicated user template and configure the following:
   - **On the Request Handling tab:**
     - Select **Signature and encryption** as the purpose.
     - Select **Allow Private key to be exported** only if you are testing this feature.
     - Select **Enroll subject without requiring any user input**.
   - **On the Cryptography tab**, specify minimum key size as 2048 bits.
   - **On the Subject Name tab:**
     - Select **Build from this Active Directory information**.
     - Select **Fully distinguished name** as subject name format.
     - Select **User principal name (UPN)** to be included as part of subject alternate name.
   - **On the Issuance Requirements tab:**
     - Select **This number of authorized signatures** and specify a value of 1.
     - Select **Application Policy** in the **Policy type required in signature** drop-down.
     - Select **Certificate Request Agent** in the **Application Policy** drop-down.
d Select **Same criteria as for enrollment** in the re-enrollment area.

On the Security tab, grant **Enroll** and **Read** rights to the account running the connector.

4 Click **Apply > Save**.

5 Type **certsrv.msc** on the elevated command prompt.
6 Click Certificate Templates and add a new Certificate Template to issue.

SCEP using NDES -- Creating user template & editing registry

You configure the SCEP derived credential template on the Windows Certificate Authority machine for the following reasons:

- Submit a Certificate Signing Request (CSR) to the Microsoft Enterprise Certificate Authority.
- Get a signed CSR from Microsoft Enterprise Certificate Authority.

To configure a SCEP derived credential template:

1 Log in to your Windows Certificate Authority machine.
2 Click Certificate Authority MMC.
3 Click the Certificate Authority on the right.
4 Right click the Templates folder and select Manage.
   The Template Management folder opens.
5 Right click the "User" template and select Duplicate Template.
6 Specify the template name and display name as "DerivedCreds_Scep_User".
7 Click Properties on the duplicated user template and configure the following:
Compatibility tab:
- Select **Windows Server 2012 R2** for the Certificate Authority.
- Select **Windows 8.1/Windows Server 2012 R2** for the certificate recipient.

Request Handling tab:
- Select **Signature and encryption** for the purpose.
- Select **Include symmetric algorithms allowed by subject**.
- Select **Allow private key to be exported**.
- Select **Enroll subject without requiring user input**.

Cryptography tab:
- Select **Key Storage Provider** for the Provider category.
- Select **ECDH_P256** for the Algorithm name if you are using the ECC certificate key and **RSA** if you are using the RSA key.
- Enter 256 for the Minimum key size if you are using the ECC certificate key and 2048 if you are using the RSA key.
- Select **Requests can use any provider available for the subject's computer**.
e  Select **SHA 256** (the CSR hash algorithm and CSR signing hash that is performed by CA) for the Request hash.

Security tab:

a  Grant the domain user **Read** and **Enroll** permissions.

In this example, the user created in the domain controller is called “ndessvc” in this configuration example.

These permissions allow the NDES web service to interact with the CA to submit the CSR on behalf of the Samsung SDS IAM & EMM connector.

b  Grant the Samsung SDS IAM & EMM connector **Read** and **Enroll** permissions.

If the connector runs a network or local system account, then use machine name as the identity. These permissions are required to request enrollment password from the SCEP server.

c  (Optional) You can add user accounts if you are testing the configuration.
Subject Name tab:

a. Select **Supply in the request**.

b. Enable the **Use subject information from existing certificates for auto enrollment renew requests** field.

Issuance Requirements tab:

c. Select the **CA certificate manager approval** field for manual approval. Unselect this field if you are using auto approvals.

d. For reenrollment, select **Valid existing certificate** and enable **Allow key based renewal**.
Publish the user template (the one you duplicated and likely named "DerivedCreds_Scep_User") to the Certificate Authority (CA).

**Editing the SCEP registry**

You edit the registry to submit enrollment requests based on duplicated user template.

To edit the registry:

1. Log in to the computer hosting NDES.
2. Open regedit and navigate to HKLM\Software\Microsoft\Cryptography\MSECP.
3. Set the following to "DerivedCreds_Scep_User" (the duplicated user template name you created on the Windows Certificate Authority machine):
   - Encryption Template
   - Signature Template
   - General Purpose Template

**Restarting IIS and verifying access**

You restart IIS to ensure all previous configurations are captured.

You verify access to confirm that the Samsung SDS IAM & EMM connector can pull the necessary password form the SCEP server.
To verify access:

1. Log in to the Samsung SDS IAM & EMM connector in the domain.

2. Open a browser window and go to your SCEP server using a URL that follows this format:
   \[http://<ndes_server.your.domain>/certsrv/mscep\]
   
   For example: \[http://dc.anil.com/certsrv/mscep\]
   
   You see a page similar to the following.

3. Click the link to get the enrollment password or go to the password URL directly.
   
   Enrollment password is displayed if all settings are correctly configured and you have the correct permissions on the SCEP derived credential template.

---

**Windows Enterprise CA -- Creating the derived credentials**

Enrolled devices must have the signed derived credentials stored on them to access protected websites and applications. You specify the certificate signing request parameters and the Microsoft Windows Certificate Authority template for Samsung SDS IAM & EMM.
to communicate with the Issuing Certificate Authority (CA) and create the signed derived credentials.

To create the derived credentials:

1. Log in to Admin Portal.
2. Click **Settings > Authentication > Derived Credentials**.
3. Specify the certificate key type (RSA or ECC).

   ECC (Elliptic Curve Cryptography) keys are stored in the secure enclave (hardware key store) on iOS 10+ devices.

   **Important:** If you use the ECC key, you must select **ECDH_P256** as the algorithm name on the Cryptography tab when creating the user template. See “SCEP using NDES -- Creating user template & editing registry” on page 210.

4. Specify the public/private key size for the derived credential certificate in the **Certificate Key Size** drop-down.

   ECC certificate keys only support the 256 key size.

5. Select the **Windows Enterprise CA** radio button.

6. Specify the CA endpoint to submit the derived credential certificate signing request in the Certificate Authority Endpoint field.

   If you do not specify this endpoint information, the default CA configuration will be used.

7. Specify the template name for the connector in the **Derived Credential Template Name** field.
This template is created on the Certificate Authority and defines the parameter for the derived credential. See “Setting up a template for issuing derived credentials” on page 208.

8 Specify the template name for the connector to request the derived credential certificates on behalf of the enrolling users in the **Enrollment Agent Certificate Template Name** field.

This template is created on the Certificate Authority. See “Setting up a template for enrollment agent” on page 206.

9 Click **Verify** to validate the template configuration.

10 Click **Save**.

**SCEP using NDES -- Creating the derived credentials**

Enrolled devices must have the signed derived credentials stored on them to access protected websites and applications. You specify the certificate signing request parameters and the certificate authority details to create the signed derived credentials.

To create the derived credentials:

1 Log in to Admin Portal.

2 Click **Settings > Authentication > Derived Credentials**.

3 Specify the certificate key type (RSA or ECC).

   ECC (Elliptic Curve Cryptography) keys are stored in the secure enclave (hardware key store) on iOS 10+ devices.

   **Important:** If you use the ECC key, you must select **ECDH_P256** as the algorithm name on the Cryptography tab when creating the user template. See “SCEP using NDES -- Creating user template & editing registry” on page 210.

4 Specify the public/private key size for the derived credential certificate in the **Certificate Key Size** drop-down.

   ECC certificate keys only support the 256 key size.

5 Select the **SCEP Server** radio button.
6 Enter the URL of the SCEP server.

7 Select the **Require Enrollment Password** check box.

   Additional enrollment password options are displayed. SCEP protocol provides enrollment password options. Different CAs implement enrollment passwords differently.

8 Select either:
   * Same Passwords for All Enrollments -- All enrollments will use the same shared secret.
     Enter the password and click **Save**. You are done.
   * New Passwords for Every Enrollment -- A different password is used for each enrollment. Only Microsoft NDES implementation is supported.
     Continue with this procedure.

9 Enter the enrollment password URL.

   You get this enrollment password URL from the SCEP server. It is the same password URL you used to verify access to the connector.

10 Specify the enrollment password expiration time in minutes.

11 Select one of the following for enrollment password URL authentication:
   * Windows Authentication (Kerberos) -- Samsung SDS IAM & EMM uses the domain credentials to allow access to the enrollment password.
   * Basic Authentication -- Enter the username and password you want Samsung SDS IAM & EMM to use for access to the enrollment password.
12 Click Save.

**Enabling the derived credential policy**

Before derived credentials can be issued to enrolled devices, you must enable this policy. To enable the derived credential policy:

1. Log in to Admin Portal.
2. Click **Polices** and select an existing policy or create a new one.
3. Click **Mobile Device Polices > Device Management Settings**.
4. Select **Yes** in the Enable Derived Credentials Issuance drop-down.
5. Click **Save**.

**Enabling applications for derived credentials**

You must enable derived credentials for all web applications where smart card login is required. Derived credentials support only web applications. All derive credential enabled applications will be opened on mobile devices using the Samsung SDS IAM & EMM built-in browser.

If you have already deployed an application and now you want to enable it for derived credentials, do the following:

1. Log in to Admin Portal.
2. Click **Apps** and select the relevant application.
3. Select the **Enable Derived Credentials for this app on enrolled devices** checkbox.
4. Click **Save**.

If you need to configure and deploy an application, see [Adding web applications](#).
Managing Application policies

You use the application policies to configure application related policies. The available policies are:

- Allow users to add personal apps
  
  By default, users can add web applications from the Samsung SDS IAM & EMM App Catalog to their user portal and devices. You use this policy to prevent them from adding applications from the user portal and using Infinite Apps.

  Applications that were added by the user before the policy was changed are blocked. The icons are still displayed on the Apps screen and on their devices, however, an error message is displayed when the user tries to open the application.

  If you assigned any web applications for optional installation (see “Configuring automatic versus optional deployment” on page 121), the applications are listed when the user clicks the Add Apps button on the user portal. However, no applications from the application catalog are listed.

- Allow users to view/copy personal passwords
  
  By default, users can view and copy their encrypted applications passwords from the user portal and devices. You use this policy to disable that ability.
Managing device configuration policies

When you use the Samsung directory for mobile device management, the Samsung service provides mobile device configuration policies you can set by using either the Admin Portal or, if you have a Samsung SDS IAM & EMM license, the Active Directory Group Policy Management Editor. See “List of device configuration policies” on page 376 for a full list of the mobile device policies available for Android, iOS, and Samsung Knox devices.

Users can see the policies enabled on their Android devices on Setup tab in the Samsung SDS IAM & EMM client and on their iOS devices in the Settings application’s General/Profiles screen.

This section contains the following topics:

- “Selecting the policy management tool” on page 221
- “Using Admin Portal to set device configuration policies” on page 222
- “Using the Group Policy Management Editor to set mobile device policies” on page 223
- “Reconciling policy settings in hierarchical policy sets and group policy objects” on page 225

Selecting the policy management tool

You select which tool you are going to use to manage group policies—Admin Portal or the Active Directory Group Policy Management Editor—by using the Admin Portal Device Policy Management setting (see “Selecting the policy service for device policy management” on page 345). You must select one method or the other.

**Note** You can switch from one tool to the other.

How you set the policies depends upon which option you select for device policy management (see “Selecting the policy service for device policy management” on page 345):

- **If you select Samsung SDS IAM & EMM policy service:** You set policies by creating and editing a policy set. Policy sets are managed from the Policies page in Admin Portal. Go to “Using Admin Portal to set device configuration policies” on page 222 to continue with managing mobile policies with Admin Portal.

- **If you select Active Directory group policy:** You need to install the Samsung SDS IAM & EMM connector and select the group policy console extension (see “Samsung SDS IAM & EMM connectors and administrator consoles” on page 355). Then go to “Using the Group Policy Management Editor to set mobile device policies” on page 223 to continue with setting the policies.

Do not select Active Directory group policy if you do not have a Samsung SDS IAM & EMM License.
Using Admin Portal to set device configuration policies

You use device configuration policies to configure the settings in Android devices and profiles in iOS devices when the user enrolls the device. To set device configuration policies when you use the Samsung SDS IAM & EMM policy service for device policy management, you create a new policy set or modify an existing policy set and then apply the policy set to a role (see How to create a policy set and assign it to users). The Samsung service then installs the policy set in the devices enrolled by the users belonging to the role. You can mix different types of devices in the same policy set.

The Samsung service installs the policies initially when the user enrolls the device. The policies are updated when the push delay period expires (see “Selecting the policy service for device policy management” on page 345 to set the period) or you can force an update after you make a change with a Admin Portal command (see “Using the device management commands” on page 165) to push the update immediately.

The Samsung service automatically updates the devices when you make changes too. You can set how long it waits after you finish editing the policy in the when you select the Samsung SDS IAM & EMM policy service for Device Policy Management (see “Selecting the policy service for device policy management” on page 345).

Click the drop-down list to enable or disable the policy. Click the information bubble for the configuration options.

The drop down menu provides the following options:

- **-- (Not configured)**: Select to keep the default value.
  
  This is the default for all policies. The setting set by the device vendor remains in effect. Users can change this setting using the device’s Settings screen if your device policies allow them to modify settings.

  **Note** The default setting can vary from one vendor to another.

  If the same policy is set in a policy set higher up on the Policies page, the previous setting is applied. See “Reconciling policy settings in hierarchical policy sets and group policy objects” on page 225 for the details.

- **Yes**: Select to enable the feature or service.
  
  When you set the policy to “Yes,” it allows the user to use that feature or service. For example, if you set the “Permit camera use” policy in Common Mobile Settings to “Yes,” the user is allowed to take pictures with the device’s camera.

- **No**: Select to disable the feature or service.
  
  When you set the policy to “No,” the user is denied use of the feature or service. For example, if you set the “Permit camera use” policy to “No,” the user is not allowed to take pictures with the device’s camera.

Some policies require additional configuration after you enable them. For example, after you enable a Wi-Fi policy, you have to specify the SSID, password, and other
communication properties. For these policies, Admin Portal displays an Add button and lets you create one or more profiles for that policy. Admin Portal lists the profiles so you can manage them.

Using the Group Policy Management Editor to set mobile device policies

You use device configuration policies to configure the settings in Android devices and profiles in iOS devices when the user enrolls the device. To set device configuration policies when you use Active Directory group policy for device policy management, you create a new or modify an existing group policy object (GPO) by using the Group Policy Management Editor and then link the GPO to an Active Directory organizational unit.

You then specify the organizational unit in the Device Enrollment Settings (see “Enabling users to enroll devices” on page 22. You can specify different policies for different roles by creating a separate GPO and linking it to a different organizational unit for each role—see “Configuring group policy objects and organizational units” on page 348.

Note If you select Active Directory to set mobile device policies, the Samsung service does not install the group policy object settings in devices that are enrolled by users with Samsung SDS IAM & EMM directory accounts. If you have some users with Active Directory accounts and others with Samsung SDS IAM & EMM directory accounts, select the Samsung SDS IAM & EMM policy service to define mobile device policies.

The Samsung service installs the policies initially when the user enrolls the device. After that, the connector polls Active Directory for changes to the group policy object on a periodic basis. If it finds a change it updates the devices. You set the update interval when you configure the Device Policy Management (see “Selecting the policy service for device policy management” on page 345).

It can take up to 10 minutes after polling for the connector to install the new profiles on all affected devices. However, if you make a lot of policy changes (for example, more than 20) the connector might issue the profile updates in multiple batches rather than all at once.

Alternatively, you can force an update after you make a change with a Admin Portal command (see “Using the device management commands” on page 165) to push the update immediately.

Enabling policies in the Windows Group Policy Management Editor

The Samsung service mobile device policies are listed alongside the Windows group policies in the Group Policy Management Editor. You can mix different types of devices (for example, Android and iOS devices) in the same group policy object.

You open the group policy object for editing and then expand the Samsung SDS IAM & EMM Management Settings categories to expose the individual policies. Double-click the policy to enable and configure it. Click the Explain tab for the configuration instructions.
By default all mobile device policies are set to “Policy not configured.” Alternatively, a policy can be set to “Policy enabled” or “Policy disabled.” These settings are defined as follows:

- **Policy not configured**: Select this to leave the device in its default setting. This is the default for all policies. The setting set by the device vendor remains in effect. Users can change this setting using the device’s Settings screen if your device policies allow them to modify settings.

  **Note**  The default setting can vary from one vendor to another.

  If the same policy is set in a parent group policy object or group policy object linked to a parent domain, the policy set in the parent is applied. See “Reconciling policy settings in hierarchical policy sets and group policy objects” on page 225 for the details.

- **Policy enabled**: Select this to set the policy. “Policy enabled” has different options, depending upon the policy. For many policies, it means that you are “turning on” this feature and setting associated values or properties. For example, you enable passcode history so that the device saves the passcodes over time and then configure how many passcodes you want to save. Or, you enable a virtual private network (VPN) policy and specify the server and VPN type.

  For other policies, you enable the policy and set it to “True” or “False.”

  - **True**: This means that you are going to impose the policy and you are going to allow it. For example, you enable Bluetooth access policy to say “I am setting this policy” and then set it to “True” to allow the user to have Bluetooth access.

  - **False**: This means that you are going to impose this policy and you are not going to allow it. For example, you enable Bluetooth access policy to say “I am setting this policy” and then set it to “False” to stop the user from using Bluetooth.

- **Policy disabled**: Select this to defer setting this policy. When you set the policy to this state, the device reverts to its default setting, regardless of the settings set by the user or a parent group policy object. The default setting can be different for different device vendors.

To enable a mobile device policy setting in the Group Policy Management Editor:

1. Open the Windows Group Policy Management administrative tool.
2. Right-click the group policy object and select **Edit** to open the Group Policy Management Editor.

   Alternatively, you can create a new group policy object by right-clicking the domain and selecting **Create a GPO in this domain, and Link it here**.
3. Expand **Samsung SDS IAM & EMM Management Settings**.
4. Double-click a group policy to open the Properties window.
Use the **Policy** tab to enable the policy. Click the **Explain** tab for an explanation of the policy and its options.

5 Click **Policy enabled**.

6 Select the options you want and enter or select the required values.

7 Click **OK** or **Apply** to save the setting.

**Reconciling policy settings in hierarchical policy sets and group policy objects**

You can create hierarchical policy sets and group policy objects to apply different mobile device policies to different sets of users. For example, if you are using the Samsung SDS IAM & EMM policy service, you can create multiple policy sets and then arrange them from bottom to top to set base and then role-specific policies (see “Using hierarchical policy sets” on page 187), respectively. If you are using Active Directory, you can use the Default Domain Policy and then create separate GPOs to link to different organizational units.

**Using the Samsung SDS IAM & EMM policy service**

If you are using the Samsung SDS IAM & EMM policy service, the policy options are “Yes,” “No,” and “--” (not configured). If the policy is set to not configured, the device-default is used.

When you set the same policy differently in multiple policy sets, the setting in the higher policy sets on the Policies page replaces the setting in a lower policy set. The following table lists the policy setting from the lower policy set in the rows and the policy setting from the upper policy set in the columns and the setting that results on the device in the individual cell.

<table>
<thead>
<tr>
<th>Lower policy set</th>
<th>Yes</th>
<th>No</th>
<th>--</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>--</td>
<td>Yes</td>
<td>No</td>
<td>--</td>
</tr>
</tbody>
</table>

Notice that the upper policy set supersedes the lower except when the upper is set to “not configured.” In this case, the lower setting is applied.

**Using Active Directory**

If you are using Active Directory, the policy options are “Policy not configured,” “Policy enabled,” and “Policy disabled.” Active Directory settings are different from the Samsung SDS IAM & EMM policy service policy options because the “Policy enabled” setting is used to both allow and deny use of the feature or service and “Policy disabled” means “revert to the device default.”
The following table lists the policy setting from the parent GPO in the columns and the policy setting from the child set in the rows and the applied setting in the individual cell.

<table>
<thead>
<tr>
<th>Child GPO Setting</th>
<th>Parent GPO Setting</th>
<th>Policy enabled</th>
<th>Policy disabled</th>
<th>Policy not configured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy enabled</td>
<td>Policy enabled*</td>
<td>Policy enabled</td>
<td>Policy enabled</td>
<td>Policy enabled</td>
</tr>
<tr>
<td>Policy disabled</td>
<td>Policy disabled</td>
<td>Policy disabled</td>
<td>Policy disabled</td>
<td>Policy disabled</td>
</tr>
<tr>
<td>Policy not configured</td>
<td>Policy enabled</td>
<td>Policy disabled</td>
<td>Policy disabled</td>
<td>Policy not configured</td>
</tr>
</tbody>
</table>

* The applied setting in this cell can be misleading. Although the policy is enabled in both cases, if the parent GPO policy is set to “True” and the child GPO policy is set to “False,” the setting applied is “False.” If you wanted to keep the setting set in the parent, you would set the child to “Policy not configured.” (Setting to “Policy disabled” restores the default setting.) This is the only cell in which the state can be misleading.
Mobile device configuration policies overview

The Samsung service provides a comprehensive range of policies for managing the security, features, and behavior of mobile devices.

This section contains the following topics:

- “Using the Common Mobile Settings” on page 228
- “Using iOS settings” on page 229
- “Using the Samsung KNOX Device Settings” on page 231
- “Using the Samsung KNOX Workspace Settings” on page 235
- “Using Touchdown settings” on page 239
- “Configuring Exchange profiles” on page 239
- “Configuring VPN profiles” on page 243
- “Configuring Wi-Fi profiles” on page 246

Notes

- Although policies are listed in the Active Directory Group Policy Management Editor and Samsung SDS IAM & EMM policy service, their availability is determined by the licenses you have purchased. See “Understanding licensing” on page 377 for the details.

- If you do not see the Samsung SDS IAM & EMM Management Settings when you open the Group Policy Management Editor, you need to install the Group Policy Console Extension on your computer. See “Installing a Samsung SDS IAM & EMM connector” on page 53 for the instructions.

- Not all policies are supported in both the Group Policy Management Editor and the Samsung SDS IAM & EMM policy service. The policy summaries in “List of device configuration policies” on page 376 indicate whether each policy is available in one or both tools.
Using the Common Mobile Settings

Common Mobile Settings contains mobile device policies and two branches—Passcode Settings and Restrictions Settings—with additional policies. See “Common Mobile Settings” on page 378 for the full list of policies.

<table>
<thead>
<tr>
<th>Policies and branches</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>You can set the following policies:</td>
</tr>
<tr>
<td></td>
<td>• Enable debug logging. Turns on the debug logging mode (the default is regular logging mode). When you set this policy, Enable Debug Logging in the device’s Setting page is set.</td>
</tr>
<tr>
<td></td>
<td>• Encrypt internal onboard storage. Automatically encrypt the storage area on Android devices.</td>
</tr>
</tbody>
</table>
|                       | Note: This policy is not supported on Samsung Knox devices.
| Restrictions Settings | Set rules governing the use of device features—for example, you can control the following:  |
|                       | • whether or not the user can use the camera  |
|                       | • whether or not the user can wipe device  |
|                       | • whether or not the user can unenroll the device  |
|                       | • Whether or not the device reports the device location  |
Using iOS settings

iOS Settings contains the policy you use to configure Exchange Sync communications on the device and a set of restrictions settings. See “iOS Settings” on page 380 for the full list of restriction settings.
In addition, you can configure the device to run in kiosk mode. In this mode, the device runs a single application and lets you control the device’s operating features while that application is running.

<table>
<thead>
<tr>
<th>Policy</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Sync Settings</td>
<td>Configure the Exchange Sync profile for the iOS devices. For example, define the Exchange Sync server name and an attribute variable for the user name.</td>
</tr>
<tr>
<td>Restrictions Settings</td>
<td>Set rules governing the use of device features—for example, permitting or prohibiting Safari, YouTube, and Photos Stream use and setting requirements for encrypted backups and an iTunes Store password.</td>
</tr>
<tr>
<td>Domain Settings</td>
<td>Specify domains so that files downloaded from these domains using Safari must be opened using managed applications. This policy requires the “Permit opening managed app documents in unmanaged apps” and “Permit opening unmanaged app documents in managed apps” settings in iOS Settings, Restrictions to be set to “No”. See “Configuring data access by domains for Safari” on page 231. Specify domains so that email addresses that do not match these domains will be highlighted in the user’s email software.</td>
</tr>
</tbody>
</table>
| Kiosk Mode              | Put the device in single application mode and designate the home launcher. Use the “Enable kiosk mode” policy to allow just a single application to run on the device and specify the application that will be the home launcher. You can use the other policies in this category to manage the user interface while the application is running. Only home launcher applications can be used in kiosk mode. After the application is installed, the device automatically opens to kiosk mode. You can specify the Samsung SDS IAM & EMM client by selecting “Use MDM client as kiosk mode application.” When you select the Samsung SDS IAM & EMM client, it behaves a little differently than in when it’s launched from the home screen:  
  • There is no Authentication tab.  
  • All web applications open in the Samsung SDS IAM & EMM client built in browser only.  
  • In the Settings tab, the Show Authenticator, Default Browser, and Unenroll Mobile Device options are hidden. |
| Global HTTP Proxy       | Filter HTTP traffic on iOS devices by defining the proxy server that the device can access. You can manually enter the proxy server information or enter the URL for the proxy settings. This policy only applies to supervised devices. |
| Per app VPN settings    | Map a mobile application to a specific VPN connection. See “Configuring VPNs in iOS devices” on page 244 for more details. |
Configuring data access by domains for Safari

You can specify that files downloaded from specific domains using Safari must be opened using managed applications.

To configure managed application data access by domains for Safari:

1. Log in to the Admin portal.
2. Click **Policies** and select an existing relevant policy or create a new one.
3. Click **Mobile Device Policies, iOS Settings, Domain Settings, Add** button associated with the Managed Safari Web Domains section.
4. Enter the relevant domains.
5. Click **Save** on the add domain window and again on the domain settings window.
6. Click Restrictions Settings.
7. Select No for the “Permit opening managed app documents in unmanaged apps” and “Permit opening unmanaged app documents in managed apps” settings.
8. Click **Save**.

**Note:** On non-Safari browsers, how documents/data are handled by managed and unmanaged applications depend upon how the browsers were installed (as managed or unmanaged applications) and how you have configured the “Permit opening managed app documents in unmanaged apps” and “Permit opening unmanaged app documents in managed apps” settings.

Using the Samsung Knox Device Settings

You use the policies in this category to configure VPN, Wi-Fi, and Exchange Sync communications and a wide variety of other controls for Samsung Knox devices. These policies are applied to the device when the user is outside the Knox container only.
The Samsung Knox Device policies have been introduced over time with each new version of the Samsung Knox device’s mobile device management (MDM) software. The MDM version required for the policy is shown in each policy’s configuration instructions and in the tables in “Samsung KNOX Device Settings” on page 385.

All of the policies in the Samsung Knox Device Settings can be applied to Samsung Knox version 1 and version 2 devices.

<table>
<thead>
<tr>
<th>Policies</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Sync Settings</td>
<td>Configure the Exchange Sync profiles for server communications and account synchronization for the email application running outside the Knox container.  &lt;br&gt;<strong>Note:</strong> You define the Exchange ActviceSync profile for server communications and account synchronization for the email application running inside the container separately in the Samsung Knox Workspace Settings.</td>
</tr>
<tr>
<td>VPN settings</td>
<td>Configure VPN connection profiles for Samsung Knox devices and applications running outside of the Knox container.  &lt;br&gt;<strong>Note:</strong> You define the VPN profiles for the Knox container and applications running inside the container separately in the Samsung Knox Workspace Settings.</td>
</tr>
<tr>
<td>APN Settings</td>
<td>Create Access Point Name profiles.  &lt;br&gt;You can create multiple access point profiles. All of the profiles are downloaded to the device, however, the only profile that appears in the configuration is the profile in which the MCC and MNC in the profile match the MCC and MNC in the SIM.</td>
</tr>
<tr>
<td>Wi-Fi Settings</td>
<td>Configure Wi-Fi connection profiles for Samsung Knox devices.</td>
</tr>
</tbody>
</table>
### Mobile device configuration policies overview

**Chapter 20 • Managing policies**

<table>
<thead>
<tr>
<th>Policies</th>
<th>To do this</th>
</tr>
</thead>
</table>
| Kiosk mode               | Set the device to single application mode  
Use the “Enable kiosk mode” policy to allow just a single application to run and specify the application. You can use the other kiosk policies to permit multiple windows, navigation and status bar visibility, and task manager access when the device is in kiosk mode.
**Important:** To use kiosk mode, make sure that you do not have the “Prevent installation of applications” policy enabled on the Application Management page.
After the application is installed, the device automatically opens to kiosk mode.
You can use either the native Android home screen, a custom application, or the Samsung SDS IAM & EMM client as the home launcher when the device is turned on. When you select the Samsung SDS IAM & EMM client, it behaves a little differently in kiosk mode:
  * There is no Authentication tab.
  * All web applications open in the Samsung SDS IAM & EMM client built in browser only.
  * In the Settings tab, the Always Show Authenticator, Default Browser, and Unenroll this device options are hidden.
  * Application statuses, such as Install and Update, are not displayed when a device is in kiosk mode.
When you select the Samsung SDS IAM & EMM client, the default is to automatically update the software when there is a change. The update is performed on the device at the time you select. If you disable, updating the software is the same procedure as though you were changing the home launcher—see “Changing home launchers” on page 234 for the details. |
| IMAP and POP Settings     | Create IMAP or POP profiles for the native email application installed in personal mode.                                                                                                                                                        |

<table>
<thead>
<tr>
<th>Policy branches</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Management</td>
<td>Define a variety of application usage restrictions, including applications the user can or cannot install, launch, or stop; application permissions; and applications whitelist and blacklist.</td>
</tr>
<tr>
<td>Bluetooth Settings</td>
<td>Configure a device’s Bluetooth interface</td>
</tr>
<tr>
<td>Device Inventory Settings</td>
<td>Enable or disable the device’s logs (for example, call information, Wi-Fi network data bytes, and data network usage).</td>
</tr>
<tr>
<td>Firewall Settings</td>
<td>Configure URL filtering and iptable allow and deny rules.</td>
</tr>
</tbody>
</table>

**Policies to do this**

- Kiosk mode
- IMAP and POP Settings
- Policy branches
- Application Management
- Bluetooth Settings
- Device Inventory Settings
- Firewall Settings
### Policy branches

<table>
<thead>
<tr>
<th>Policy branches</th>
<th>To do this</th>
</tr>
</thead>
</table>
| Passcode Settings   | Set the rules governing password use in Samsung Knox devices—for example, forbidden strings, password pattern enforcement, and minimum number of changed characters in a new password. This category also includes policies that manage other password-related behaviors including password and screen-lock visibility and wiping external storage in the event the user fails to enter the correct password. There are several passcode policies labelled as Advanced. In the Group Policy Management Editor they are listed in a separate category and in the Samsung SDS IAM & EMM policy service they are called out in the bubble text. Changing the settings in these policies will require all users affected by this policy to change their password regardless of whether their current password meets the new criteria. \* Notes:\*  
  • The Samsung default requirements set in the device may be stronger than the values you set in the mobile device policies. If you set a value that is weaker, the stronger policy is enforced.  
  • You set the rules governing the container passcode in a separate policy—see the Samsung Knox Workspace Container Passcode settings. |
| Restrictions Settings | Set rules governing the use of device features. There’s a long list of policies available to enable or disable such features as varied as Bluetooth access, Android and S Beam use, audio recording, and home-key functionality. \* Note:\* You enable or disable Wi-Fi and VPN using the policies in this policy category. However, you define the Wi-Fi and VPN profiles in separate nodes. |
| Roaming Settings    | Enable or disable operation of the device in roaming mode. |
| Security Settings   | Enable or disable enrollment with an MDM server, enable a SIM card lock, and encrypt or not encrypt the external storage. |
| VPN Restrictions    | Configure to allow only IPsec or SSL/TLS VPN connections. |
| Wi-Fi Restrictions  | Configure a wide variety of Wi-Fi network access point properties and user privileges. |

### Changing home launchers

When you change the home launcher settings for Samsung devices, the device will not display the newly selected launcher until the device has been reset to use the default TouchWiz launcher.

To change the home launcher:

1. On the Kiosk Mode page, select No in the Enable Kiosk Mode dropdown. This selection will allow the device to prompt for selection of the default TouchWiz launcher.
2. Click Save and push the policy to the devices.
3 Request the device user to select either of the two TouchWiz launcher options and Just Once on the device.

4 On the Kiosk Mode page, select Yes in the Enable Kiosk Mode dropdown then select the new launcher.

5 Click Save and push the policy to the devices.

The newly selected home launcher should now be available on the device.

**Using the Samsung Knox Workspace Settings**

The Samsung Knox Workspace Settings policies enable users to create a Samsung Knox enterprise container when they enroll their device and let you manage the policies settings that apply when users are in the container. For example, you can configure separate Exchange Sync, VPN, IMAP/POP email, firewall, and device restrictions settings for Samsung Knox containers.

The following tables summarize the policies in Samsung Knox Workspace Settings. See “List of device configuration policies” on page 376 for the full list.

See “Working with Samsung Knox devices” on page 173 for procedures that show you how to use a Knox Workspace Settings policy to enable users to create a Samsung Knox container and add a mobile application to the Applications SSO whitelist.

**Samsung Knox Workspace policies**

<table>
<thead>
<tr>
<th>Policy</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure applications that can sync with container</td>
<td>Synchronize data between the personal and Knox mode instances of the Contacts and S Planner (Calendar) applications.</td>
</tr>
<tr>
<td>Policy</td>
<td>To do this</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Enable Common Criteria mode                | Enable the following policies for Samsung Workspace devices only:  
  - Common Mobile Settings/Encrypt internal onboard storage  
    The user encrypts the internal onboard storage from the SETUP REQUIRED screen in Samsung SDS IAM & EMM client.  
  - Common Mobile Settings/Passcode Settings/Maximum number of failed attempts  
    The number of failed attempts is set to the value you set in the Enable Common Criteria mode policy for the Samsung devices only.  
  - Samsung Knox Device Settings/Security Settings/Encrypt removable storage  
    The user encrypts the removable storage from the SETUP REQUIRED screen in Samsung SDS IAM & EMM client.  
  In addition, when you set Enable Common Criteria mode, the Common Mobile Settings/Passcode Settings/Passcode History policy is disabled.  
  The policy settings are implemented on the devices only—they are not indicated in the Admin Portal policy set or the Active Directory group policy object. This allows you to have separate settings for these policies for other types of devices.  
  Common Criteria mode puts the target device in an operational mode that enforces the following security features and policies:  
    - Bootloader blocks KIES download mode, enforces an integrity check of the kernel, and self-tests the crypto modules.  
    - The device verifies additional signature on firmware-over-the-air (FOTA) updates using RSA-PSS signature and uses FIPS 140-2 validated crypto module for EAP-TLS wi-fi connections  
  This policy is only available on the following Knox 2 devices: Galaxy S4, Galaxy S5, Galaxy Note 3, Galaxy NotePro, Galaxy Note 10.1 and Galaxy Note 10.1 2014 Edition. |
| Enable Enterprise Billing                   | Enable separate bill generation for personal and enterprise data usage.  
  To enable enterprise billing, two different Access Point Names (APNs) are configured on the Knox device. Personal data is routed via the default APN and enterprise data is routed via the dedicated enterprise APN specified in the policy.  
  **Note:** This policy is only available for Knox 2.1 devices. |
| Enable Knox container                       | Enable the device to allow the user to create a Samsung Knox enterprise container after the device is enrolled.  
  See “Enabling the device to allow users to create an enterprise container” on page 176 for more details.  
  **Note:** On some Samsung devices, users can also create a Knox personal container. You do not need to set a policy to allow them to create the personal container. |
### Samsung Knox Workspace Container categories and policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>To do this</th>
</tr>
</thead>
</table>
| Enable ODE Trusted Boot        | Enable to consider attestation state before decrypting the data partition.  
Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current attestation status is shown in the device details in Admin Portal. |
| verification                  |                                                                                                                                                                                                          |
| Enable TIMA Key Store          | Enable to use the TIMA key store to store symmetric keys, RSA key pairs and certificates. The TIMA key store is implemented as a key store provider for the Java Keystore class. When this policy is enabled, it provides TrustZone-based secure storage and controls access based on the attestation state.  
Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current attestation status is shown in the device details in Admin Portal. |
| Require attestation verification| Enable to consider attestation state before allowing the user to create a Knox container.  
Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current attestation status is shown in the device details in Admin Portal. |
<p>| VPN Settings                   | Configure VPN profiles for Samsung Knox Workspace devices.                                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Categories</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Management</td>
<td>Define a variety of operating parameters for applications installed in the container. For example, policies are provided that let you set the following:</td>
</tr>
<tr>
<td></td>
<td>• Define which mobile applications are allowed to use the Knox container single sign-on service.</td>
</tr>
<tr>
<td></td>
<td>• Define which applications can be installed and added to the home screen.</td>
</tr>
<tr>
<td></td>
<td>• Define which applications can synchronize data with applications outside the container.</td>
</tr>
<tr>
<td></td>
<td>• Define which applications are disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you are installing any applications that use the Samsung Knox SSO service you must add them to the Application SSO whitelist policy in this category before users can open them. See “Adding mobile applications that use SSO to the Application SSO whitelist” on page 180 for the details.</td>
</tr>
<tr>
<td>Browser Settings</td>
<td>Control browser behavior—for example, enable or disable pop-up windows, cookies, and JavaScript</td>
</tr>
<tr>
<td>Container Account Settings</td>
<td>Create a whitelist and blacklist of user accounts to limit the types of accounts users can create in the Knox container.</td>
</tr>
<tr>
<td>Email Settings</td>
<td>Control email application behavior—for example, prohibit adding new accounts and forwarding email through a personal account.</td>
</tr>
<tr>
<td>Firewall Settings</td>
<td>Configure URL filtering and iptable allow and deny rules.</td>
</tr>
<tr>
<td>Passcode Settings</td>
<td>Configure rules governing passcode properties (for example, minimum length, character occurrence, number of complex characters, and sequence length), usage (for example, number of failed attempts, visibility, and history), and quality.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td></td>
<td>• The Minimum password length policy sets the minimum length for the password and the PIN.</td>
</tr>
<tr>
<td></td>
<td>• The “Require two factor authentication” policy is only available for devices that have a fingerprint reader and applies only to opening the container. (It does not apply to opening the device.)</td>
</tr>
<tr>
<td></td>
<td>• There are several more passcode policies in the Advanced category. Changing the settings in these policies will require all users affected by this policy to change their password regardless of whether their current password meets the new criteria.</td>
</tr>
<tr>
<td>Restriction Settings</td>
<td>Permit or prohibit use of container and device features, such as moving files between the device and the container, screen capture, the camera, and more.</td>
</tr>
</tbody>
</table>
Samsung Knox Workspace Device policies

<table>
<thead>
<tr>
<th>Policies</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Audit Log</td>
<td>Enable the device to keep an activities log.</td>
</tr>
<tr>
<td></td>
<td>You can fetch the audit log using a Admin Portal command.</td>
</tr>
<tr>
<td>Enable certificate validation before installation</td>
<td>Validate the certificate before installation in the device's certificate store</td>
</tr>
<tr>
<td>Enable revocation check for application SSL connections</td>
<td>Specify applications to check for certificate revocation</td>
</tr>
<tr>
<td>Per app VPN settings</td>
<td>Map a mobile application to a specific VPN connection for applications installed in personal mode (outside the container). You can specify multiple VPN profiles and application pairs. You configure the VPN profiles in the Samsung Knox Workspace VPN Settings policy.</td>
</tr>
<tr>
<td>Trusted certificate authorities</td>
<td>Add a list of trusted CA certificates</td>
</tr>
</tbody>
</table>

Using Touchdown settings

You use this Exchange Sync Settings to define the Exchange Sync profile on Android devices that use the Touchdown application for email.

Configuring Exchange profiles

You use the Exchange Settings policy to configure Exchange account profiles that are downloaded to devices by the Samsung service. Each profile defines the security and synchronization properties assigned to a specific Exchange Sync server. You must create a separate profile for each Exchange server.

You configure the Exchange Sync server profile separately for each type of device. For example, if your users have a mix of Android, iOS, and Samsung Knox devices, you would define profiles in the following branches:

- Touchdown Settings: You use this policy for Exchange Sync configuration for Android devices that do not provide a configurable email client.
  
  Note  Touchdown policy is not supported on Samsung Knox devices. Use the Exchange policies instead.

- iOS Settings: Use these policies for the iOS devices that use Exchange Sync servers.
  
  Note  If you have a POP or IMAP server for your iOS email, do not use this policy. Instead, use theiOS Settings > Mail settings policy instead.

- Samsung Knox Device Settings: Use the policy in this category to configure the email application installed outside the Samsung Knox container.

- Samsung Knox Workspace Container Settings: Use the policy in this category to configure the email application installed inside the Knox container.
Note  You can have separate policies for the email application running outside and inside the container on Samsung Knox Workspace devices.

Do not create multiple profiles for any one platform (for example, an iOS or Android device) in the same group policy object or policy set unless each profile applies to a different Exchange server.

Setting the user name

If you are using Active Directory or another LDAP server as your ID repository, you can use an attribute variable to specify an account’s user name. You can use any Active Directory/LDAP attribute that contains the user’s name, but the most useful ones are the following:

<table>
<thead>
<tr>
<th>Active Directory/LDAP attribute</th>
<th>Enter this variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>userPrincipalName</td>
<td>%{userPrincipalName}</td>
</tr>
<tr>
<td>samAccountName</td>
<td>%{samAccountName}</td>
</tr>
</tbody>
</table>

For example, the following Exchange profile for an iOS device uses the Active Directory/LDAP userPrincipalName variable in the User Name field:

When a user enrolls a device, the Samsung service contacts Active Directory/LDAP to resolve the user name attribute value for that device.

When an authentication domain is specified in the profile, the Samsung service builds the user name with the authentication domain first, followed by a backslash and then the user name. For example, the Samsung service would resolve the following values to user name gmail.com\j.weeks:

- Active Directory/LDAP user: j.weeks@acme.com
- Authentication Domain: gmail.com
- User Name attribute variable: %{samAccountName}
Using certificates

You can configure the profile so that the Samsung service installs a certificate generated either by the Samsung SDS IAM & EMM CA or the Active Directory Certificate Services certification authority you designated (see “Selecting the policy service for device policy management” on page 345). The certificate, regardless of the source, is automatically generated and installed in the device when the user enrolls the device.

When you use a certificate for authentication be sure to set the “Provide client certificate” option in the profile.

If you are using the Samsung SDS IAM & EMM policy service for device management policy, the Samsung SDS IAM & EMM CA is used to generate certificates. If you’re using Active Directory group policy for device management policy, the Windows Certificate Authority server is used to generate certificates. You cannot have a hybrid in which, for example, you select the Samsung SDS IAM & EMM policy service for device management policy but use the Windows Certificate Authority server is used to generate certificates.

Some configuration is necessary to Windows servers if you are using either source:

- If the Samsung service uses the Samsung SDS IAM & EMM CA to generate certificates, you must modify the configuration of the Exchange server—see “Modifying the IIS (Web) and Exchanger servers configuration for Samsung SDS IAM & EMM CA certificates” on page 241.

- If the Samsung service uses the Windows Certificate Authority to generate certificates, you must create a certificate computer and/or user templates on the Windows Certificate Authority server first. See “Using Active Directory certificates in devices for authentication” on page 365 for the details.

Modifying the IIS (Web) and Exchanger servers configuration for Samsung SDS IAM & EMM CA certificates

There are two phases to configuring the Exchange server to trust the Samsung SDS IAM & EMM CA

- Adding the Samsung SDS IAM & EMM CA certificate.
- Configuring IIS to support client certificate authentication.

The following procedures illustrate one way to perform these tasks. However, if you have more familiar procedures you can use them.

To add the Samsung SDS IAM & EMM CA certificate to the Exchange server:

1  Open Admin Portal, click Settings, and click Certificates.
   Click Download and copy the certificate to a folder you can access from the Exchange server.

2  Open the Exchange server using an administrator account enter the following PowerShell command:
certutil -dpublish <cert name>.cer NTAuthCA

where <cert name> is the name of the certificate you downloaded in Admin Portal.

This command enters the certificate into the Active Directory configuration container. To confirm, you can open ADSI Edit and expand the Configuration container to CN=Public Key Services. The certificate should be added to the list.

3 Open the Certificate Import Wizard.

For example, double click the certificate’s file icon to open the Certificate Import Wizard and click Install Certificate.

4 Select Local Machine and click Next.

5 Select Automatically select the certificate store based on the type of certificate and click Next.

6 Click Finish.

7 Click OK to exit the wizard.

To configure the IIS connections to support client certificate authentication:

1 On the Exchange server select Connections configuration and click the Exchange server node.

2 Open the Authentication icon.
3 Enable **Active Directory Client Certificate Authentication**.
4 Expand **Default Web Site** and click **Microsoft-Server-ActiveSync**.
5 Open the **Authentication** icon.
6 Disable all of the authentication methods.
7 Under IIS, open the **SSL Settings** (not shown in this picture).
8 Set **Require SSL** and for Client certificates select either **Accept** or **Require**.
9 Open the **Configuration Editor** icon.
10 Expand **system.webServer > security > authentication** and enable **clientCertificateMappingAuthentication**.
11 Expand **Exchange Back End** and select **Microsoft-Server-ActiveSync**.
12 Open the **Authentication** icon.
13 Enable **Anonymous Authentication** and **Windows Authentication**.
14 Open the **SSL Settings**.
15 Set **Require SSL** and for Client certificates select either **Accept** or **Require**.

**Configuring VPN profiles**

You use the VPN Settings policy to configure profiles that are downloaded to devices by the Samsung service. Each profile defines a VPN connection name, the server name, VPN type (PPTP, IPsec, SSL third party VPN), and other properties.

You configure a VPN connection profile separately for each type of device associated with either the policy set (when you use the Samsung SDS IAM & EMM policy service for device management policy) or group policy object (when you use Active Directory group policy for device policy management. For example, if your users have a mix of Samsung Knox devices and iOS devices, you would define profiles in the following categories:

- **iOS Settings**: Define profiles for the iOS devices.
  - You can configure a single VPN profile for all mobile applications or you can create multiple profiles and map each one to different applications.

- **Samsung Knox Device Settings**: Define profiles for the Samsung Knox devices that do not have a Workspace license.

- **Samsung Knox Workspace Settings**: Define profiles for use inside and outside the container on devices with a Workspace license.
  - The VPN profiles in Samsung Knox Workspace devices are configured separately for device and container use. See “Configuring VPN profiles for KNOX devices” on page 245.
Do not define multiple profiles for the same VPN server for the same device type.

Certificate-based authentication is available for VPN connections. When the profile specifies certificate authentication, the Samsung service calls either the Samsung SDS IAM & EMM CA or the Active Directory Certificate Services certification authority server you designated in (see “Selecting the policy service for device policy management” on page 345) to create the certificate when the user enrolls the device and then automatically installs it on the device.

“Configuring a VPN to use certificates for authentication” on page 244 has more details if you plan to use certificates for authentication.

**Configuring a VPN to use certificates for authentication**

When you use certificates for authentication, the user or computer certificate is automatically generated and installed when the user enrolls the device. If you are using the Samsung SDS IAM & EMM policy service for device policy management, the Samsung service uses Samsung SDS IAM & EMM CA to generate the certificate. If you are using Active Directory group policy for device policy management, the Samsung service uses the Windows certification authority server you designated in the connector to generate the certificate.

If the Samsung service uses the Windows certification authority server, you need to create the user and computer certificate templates—see “Using Active Directory certificates in devices for authentication” on page 365 for the details.

When you configure the policy in the Samsung SDS IAM & EMM policy service, you may need to upload the certificate for the certification authority that issued the certificate for the VPN concentrator. You don’t need to upload the certification authority’s certificate if the VPN concentrator’s certificate was issued by a well-known, commercial, certification authority or is self-signed. However, if the VPN concentrator’s certificate is neither, you need to upload the certification authority’s certificate to the Samsung service. You upload this certificate using the VPN Setting policy.

See your VPN concentrator or server vendor’s instructions for uploading the Samsung SDS IAM & EMM CA certificate. You create a Samsung SDS IAM & EMM CA certificate for uploading by clicking Download on the Device Policy Management page in Admin Portal Settings (see “Selecting the Samsung SDS IAM & EMM policy service” on page 346).

**Configuring VPNs in iOS devices**

You can define a VPN connection profile in the VPN Settings policy for use by all applications or only for use by an individual application. If you set the profile for “only for selected applications,” you assign the VPN profile to the application in the **Per App VPN settings** policy.

**Note** Some VPN clients do not support both options. For example, the Cisco client supports the “VPN is only for selected applications” only.
When you set a VPN connection “only for selected applications,” you can also configure it to auto connect when the application is opened. There are two settings available:

- **Auto connect when the application is launched:** Set this option if you are assigning the VPN to native iOS applications.

- **Auto connect when visiting the below domains:** Use this option to open the connection automatically when the user opens a web application from Safari. Enter the web application’s domain name to automate opening the connection.

  **Note** To open the VPN connection automatically from the Samsung SDS IAM & EMM client browser, map the following package name to the VPN connection in the Per App VPN settings policy:

  com.centrify.samsung.knoxemm

If you are using one profile for all applications, you can use certificates for authentication by selecting **Third Party VPN** as the VPN type in the General tab and then in the Security tab selecting **Certificate** for User Authentication. When you select Certificate, you need to specify the file name for the VPN server certificate in the **VPN CA Certificate** field.

**Note:** For Juniper VPN, we support the Pulse Secure iOS client.

### Configuring VPN profiles for Knox devices

You create VPN profiles for Knox Workspace devices in either or both the Samsung Knox Device Settings and the Samsung Knox Workspace Settings, depending upon whether or not you have Samsung Knox Workspace devices.

When you create the profile for a Samsung Knox Workspace device, you may have the option to designate it for one of two purposes, depending upon the VPN client you are using on the device:

- **VPN for all mobile applications**—Mocana (IPSec), F5 (SSL), and Juniper (SSL) clients
- **VPN is only for selected mobile applications**—Mocana (IPSec), F5 (SSL), Juniper (SSL) and Cisco (IPSec and SSL) clients

(These options are not available for VPN profiles in the Samsung Knox Device Settings.)

If you select “VPN for all applications,” you create one VPN profile, and it is used by all of the mobile applications installed in personal mode and inside the Knox mode container.

If you select “VPN is only for selected applications,” you can create multiple VPN profiles and then you use the “Per app VPN settings” policy in the Device Settings and Container Settings to map a profile to specific mobile applications. The mappings in the Device Settings category apply to the mobiles applications installed in personal mode and the policy in the Container Settings category for mobile applications installed in the Knox mode container.

The “Per app VPN settings” policy Explain tab in the Group Policy Management Editor and tooltip help in the Samsung SDS IAM & EMM policy service explain how to set a single VPN profile for use by all applications or different VPN profiles for individual applications.
Notes

- When you use Active Directory group policy for device policy management, you can specify certificate-based authentication for Samsung Knox Workspace devices with SSL-type VPNs using either the Juniper or F5 client. For IPSec type VPNs, you can specify certificate-based authentication using the Mocana client. (Certificate-based authentication is not available for Active Directory users using the Cisco client.)

  To use certificates, you must create a user and computer certificate template on the Windows certification authority server first. See “Using Active Directory certificates in devices for authentication” on page 365 for the details.

- Similarly, when you use the Samsung SDS IAM & EMM policy service for device policy management, the Juniper and F5 SSL clients and Mocana IPSec client support certificate-based authentication. (Again, the Cisco based clients do not support certificate-based authentication.)

  When you configure the policy in the Samsung SDS IAM & EMM policy service, you need to specify the VPN server’s certificate file in the profile to upload it to the Samsung service.

- There is a slight operational difference for devices with Knox 1 versus Knox 2 containers. From the policy configuration perspective, there is no difference. That is, configuring the VPN and Per app VPN policies are the same regardless of the container version.

  However, users with Knox 2 containers will have two VPN clients installed: one outside the container and one inside the container. (The Samsung SDS IAM & EMM client automatically installs both copies when you deploy the VPN client software from Admin Portal.) In addition, if users are required to enter their password to open the VPN, they will have to provide their password for both clients. On Knox 1 devices, just one VPN client is installed.

- When you configure the VPN profile for the Juniper client, you must specify the authentication realm and User role fields. However, you can leave the User name field blank. Users can fill in this field in the Samsung SDS IAM & EMM client when they configure the VPN settings.

- If you are using the Mocana VPN client, you must use a version later than 2.3.6.

Configuring Wi-Fi profiles

You use the Wi-Fi Settings policy to configure profiles that define the security type (for example WPA or WEP), accepted EAP types, and other properties for a Wi-Fi service set identifier (SSID).

You configure Wi-Fi profiles for iOS and Android separately from Samsung Knox devices:
• Use the Common Mobile Settings for the iOS and Android devices.

• Use Samsung Knox Device Settings for all Samsung Knox devices.

The Samsung Knox Device Settings provide additional policies in the **Wi-Fi Restrictions** category. You use them to control the users ability to modify the wi-fi connections in the Samsung device’s Settings application. However, these go into effect only for the profiles you define in Samsung Knox Device Wi-Fi settings.

You can define separate Wi-Fi profiles for the same SSID in the Common Mobile Settings and Samsung Knox Device Settings.

Certificate-based authentication is available for establishing a Wi-Fi connection. If you are using the Samsung SDS IAM & EMM policy service for device policy management, you use Admin Portal to create a policy set with the Wi-Fi profiles. In this case, the certificates are automatically issued by the Samsung SDS IAM & EMM CA and installed by the Samsung service when the user enrolls the device. You must select either WEP Enterprise or WPA/WPA2 Enterprise as the Security type on the General tab and TLS as the EAP type to use certificates.

When you configure the policy in the Samsung SDS IAM & EMM policy service, you may need to upload the certificate for the certification authority that issued the certificate for the Wi-Fi access point. You don’t need to upload the certification authority's certificate if the access point’s certificate was issued by a well-known, commercial, certification authority or is self-signed. However, if the access point’s certificate is neither, you need to upload the certification authority's certificate to the Samsung service. You upload this certificate using the Wi-Fi Setting policy.

See your Wi-Fi access point vendor’s instructions for uploading the Samsung SDS IAM & EMM CA certificate. You create a Samsung SDS IAM & EMM CA certificate for uploading by clicking **Download** on the Device Policy Management page in Admin Portal Settings (see “Selecting the Samsung SDS IAM & EMM policy service” on page 346).

If you are using Active Directory group policy for device policy management, you use the Active Directory Group Policy Management Editor to create the Wi-Fi profiles. In this case, the certificates are automatically issued and renewed by the Active Directory Certificate Services certificate server you designate (see “Selecting the policy service for device policy management” on page 345) and installed by the Samsung service when the user enrolls the device. You must create user and computer templates for the certificates on the Windows Certificate Authority server. See “Using Active Directory certificates in devices for authentication” on page 365.
Managing roles

The Roles page lists the default Samsung service roles plus the roles you have added. You can use the column headers to sort the applications by name, type, description, and status.

Note Your role must have the Roles Management administrative right to view, add, and modify roles. See “Creating Samsung service administrators” on page 252 for the details.

You use roles to assign applications, permissions, and policies to separate sets of users. This chapter contains the following topics:

- “Predefined roles” on page 249
- “Removing users or groups from a role” on page 250
- “Assigning applications to and removing them from roles” on page 251
- “Creating Samsung service administrators” on page 252
- “Deleting roles” on page 256
Predefined roles

The Samsung service provides the following predefined roles:

- **Everybody**: By default, all Samsung service users are assigned to this role. For example, all users that are added to the Samsung SDS IAM & EMM directory by using bulk import are added to the Everybody. Similarly, if you are using Active Directory/LDAP as your directory service, users are automatically added to Everybody when they log in to the Samsung SDS IAM & EMM user portal the first time or enroll a device. When you add an individual user, the default setting is to add the account to the Everybody role. To exclude a user from the Everybody role, select the **Is Service User** option on the user Account page.

  It is best practice to assign most users to the Everybody role. For example, the Samsung SDS IAM & EMM User Portal application is automatically assigned to members so that they can log in to the user portal. However, there are users you may not want to have in the Everybody role; for example, temporary users such as service contractors. Users that are not assigned to the Everybody role cannot log in to the user portal until they are members of a role to which you have explicitly deployed the Samsung SDS IAM & EMM User Portal application. (See “Deploying the Samsung SDS IAM & EMM User Portal application” on page 117 for more information.)

- **Invited Users**: This role is created when you use the Invite Users button and select Invited Users as the Role. The Samsung SDS IAM & EMM User Portal application is automatically assigned to this role.

  **Note** If you do not use the Invite users button or select the Invited Users role when you invite a user, this role is not created.

- **sysadmin**: This role grants full access to all Admin Portal settings. By default, the Samsung SDS IAM & EMM directory account for the user who signed up for the Samsung service is a sysadmin role member. You cannot delete or rename the sysadmin role.

  Only sysadmin role members can add more users to the sysadmin account.
Removing users or groups from a role

You open the role and click the Members tab to add and remove Samsung SDS IAM & EMM directory accounts and roles to and from a role. If you are also using Active Directory/LDAP for user authentication, you can add Active Directory/LDAP user accounts and groups to a role.

To remove a role member:

1. In Admin Portal, click Roles.
2. Click the role.
3. Click Members.
4. Click the check box for each member you want to remove.
   - The Add button is replaced by an Actions button.
5. From the Actions drop-down menu, click Delete.
6. Click Save.
Assigning applications to and removing them from roles

The role’s details page displays the applications assigned to it. You can use either this window or the User Access window in the application’s configuration page (see “Removing an application” on page 130) to assign an application to a role.

Role members who are logged in to the user portal see the changes within seconds. On the role members’ devices, the change appears the next time they open the Samsung SDS IAM & EMM client. Alternatively, they can refresh the Apps screen to see the changes immediately.

To add applications to a role on the Roles page:

1. In Admin Portal, click Roles.
2. Click the role.
3. Click Assigned Applications.
4. Click the Add button.
   The Add Applications pop up window contains all of the applications listed on the Apps page, including the applications that have already been assigned to the role.
   To search for an application, enter the first few characters in the name. When you stop, the pane contains all applications that match the string.
5. To add an application, click the check box.
   You can select multiple applications. Click Add.
   To add more applications, click the Add button again, enter the search string, and click Add again.
6. Click Save.

To remove applications assigned to a role on the Roles page:

1. In Admin Portal, click Roles.
2. Click the role.
3. Click Assigned Applications.
4. Click the check box for the applications you want to remove.
   The Add button is replaced by an Actions button.
5. From the Actions drop-down menu, click Delete.
6. Click Save.
Creating Samsung service administrators

You use roles to create Samsung service service administrators. Only users in the sysadmin role and users in roles with administrative rights other than Enroll Devices can open the Admin Portal.

To create a Samsung service service administrator, you create a role, assign one or more Admin Portal administrative rights, and then add users to the role. The administrative rights let you define roles with separate application, user, device, report, and role management permissions.

For example, you can create an role that limits the administrator to managing applications and the application-to-roles assignments only. In this role, the administrators can perform all the functions on the Apps page and see the contents of the Users and Roles pages. However, they get an error message when they try to make a change on the Users and Roles pages. In addition, the Devices page for these administrators is blank.

Similarly, you can create administrative roles with just device, user, and report management permissions.

System administrator role permissions

The sysadmin role members have access to all Admin Portal tabs and the Samsung SDS IAM & EMM connector configuration program settings and are the only administrators who can perform the following tasks:

- Add users to or remove them from the sysadmin role.
- Modify the Account Customization tab on the Settings page in Admin Portal.
- Modify connector settings in the Samsung SDS IAM & EMM connector tab on the Settings page in Admin Portal.
- Modify policy sets.

These rights cannot be assigned to other roles.

Admin Portal administrative rights

The following table describes the administrative rights (also referred to as permissions) you can assign to a role. Users cannot log in to Admin Portal unless they have at least one of the following administrative rights.

If an administrator attempts to perform a task in Admin Portal for which they do not have the associated administrative right, Admin Portal displays an error message. In addition, Admin Portal does not display data if it’s not pertinent to the administrator’s privileges. For
example, if the administrator has the Application Management privilege only, Admin Portal does not display any devices on the Devices page.

<table>
<thead>
<tr>
<th>Administrative right</th>
<th>Associated permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Management</td>
<td>Access to any activities that originate on the Apps page, such as the ability to add, modify, or remove applications. From the Application Settings dialog box, this right also grants the ability to change which roles are assigned to a specific application.</td>
</tr>
</tbody>
</table>
| Device Management (Limited)              | Use of all the commands that originate from the Devices page except the following:  
  All devices:  
  • Wipe Device  
  • Unenroll Device  
  Samsung devices only:  
  • Device Lockout  
  • Remove Container  
  The purpose of this permission is to provide limited device management rights to, for example, helpdesk staff. This allows users with this permission to help users but prevents them from performing any destructive actions to a device or a container. |
| Device Management (All)                  | Use of all the commands that originate from the Devices page, such as the ability to update policies, lock, reset the passcode, wipe, unenroll, delete, or view device details.  
  Note: The user must have the Device Management permission to run the APNS Certificate, Mass Deployment, and Exchange ActiveSync Server Settings options on the Settings page in Admin Portal. |
| Federation Management                    | Permission to create, manage, and delete federation partnerships. See “Managing Business Partner Federation” on page 312 for information on setting up partner federations. |
| Privilege Management (Portal Login)      | Users with this administrative right can access resources using the accounts where they have Portal Login permissions in Privilege Manager. This right allows users who do not access the Privilege Manager portal to log on to selected resources using selected accounts directly from the User Portal. |
| RADIUS Management                        | Permission to create, manage, and delete the RADIUS server. See “Configuring Samsung SDS IAM & EMM RADIUS Support” on page 298 for information on using the Samsung SDS IAM & EMM connector as a RADIUS server. |
| Read Only System Administrator           | Access to all of the Admin Portal tabs, however, the user cannot make any changes. An error message is displayed when the user attempts to save the change. |
Creating Samsung service administrators

Admin Portal user’s guide

To add administrative rights to a role:

1. In Admin Portal, click **Roles**.
2. Click the role.
3. Click **Administrative Rights**.
4. Click **Add**.
5. In the **Add Rights** window, click the check box for each right you want to add and click **Add**.
6. Click **Save**.

To remove administrative rights from a role:

1. In Admin Portal, click **Roles**.
2. Click the role.
3. Click **Administrative Rights**.
4. Click the check box for the administrative rights you want to remove.

   The Add button is replaced by an Actions button.
5. From the **Actions** drop-down menu, click **Delete**.
6. Click **Save**.

### Administrative right | Associated permissions
---|---
Register connectors | Register a Samsung SDS IAM & EMM connector in your Samsung service account. During the connector installation, the wizard prompts you to enter the account of a user that has the Register connectors right. This must be a Samsung SDS IAM & EMM directory account. Make sure the account you specify is a member of a role with this permission. If this is the only permission for a role, members can open Admin Portal, however, the pages for all of the tabs except for Settings are blank.
Report Management | Create, delete, and run reports.
Role Management | Access to any activities that originate on the Roles page, such as the ability to add, modify, or delete roles; this includes the ability to assign rights.
User Management | Permission to use the Add User and Bulk User Import buttons to add users and modify Samsung SDS IAM & EMM directory user properties.
Updating a user rights

If a user who is affected by a change to the role’s administrative rights, the change does not take affect until the user logs in again. If the user is logged in when you make the change, the pre-existing rights persist.

Use the following procedure to update the user’s rights immediately.

To update a user’s administrative rights immediately:

1. In Admin Portal, click Users.
2. Select all of the affected users.
3. In the pop up window, click Reload.
Deleting roles

You can delete any role you created. You cannot delete the sysadmin and Everybody roles. When you delete a role, the applications assigned to the role members are deleted from the Apps page in the Samsung SDS IAM & EMM user portal and their devices.

To delete Samsung service roles:

1. In Admin Portal, click Roles.
2. Select one or more roles.
   
   The Add Role button is replaced by an Actions button.

3. From the Actions drop-down menu, click Delete.
4. Click Yes to confirm the deletion.
Chapter 22

Managing customer Samsung services

The Customers page lists the Samsung services you have created for your customers and their status. You use this page to perform the following tasks:

- Create a new Samsung service for an organization.
- Disable and enable a Samsung service.
- Log in as a system administrator to a customer’s Samsung service.

You must be a sysadmin or a member of a role that has the Customer Management permission to view the contents of the Customers page and create, disable, and log in to a customer’s Samsung service.

**Note** The Customer page is only displayed in Admin Portal on Managed Service Provider accounts. It is not displayed in customer accounts.

This chapter contains the following topics:

- “About customer Samsung services” on page 258
- “Creating an Samsung service for a customer” on page 259
- “Disabling and enabling a customer Samsung service” on page 261
- “Logging in to a customer Samsung service” on page 262
- “Creating roles that can create and manage customer Samsung services” on page 263
About customer Samsung services

A customer Samsung service is a full implementation of the Samsung service. The customer identity platform has the following high-level features:

- The customer’s Samsung service has its own unique customer ID and login suffix.
- The system administrators have full control over the users, apps, devices, roles, etc. in their Samsung service.
- The user accounts, policy sets, roles, enrolled devices, etc. are unique to that Samsung service.

Only Managed Service Providers (MSPs) have the ability to create Samsung services for customers. Administrators for the customer’s Samsung service, for example, cannot create additional Samsung services.

When you create an Samsung service for a customer, a MSP administrator account—mspadmin@<new login suffix>—is created on the customer’s Samsung service. This account lets you log in to the customer’s Samsung service with full system administrator privileges. This user account cannot be deleted.
Creating an Samsung service for a customer

You create a Samsung service for a customer from the Customers page in Admin Portal. Fully preparing a Samsung service for a customer is a two-part process:

- First, you create the Samsung service for the organization.
- Second, you log in to it to configure the basic settings, create, minimally, a system administrator account for the customer, and then invite that user to log in to their Samsung service.

Creating the Samsung service

To create the account, you enter the email address and a user name, phone number, job title, company, etc. for the customer. This person does not need to be an administrator and does not have any special privileges in the new Samsung service.

**Note** The login suffix in the email account is the default login suffix for new user accounts. If that login suffix is already in use by another customer, it cannot be re-used, and the Samsung service automatically appends a number to make it unique. The full login suffix (that is, with the number) then becomes the default login suffix for new user accounts in that Samsung service. You can create additional login suffixes by logging into the customer’s Samsung service and using the Login Suffix tab in the Settings tab in Admin Portal—see “Using login suffixes” on page 337.

The new Samsung service is added to the Customers page. To continue the second preparation phase, you log in to the new Samsung service from this page.

To create a Samsung service for an organization:

1. Open Admin Portal and click the Customers tab.
2. Click Create Customer.
3. Fill in all of the fields for the customer account.
4. Select an Samsung service location.
   - Click the drop-down menu and select the Samsung service location that is closest to the organization’s offices.
5. Click Submit.

Preparing a Samsung service for customer take over

After you create an Samsung service, it has only one account—mspadmin, the Default Policy settings are applied to all users, and the General Options (see “Customizing Samsung service user interfaces” on page 291) are set to the default values. At this point, only you can log in to Admin Portal for this Samsung service.
Minimally, you should create one user account for the customer, add it to the System Administrator role, and then invite that user to log in to the Samsung service. You do this by logging in to the Samsung service you just created (see “Logging in to a customer Samsung service” on page 262) and then do the following:

1. Create an account for the customer’s IT administrator.
   
   See “Creating user accounts” on page 5 for the details.

2. Add that account to the System Administrator role.
   
   See “Creating Samsung service administrators” on page 252 for the details.

3. Inviting the administrators to log in to their Samsung service.
   
   See “Sending invitations to users” on page 110 for the details.

   **Note** The invitation logs the user in to the user portal. However, because the account is a member of the System Administrator role, the user can open Admin Portal from the user portal.

Alternatively, you can more fully configure the Samsung service for the customer. For example, you can do the following to help the customer get started faster:

- Customize the user interface with the customer’s colors and logo (see “Customizing Samsung service user interfaces” on page 291).
- Modify the default policy set or create new policy sets (see “Managing policies” on page 185).
- Add default web and mobile applications (see “Adding web applications by using Admin Portal” on page 131 and “Adding and deploying mobile applications using Admin Portal” on page 138).
Disabling and enabling a customer Samsung service

By default, a customer’s Samsung service is enabled when you create it. You can disable but you cannot delete a customer’s Samsung service. The current state of the Samsung service is shown in the **Status** column.

Disabling a Samsung service has the following results:

- You cannot log in to Admin Portal for the customer’s Samsung service.
- The customer’s administrators cannot log in to Admin Portal.
- The customer’s users cannot log in to the user portal.
- On the users’ devices, the Samsung SDS IAM & EMM client remains installed, however, single sign-on is not provided for the web applications.
- If the customer installs connectors, the connector blocks all communications with the Samsung service.

The listing remains on the Customers page so that you can enable it again.

To disable a customer’s Samsung service:

1. Open Admin Portal and click the **Customers** tab.
2. Click the customer’s check box.
3. Expand the **Actions** menu and click **Disable**.

To enable a disabled account, repeat the procedure and click **Enable**.
Logging in to a customer Samsung service

When you log in to a customer’s Samsung service from the Customers page, you are logged in using the mspadmin account and have system administrator permissions.

Note  When you log in to customer’s Samsung service, the Admin Portal session is opened in a separate tab. The top area of the new window displays the customer name to distinguish that session from your own Admin Portal session.

To log in to a customer’s Samsung service:

1  Open Admin Portal and click the Customers tab.
2  Click the customer’s check box.
3  Expand the Actions menu and click Login.
   
   You are automatically authenticated to the customer’s Admin Portal using the mspadmin account.
Creating roles that can create and manage customer Samsung services

Only members of the System Administrators role or a Samsung service role that has the Customer Management administrative right can view, create, disable or log in to customer Samsung services. You create roles and add administrative rights to them from the Roles page in Admin Portal. See “Creating roles and adding users to roles” on page 11 for the details.

The Customer Management administrative right is only available on Managed Service Provider accounts. For all other accounts, this administrative right is not displayed. For example, the administrative rights available when your customer’s system administrator lists the Administrative Rights does not include Customer Management.

See the procedure, “To create a role with users, administrative rights, and applications:” on page 11 to continue and then go to “Creating Samsung service administrators” on page 252 to add the administrative rights that allow the user to log in to Admin Portal. To give a role the ability to create, disable, and log in to customers’ Samsung services, add the Customer Management administrator right to the selected role.
Creating roles that can create and manage customer Samsung services
Managing reports

You can create reports to find out specific information about your data and then share that information with other Samsung service administrators. A report is a SQL query against your database tables and the results that the query generates. You can create reports as a way to find out specific information about your data: applications, devices, users, roles, connectors, and so forth.

You can use the default, built-in reports, or you can search for specific kinds of data by building your own report queries. You can also share reports with your other Samsung service administrators.

This section includes the following topics:
- “What’s in the Report Library” on page 266
- “Reports provided in Admin Portal” on page 267
- “Access to shared reports and report data” on page 268
- “Selecting report data” on page 270
- “Working with reports” on page 277
- “Report query examples: Built-in report definitions” on page 281
- “Report syntax examples” on page 283
What’s in the Report Library

Use the Reports page to view, create, and share your reports. When you click Reports, the page opens to the My Reports folder. This folder lists all of the reports you have created. If you have not created any reports of your own, you might want to start by browsing through the predefined reports provided in the Builtin Reports folder and its subfolders. For example, if you expand the Builtin Reports folder and select the Mobile subfolder, you would see a list of the prebuilt reports for mobile devices.

Admin Portal provides the following folders to store reports:

**Builtin Reports**: Admin Portal provides some prebuilt reports in this folder. You can copy these reports into your My Reports folder or the Shared Reports folder. After you copy a report to another location you can then modify the report.

**My Reports**: When you create a new report or modify a report, Admin Portal saves it here. You can also copy built-in or shared reports to this folder so that you have all the reports that you use in one place. Only you can see the reports in your My Reports folder.

**Shared Reports**: To share reports with other administrators, you move or copy the reports here.
Reports provided in Admin Portal

Admin Portal provides built-in reports for applications, mobile devices, resources, and security. The reports are organized into subfolders. You can browse the subfolders in the top-level Built-in Reports folder to see the reports that Admin Portal provides.

These built-in reports demonstrate the kinds of data you can gather and display in your reports.

What you can do with a report and whether or not you can modify it depends on where the report is. You can modify, export, copy, move, or delete reports in the My Reports folder. You can export or copy reports in the Built-in Reports folder.

Exporting a report creates a file on your computer; you can specify either CSV or Microsoft Excel format. Copying a report duplicates the report into another reports folder.
Access to shared reports and report data

When you view a report, you can only read the data that you have permission to access. If you don’t have read permission to a particular kind of data, such as applications, devices, or users, then the report doesn’t display that information for you. (Permissions are granted to roles by the sysadmin—see “Assigning applications to and removing them from roles” on page 251 for the details.

Note The report doesn’t indicate any limitations to that user’s permissions. This means that people with different permissions can view the same report but see different results.

You can share any report in the Shared Reports folder. Sharing a report involves assigning it to specific roles and also to the folder(s) that contain the report.

When you assign a report or a report folder to a role, you also specify the level of access that the role has—read access, read and write access, or owner access. If you specify a role as an owner of a report or a report folder, then that role can modify, rename, share, or delete the report.

There are three kinds of access permission for reports:

- The level of access to the report definition
- Access to the data that is read by the report
- Access to the folder that contains the report

The report access level determines whether you can read, copy, modify, or share the report definition.

You can create reports in the Shared Reports folder, or you can copy reports from either the My Reports or Builtin Reports folders into the Shared Reports folder.

When you modify a report in the Shared Reports folder, you can also assign the report to roles. When you assign the report to a role, you also specify what the administrators in that role can do with the report by specifying either the Read, Read and Write, or Owner access. You also specify similar levels of access for the report folders.

- **Read**: Administrators can view and copy the report, but they cannot modify it, move it, or share it.

- **Read and Write**: Administrators can view, copy, move, and modify the report.

- **Owner**: Administrators can view, copy, move, and modify the report. Administrators can also grant other administrators access to the report.

At the minimum, you need to assign administrators to a role with at least the Read Only System Administration permission to enable them to view built-in and their own reports.

In order to share reports, you need to assign administrators to a role with Report Management permission.
However, you also need to grant administrators access to the types of data that you want them to view in the report. Administrators do not see report data for which they do not have permission to view.

Administrators can always view report data related to their own mobile devices.

For example, if an administrator has the Application Management permission but not the Device Management permission, when that administrator opens a report that generates both application and device results, the administrator sees only the application data.
Selecting report data

You can open the data dictionary to see the tables and column names that you can use in your reports. When you create a report, you open the Data Dictionary by clicking the >> button in the upper right area of the screen.

With the Data Dictionary visible, you can find the column names in a particular table by clicking the triangle next to a table name. The Data Dictionary provides table names, column names, and data types so that you know what to enter in your SQL query.

Although there are other tables in the database that you can use in your reports, the tables mentioned below are likely to be the most useful to you.

- **ADUser**: The Active Directory User table stores some basic information related to users, such as SamAccountName, UserPrincipalName, Mail, and so forth.

- **Application**: Stores information related to web and mobile applications, such as web application type, mobile application type, application version, and so forth.

- **Device**: Stores information related to mobile devices, such as operating system version, compliance status, and when the device last connected with the Samsung service.

- **Event**: Stores activity information related to applications, devices, and users, such as counts for application launches, logins, device types, and so forth.

Note  When creating queries with the Event table, you must specify a time boundary. There are too many records in the Event table to query all records. For details, see “Filtering events by time with DateFunc()” on page 272.

Report query syntax

Creating the query for a report involves using SQL statements. SQL is a Structured Query Language for retrieving data from databases. SQL statements can be simple or complex,
Selecting report data

depending on the data that you want to find and how you want it to display. The key is to know what you want to see in your report, and understanding what kind of data is available to you.

For example, here’s a simple SQL statement:

```sql
SELECT Owner FROM Device
```

This query looks for the listed owners of enrolled mobile devices, as recorded in the Owner column of the Device table.

The main component of a SQL query is the SELECT statement. SELECT does just that - it selects which data to display. You can select one or more columns from one or more tables to retrieve. You can use any of the following SELECT statements in Admin Portal report queries:

- **SELECT**: Selects data from the specified columns in the specified tables.
- **SELECT ***: Selects all records from the specified table.
- **SELECT DISTINCT**: Selects the unique records from the specified columns in the specified tables. The DISTINCT keyword trims out the duplicate records.

If you want to look at columns in different tables, you can also combine the results by using UNION or one of the JOIN statements.

In addition to selecting the database tables to retrieve, you can also provide conditions to further refine your query results. You can use any of the following SQL statements to specify conditions:

- **AND / OR**: Selects data that meets both conditions (AND) or one of the specified conditions (OR).
- **BETWEEN**: Use BETWEEN to select results that are within a specified range.
- **IN / NOT IN**: Use IN or NOT IN to specify multiple values in a WHERE clause.
- **LIKE**: Use LIKE to search for a specified pattern in a column.
- **WHERE**: Use WHERE to specify criteria to filter for, such as column values and so forth.

**Note** Admin Portal uses a subset of SQL-92 that only supports SELECT statements. SQL commands that change database values are not valid (CREATE, ALTER, DELETE, DROP, INSERT, SELECT INTO, TRUNCATE, UPDATE, and so forth).
Filtering events by time with DateFunc()

When you query the Event table, you must include a time boundary to limit your query results. Admin Portal provides a DateFunc() SQL function to filter events based on time.

**DateFunc Syntax**

Use the following syntax:

```
DateFunc( <stringdate>, [<offset>])
```

where

- `<stringdate>` can be one of the following three options:
  - 'now' - this means now (current time)
  - 'today' - this means the start of today (current day)
  - `<date string>` - a string that represents a specific date and time, such as '09.30.2016:0100'.
- `<offset>` is a string representing an offset.
  - '-n' means minus n days
  - '-5:00' means minus 5 hours

---

<table>
<thead>
<tr>
<th>Description</th>
<th>SQL Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events that occurred in the last 30 days</td>
<td><code>select WhenOccurred, FailUserName, FromIPAddress from event where EventType = 'Cloud.Core&gt;LoginFail' and whenoccurred &gt;= DateFunc('now', '-30')</code></td>
</tr>
<tr>
<td>Events that occurred in the last 24 hours</td>
<td><code>select WhenOccurred, EventType from Event where WhenOccurred &gt; DateFunc('now', '-1')</code></td>
</tr>
<tr>
<td>Events that occurred in the last 48 hours</td>
<td><code>Select * from Event where WhenOccurred &gt; DateFunc('now', '-2')</code></td>
</tr>
<tr>
<td>Events that occurred in the last 54 hours</td>
<td><code>Select * from Event where WhenOccurred &gt; DateFunc('now', '-2.06:00')</code></td>
</tr>
<tr>
<td>Events that occurred on or before August 7, 2013</td>
<td><code>select WhenOccurred, UserName, FromIPAddress, AuthMethod, Factors from Event where EventType = 'Cloud.Core/Login' and WhenOccurred &gt; datefunc('now', -7)</code></td>
</tr>
<tr>
<td>Events that occurred yesterday</td>
<td><code>select eventType,WhenOccurred from event where whenoccurred&gt;datefunc('now', '-3') and whenoccurred &lt; datefunc('now', '-2')</code></td>
</tr>
</tbody>
</table>
Note  The Samsung service operates using UTC time and displays in local time. So, “today” means the start of today according to UTC time, and ‘3:15’ means 3:15 today in UTC time. For example, if you specify ‘3:15’ while you’re in California during Daylight Savings Time, you’re actually specifying 8:15 am UTC time.

**Formatting dates to strings with Formatdate()**

You can use the Formatdate() function to convert a date to a string. Use the following syntax:
```
formatdate(<date>, <format_string>)
```

For example, to extract the month number from a date, use the following syntax:
```
formatdate(<date>, "MM")
```

If you process a date in November through the above example, it returns an “11” to indicate November.

**Selecting location data**

You can also include a geographic map of logins or devices where it displays the last known location. Location data for a device is encrypted, but you can extrapolate it from the IP address. Keep in mind, however, that location data is accurate to within about 50 miles—the locations are not precise.

Use the IpLookup() function to convert IP address data to geographical data, with the following syntax:
```
Iplookup(<ipaddress>, 'country|country_code|longitude|latitude|city')
```

For example, the following report query returns the locations of failed logins within the last 30 days.
```
select
    iplookup(FromIPAddress,'longitude') as Longitude,
    iplookup(FromIPAddress,'latitude') as Latitude,
    FailUserName || ' - ' || formatdate(whenoccurred , 'G') as Name from event
where eventtype='Cloud.Core.LoginFail'
    and whenoccurred > datefunc('now', -30) limit 1000
```

In order for a report to display results in a geographical map, you must select the option “Report can be displayed on a map” and also include the following column labels in your report query:

- Latitude
- Longitude
- Name (this is any string value; it’s used to label a location on the map)

Note  Map view is not available in reports preview mode.
Note  Country names and city names are in English.
Common events that you can search for

When collecting information from the Event table, you specify types of events that you want to have in your report. Here's a list of the most common types of events that you might see in the Event table.

Cloud.Saas.ApplicationLaunch
Cloud.Saas.Application.AppAdd
Cloud.Saas.Application.AppModify
Cloud.Saas.Application.AppDelete
Cloud.Saas.Application.SamlResponseGenerate
Cloud.Saas.ProfileUpdate
Cloud.Saas.PasswordChange
Cloud.Core>Login
Cloud.Core.Login.MultiFactorChallenge
Cloud.Core.LoginFail
Cloud.Core.Logout
Cloud.Core.SamlTokenValidate
Cloud.Core.SamlTokenValidateFail
Cloud.Core.Access.CheckRightsFailure.Table
Cloud.Core.Access.CheckRightsFailure.Table.Row
Cloud.Mobile.Enroll
Cloud.Mobile.StateChange
Cloud.Mobile.AppChange
Cloud.Mobile.DeviceAction
Cloud.Mobile.Device.DeviceAction
Cloud.Mobile.Device.AppChange
Cloud.Mobile.Device.StateChange
Cloud.Mobile.Device.Enroll
Common events that you can search for

Cloud.Mobile.GpChangeDetected
Working with reports

When you open a report, use the Actions menu to invoke the following commands:

<table>
<thead>
<tr>
<th>Action menu command</th>
<th>To do this</th>
</tr>
</thead>
</table>
| View                | Display the reports details and set the following properties:  
                     • Report can be displayed on a map  
                     • Validate report on save  
                     The details include the report name, description, and SQL query.  
                     You can generate a preview of the results in this option too. |
| Export Report       | Save the SQL script in a CSV or Excel spreadsheet file. |
| Email               | Send the query results to an email account. You can send the data as an Excel spreadsheet or HTML table. |
| Copy                | Copy the report to your My Reports or Shared Reports folder. |

Viewing reports

When viewing a report, you can click any column heading to sort by that column. You can also click and drag a column heading to move it and adjust the column widths.

To view a report:

1. In the Reports page, select a report folder.
   - By default when you first open the Reports page it opens to your “My Reports” folder.
2. Navigate to a report and click it to open it.
3. Expand the Actions menu and click View.

   Note Some reports offer two viewing options: Mapped Reports and Reports. Select Mapped Reports to view the data on a geographical map or Reports to view the data in rows and columns.

Modifying applications or devices directly from a report

If your report includes web applications or devices in the report results, you can click a specific application or device to see the details for that object. This works when a specific object (device ID or application name) displays in the result set, not a grouping of objects.

For example, if you create a report that lists a mobile device ID, you can right-click the Device ID and perform device-related actions - such as delete, update policies, unenroll, and so forth.
Exporting report data

When viewing report results, you can select one or more rows and export the results to a CSV or Microsoft Excel file.

Creating a new report

To create a new report:

1. In the Reports page, click New Report.
2. Enter the report name and description.
   Names can contain letters, numbers, and underscores. Do not include special characters or white space.
3. In the Query text box, enter SQL statements to populate your report.
4. To open the Data Dictionary and locate the available table and column names, click the << button in the upper right corner of the dialog box. (Click >> to close the Data Dictionary.)
   Folders represent tables, and the items within each folder are the table columns.
5. Click Preview to see what results your query produces.
   **Note** Preview mode does not support map views.
6. Continue editing the SQL statement and clicking Preview until you get the data that you’re looking for.
7. If your query includes geographical data for a map, select **Report can be displayed on a map**.
8. Click Save.
   Admin Portal saves your report in the My Reports folder.

Copying an existing report

To copy an existing report:

1. In the Reports page, navigate to the report that you want to copy.
   You can copy any report in any folder that you have access to.
2. Right-click the report and click **Copy**.
3. Select the folder where you want to copy the report to.
   You can copy reports to either My Reports or Shared Reports.
4. Enter the name of the new report, and click **Save file**.
Admin Portal saves a copy of the selected report in the specified location with the specified name.

Sharing a report and granting report access

You share a report by assigning it to one or more roles, and giving each role either Read, Read and Write, or Owner level of access. Before you can share a report, you must move or copy it to the Shared Reports folder.

You must have the Report Management permission in order to copy reports in the Shared Reports folder.

To share a report:

1. Make sure that the report is in the Shared Reports folder.
2. Right-click the report and click Modify.
   The Report Settings dialog box opens.
3. Click the Role Access tab.
4. Select the roles that define who should get access to the report.
5. For each role, specify the level of access: Read, Read and Write, or Owner.
6. Click Save.

Administrators assigned to the designated roles can now access the report as specified.

Deleting a report

You can delete a report in the Shared Reports or My Reports folders.

To delete a report:

1. Right-click the desired report and click Delete.
   You can also select multiple reports and click Delete in the pop-up menu.
2. In the confirmation dialog box, click Yes.
   Admin Portal deletes the specified report.

Creating a new report folder

You can create new folders in the Shared Reports or My Reports folder. You can grant access to folders in the Shared Reports folder.

To create a report folder:

1. Right-click either the Shared Reports or My Reports folder and click New Folder.
2 Enter the folder name.
3 Click **Save new folder**.
   Admin Portal creates the new folder.

**Granting access to a report folder**

You can modify who has access to the Shared Reports folder or any its subfolders that you create. Granting access to a folder grants access to open the folder; you specify access to the reports in that folder separately.

To grant access to a shared reports folder:
1 Right-click the Shared Reports folder and click **Modify**.
2 Select the desired roles for whom you want to grant report folder access to.
3 For each role that you select, specify the report access level.
   - Read
   - Read and Write
   - Owner
4 Click **Save**.
   Admin Portal saves the changes.
## Report query examples: Built-in report definitions

Admin Portal provides some built-in reports that you can use or copy and then modify as desired. You can view the SQL statements for any of the built-in reports in Admin Portal. For convenience, here are some examples of the report definitions for several of the built-in reports so you can see examples of the SQL syntax being used.

<table>
<thead>
<tr>
<th>Report description</th>
<th>Query syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web apps used the most often during the last 30 days</td>
<td><code>select ApplicationName as Name, count(*) as Count from Event where WhenOccurred &gt;= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch' group by Name order by count desc</code></td>
</tr>
<tr>
<td>Web apps added and used in the last 30 days</td>
<td><code>select distinct ApplicationName from Event where EventType='Cloud.Saas.Application.AppLaunch' and ApplicationName in (select applicationname from event where WhenOccurred &gt; DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppAdd')</code></td>
</tr>
<tr>
<td>Web apps that weren't used in the last 30 days</td>
<td><code>select Name from application where DisplayName not in (select ApplicationName from Event where WhenOccurred &gt;= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch') and AppType = 'Web'</code></td>
</tr>
<tr>
<td>A listing of the different Android versions in use</td>
<td><code>select OSVersion, Count(*) as Count from device where InternalDeviceType = 'A' group by OsVersion order by Count desc</code></td>
</tr>
<tr>
<td>Number of devices, organized by mobile carrier</td>
<td><code>select Carrier, count(*) as Count from device group by Carrier</code></td>
</tr>
<tr>
<td>Number of devices, organized by iOS, Mac, Android, and Windows</td>
<td><code>select case(InternalDeviceType) when 'I' then 'iOS' when 'M' then 'Mac' when 'A' then 'Android' when 'W' then 'Windows' end as Platform, Count(*) as Count from device group by InternalDeviceType order by Count desc&quot;, &quot;DisplayName&quot;: 'DeviceByPlatform'</code></td>
</tr>
<tr>
<td>A listing of the different iOS versions in use</td>
<td><code>select OSVersion, Count(*) as Count from device where InternalDeviceType = 'I' group by OsVersion order by Count desc</code></td>
</tr>
<tr>
<td>All mobile apps, organized by the number of installations</td>
<td><code>select Name, Count(*) as Count from InstalledApp group by Name order by Count desc</code></td>
</tr>
<tr>
<td>Report description</td>
<td>Query syntax</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed logins in the last 30 days</td>
<td><code>select WhenOccurred, FailUserName, FromIPAddress from event</code></td>
</tr>
<tr>
<td></td>
<td><code>where EventType = 'Cloud.Core.LoginFail'</code></td>
</tr>
<tr>
<td></td>
<td><code>and whenoccurred &gt;= DateFunc('now', '-30')</code></td>
</tr>
<tr>
<td>Users who haven't logged in during the last 30 days</td>
<td><code>select UserName, DisplayName, LastLogin from User where ID</code></td>
</tr>
<tr>
<td></td>
<td><code>not in</code></td>
</tr>
<tr>
<td></td>
<td><code>select UserGUID from Event</code></td>
</tr>
<tr>
<td></td>
<td><code>where EventType = 'Cloud.Core.Login'</code></td>
</tr>
<tr>
<td></td>
<td><code>and WhenOccurred &gt;= DateFunc('now', '-30')</code></td>
</tr>
<tr>
<td>The users who have logged in the most often during the</td>
<td><code>select NormalizedUser as User, Count(*) as Count from Event</code></td>
</tr>
<tr>
<td>past 30 days</td>
<td><code>where EventType = 'Cloud.Core.Login'</code></td>
</tr>
<tr>
<td></td>
<td><code>and WhenOccurred &gt;= DateFunc('now', '-30')</code></td>
</tr>
<tr>
<td></td>
<td><code>group by User</code></td>
</tr>
<tr>
<td></td>
<td><code>order by count desc</code></td>
</tr>
</tbody>
</table>
Report syntax examples

SQL statements to retrieve data from tables and columns (basic)

<table>
<thead>
<tr>
<th>SQL Statement</th>
<th>Syntax</th>
<th>Example Statement</th>
<th>Example Result or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELECT</td>
<td><code>SELECT column_name(s)</code></td>
<td>select Name from application</td>
<td>Use SELECT to get the data in one or more columns of a table.</td>
</tr>
<tr>
<td></td>
<td>FROM table_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SELECT *</td>
<td><code>SELECT *</code></td>
<td>select * from ADGroup</td>
<td>Use SELECT to get all records from a table.</td>
</tr>
<tr>
<td></td>
<td>FROM table_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SELECT DISTINCT</td>
<td><code>SELECT DISTINCT column_name(s)</code></td>
<td>select distinct ApplicationName from Event</td>
<td>Use SELECT DISTINCT to return just the values that are unique (distinct). Duplicate values are ignored.</td>
</tr>
<tr>
<td></td>
<td>FROM table_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNION (ALL)</td>
<td><code>SELECT column_name(s)</code></td>
<td>select * from ADGroup</td>
<td>Use the UNION statement to combine result sets of two or more SELECT statements. Only distinct values are returned. To return all values, including duplicate values, use UNION ALL.</td>
</tr>
<tr>
<td></td>
<td>FROM table_name1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>UNION</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>SELECT column_name(s)</code></td>
<td>select * from ADGroup</td>
<td>Use the UNION statement to combine result sets of two or more SELECT statements. Only distinct values are returned. To return all values, including duplicate values, use UNION ALL.</td>
</tr>
<tr>
<td></td>
<td>FROM table_name2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SQL components to specify conditions

<table>
<thead>
<tr>
<th>SQL Statement</th>
<th>Syntax</th>
<th>Example Statement</th>
<th>Example Result or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND / OR</td>
<td><code>SELECT column_name(s)</code> FROM table_name WHERE condition AND/OR condition</td>
<td>select WhenOccurred, FailUserName, FromIPAddress from event where Event_Type = 'Cloud.Core&gt;LoginFail' and when_Occurred &gt;= DateFunc('now','-30')</td>
<td>Use AND to combine conditions - results display if the database record meets both conditions. Use OR to show results that meet either the first or second condition.</td>
</tr>
<tr>
<td>BETWEEN (advanced)</td>
<td><code>SELECT column_name(s)</code> FROM table_name WHERE column_name BETWEEN value1 AND value2</td>
<td>select OSVersion, Count(*) as Count from device where InternalDeviceType = 'I' and OSVersion BETWEEN '6' and '7' group by osversion order by count desc</td>
<td>Use BETWEEN to select results that are within a specified range.</td>
</tr>
<tr>
<td>SQL Statement</td>
<td>Syntax</td>
<td>Example Statement</td>
<td>Example Result or Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------</td>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td><strong>IN / NOT IN</strong></td>
<td><code>SELECT column_name(s) FROM table_name WHERE column_name IN (value1,value2,...)</code></td>
<td><code>SELECT UserName, DisplayName, LastLogin from User where username not in (select NormalizedUser from Event where EventType = 'Cloud.Core&gt;Login' and WhenOccurred &gt;= DateFunc('now', '-30'))</code></td>
<td>Use IN to select results where a column name is one of a specified list of values (or not).</td>
</tr>
<tr>
<td><strong>LIKE</strong></td>
<td><code>SELECT column_name(s) FROM table_name WHERE column_name LIKE pattern</code></td>
<td><code>SELECT * from Users where username like 'j%'</code></td>
<td>Use LIKE to select results that match a specified pattern. Use % to indicate the pattern. Use _ (underscore) for a single character.</td>
</tr>
<tr>
<td><strong>CASE</strong></td>
<td><code>CASE when... then, end</code></td>
<td><code>CASE(InternalDeviceTyp e) WHEN 'I' THEN 'iOS' WHEN 'M' THEN 'Mac' WHEN 'A' THEN 'Android' WHEN 'W' THEN 'Windows' END as Platform, Count(*) as Count from device GROUP BY InternalDeviceType ORDER BY Count desc</code></td>
<td>Use CASE when you want to do an if/then/else statement. You can specify to have the base expression evaluated once or multiple times.</td>
</tr>
<tr>
<td><strong>WHERE</strong></td>
<td><code>SELECT column_name(s) FROM table_name WHERE column_name operator value</code></td>
<td><code>SELECT ApplicationName as Name, count(*) as Count from Event where WhenOccurred &gt;= DateFunc('now', '-30') and EventType='Cloud.Saas. Application.AppLaunch' group by name order by count desc</code></td>
<td>Use WHERE to specify the condition, such as a column name value.</td>
</tr>
</tbody>
</table>
### SQL components to specify sorting, displaying, grouping

<table>
<thead>
<tr>
<th>SQL Statement</th>
<th>Syntax</th>
<th>Example Statement</th>
<th>Example Result or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AS (alias)</strong></td>
<td><code>SELECT column_name AS column_alias FROM table_name</code> or <code>SELECT column_name FROM table_name AS table_alias</code></td>
<td><code>select Carrier, count(*) as Count from device group by Carrier</code></td>
<td>Use AS if you want to provide a different label for a column in the report results.</td>
</tr>
<tr>
<td><strong>GROUP BY</strong></td>
<td><code>SELECT Carrier, count(*) AS Count from device GROUP BY Carrier</code></td>
<td></td>
<td>Use GROUP BY to organize the report results by a specified column value.</td>
</tr>
<tr>
<td><strong>ORDER BY</strong></td>
<td>`SELECT column_name(s) FROM table_name ORDER BY column_name [ASC</td>
<td>DESC]`</td>
<td><code>select Name, Count(*) as Count from InstalledApp group by name order by count desc</code></td>
</tr>
</tbody>
</table>

### SQL Function examples

<table>
<thead>
<tr>
<th>SQL Statement</th>
<th>Syntax</th>
<th>Example Statement</th>
<th>Example Result or Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HAVING</strong></td>
<td><code>SELECT column_name, aggregate_function(column_name) FROM table_name WHERE column_name operator value GROUP BY column_name HAVING aggregate_function(column_name) operator value</code></td>
<td></td>
<td>Use HAVING to specify conditions when using SQL aggregate functions. (Use instead of WHERE for aggregate functions.)</td>
</tr>
<tr>
<td><strong>AVG()</strong></td>
<td><code>SELECT AVG(column_name) FROM table_name;</code></td>
<td></td>
<td>Use AVG() to calculate the average value of the non-null records in the specified column.</td>
</tr>
<tr>
<td>SQL Statement</td>
<td>Syntax</td>
<td>Example Statement</td>
<td>Example Result or Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>COUNT()</td>
<td><code>SELECT COUNT(column_name)</code> <code>FROM table_name;</code></td>
<td><code>select ApplicationName as Name, count(*) as Count from Event where WhenOccurred &gt;= DateFunc('now', '-30') and EventType='Cloud.Saas.Application.AppLaunch' group by name order by count desc</code></td>
<td>COUNT (Column_name) returns the number of non-null values in the specified column. COUNT (*) returns the number of records in a table. COUNT (Distinct column_name) returns the number of distinct values in the specified column.</td>
</tr>
<tr>
<td>MAX()</td>
<td><code>SELECT MAX(column_name)</code> <code>FROM table_name;</code></td>
<td></td>
<td>Use MAX() to return the maximum value of all values in the group. use MIN() to return the minimum, non-null value of all values in the group. The results include null values only if there are no non-null values.</td>
</tr>
<tr>
<td>MIN()</td>
<td><code>SELECT MIN(column_name)</code> <code>FROM table_name;</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Configuring Samsung service settings

You use the Admin Portal Settings page to configure the following Samsung service options. Before you develop your Samsung service deployment plan, review these options. Some of them may be necessary to support certain mobile devices (for example, the Apple Push Notification Service certificate for iOS devices and Samsung Knox Workspace license key for Samsung Knox Workspace devices) while others are optional (Account Customization and Exchange ActiveSync Server Settings).

Modifying a setting requires specific Admin Portal administrative rights. The third column lists the required rights. To learn more about the roles and rights required to make these changes see “Assigning applications to and removing them from roles” on page 251.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Why you use this setting</th>
<th>Role or rights needed to modify these settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Customization</td>
<td>Customize the user portal and Admin Portal login prompts and email messages to incorporate your organizations brand and logos. See “Customizing Samsung service user interfaces” on page 291.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>ActiveSync Device Quarantining</td>
<td>Configure the Samsung service to block email access for devices that are not enrolled. See “Enabling email quarantining” on page 325.</td>
<td>Device Management rights or Sysadmin role</td>
</tr>
<tr>
<td>Android for Work</td>
<td>Android for Work specific settings, such as domain mapping. See “Mapping Domains” on page 142.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>APNS Certificate</td>
<td>Get an Apple Push Notification Service (APNS) certificate so users can enroll iOS-based devices. See “Generating an APNS certificate” on page 332. Notes: * You must upload an APNS certificate to Admin Portal before users can enroll these devices. * If the certificate expires, users cannot enroll devices and enrolled iOS devices have service restrictions.</td>
<td>Device Management rights or Sysadmin role</td>
</tr>
<tr>
<td>Apple Configurator</td>
<td>Install a base security policy on iOS devices to pre-configure the mobile device manager and simplify device enrollment. See “Using Apple Configurator to mass deploy iOS devices” on page 327.</td>
<td>Device Management rights or Sysadmin role</td>
</tr>
<tr>
<td>Apple DEP Configuration</td>
<td>Add your Samsung service account as an MDM server in the Apple Device Enrollment Program, upload token, and set the initial enrollment profile. See “Linking to the Apple Device Enrollment Program” on page 340.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Setting</td>
<td>Why you use this setting</td>
<td>Role or rights needed to modify these settings</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Authentication Profiles</td>
<td>Define the required authentication mechanisms such as password, email confirmation code, mobile authenticator, etc. You use the authentication profile when you create your authentication rule. See “Creating authentication profiles” on page 30.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Admin Portal</td>
<td>Display the list of Samsung SDS IAM &amp; EMM connectors, configure Integrated Windows Authentication settings, and add or delete a Samsung SDS IAM &amp; EMM connector. See “Configuring connectors” on page 296.</td>
<td>Sysadmin role to modify all settings Register proxies permission to add a connector</td>
</tr>
<tr>
<td>Corporate IP Range</td>
<td>Specify the public IP addresses you want to include within the corporate intranet. The Samsung service uses these addresses for Integrated Windows Authentication and application multifactor authentication. See “Setting Corporate IP ranges” on page 343.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Corporate-owned Devices</td>
<td>Import serial numbers of enrolled devices to convert the ownership attribute from Personal Owned to Corporate Owned. See Tag devices as corporate owned.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Device Policy Management</td>
<td>Select either Active Directory group policy or the Samsung SDS IAM &amp; EMM policy service as the source for mobile device policies. If you use the Samsung SDS IAM &amp; EMM policy service you also use this tab to select the default Active Directory certificate service or the Samsung SDS IAM &amp; EMM CA to generate user certificates. See “Selecting the policy service for device policy management” on page 345.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Add LDAP or Google as your directory service and view existing configured directory services. See “Adding LDAP as a directory service” on page 309. See “Adding Google as a directory service” on page 311.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>External Users</td>
<td>Allow your customers to use their social media credentials for single sign-on access to applications. See “Managing social login users” on page 317.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Idle User Session Timeout</td>
<td>Enable a timeout and set the time period to log out inactive users from Admin Portal and Samsung SDS IAM &amp; EMM user portal. See “Enabling automatic log out from the Samsung SDS IAM &amp; EMM user portal and Admin Portal” on page 336.</td>
<td>Sysadmin role</td>
</tr>
<tr>
<td>Licenses</td>
<td>View your Samsung Knox licenses and add to them. See “Managing your Samsung KNOX licenses” on page 335</td>
<td>Sysadmin role</td>
</tr>
</tbody>
</table>
## Chapter 24 • Configuring Samsung service settings

### Login suffix
- **Why you use this setting:** Create a list of the login suffixes (the name that follows @ in the full user name) that users enter to log in to Admin Portal and the Samsung SDS IAM & EMM user portal and enroll devices. Users that do not have a login suffix in this list cannot log in to the portals or enroll a device.
- **See:** “Using login suffixes” on page 337.
- **Role or rights needed to modify these settings:** Sysadmin role

### Mobile Device Management
- **Why you use this setting:** If you select the Samsung service for mobile device management and you have devices that have the Universal Mobile Device Management Client (UMC), you can also enable a service that synchronizes the login suffixes you create with the Samsung Enterprise Gateway.
- **See:** “How to configure Mobile Device Management or single sign-on only” on page 18
- **Role or rights needed to modify these settings:** Sysadmin role

### OATH Tokens
- **Why you use this setting:** You can authenticate the Samsung SDS IAM & EMM identity service using your existing third-party OATH tokens (for example, those generated by a YubiKey) by bulk uploading those tokens. Samsung SDS IAM & EMM identity service uses those tokens to generate one-time passcodes (OTP) that users with enrolled devices can immediately use to log in to the Samsung SDS IAM & EMM user portal.
- **See:** “Importing OATH tokens in bulk” on page 353.
- **Role or rights needed to modify these settings:** Sysadmin role

### Partner Management
- **Why you use this setting:** Allows you to add business partners so that you can share your Samsung (Samsung SDS IAM & EMM User Suite) with your partners. Partner federation is achieved through SAML, where your server serves as the host (the Service Provider in SAML terms), and your business partners access the service and its associated resources by passing a SAML token obtained from their Identity Provider (IDP).
- **See:** “Managing Business Partner Federation” on page 312.
- **Role or rights needed to modify these settings:** Sysadmin role

### Provisioning
- **Why you use this setting:** Run application user provisioning synchronization, configure the provisioning report options, and specify daily synchronizations.
- **See:** User provisioning overview in the Application Configuration help for the details.
- **Role or rights needed to modify these settings:** Sysadmin role

### RADIUS Connections
- **Why you use this setting:** Allows you to configure your RADIUS clients/servers. You can use the Samsung SDS IAM & EMM connector as a RADIUS server for clients that support RADIUS authentication, such as VPNs. Additionally, you can configure RADIUS server settings to allow third-party RADIUS authentication.
- **See:** “Configuring Samsung SDS IAM & EMM RADIUS Support” on page 298.
- **Role or rights needed to modify these settings:** Sysadmin role
<table>
<thead>
<tr>
<th>Setting</th>
<th>Why you use this setting</th>
<th>Role or rights needed to modify these settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Settings</td>
<td>Define security related settings such as securely capture users' passwords at login or enabling forgotten username self-service. See <a href="#">Managing security settings</a> for more information.</td>
<td>Sysadminrole</td>
</tr>
</tbody>
</table>
| Tenant URLs    | Create a URL that is specific to your company so that your users can easily remember the Samsung service URL. Any existing URLs will be redirected to the one marked “Default URL”.  
URLs requirements”  
• Always begin with an alphabet  
• Maximum of 63 characters  
• Can only contain alphabets, numbers, and dashes (-) | Sysadmin role                                  |
Customizing Samsung service user interfaces

You use the Account Customization option to change the background color and images displayed in your organization's Samsung SDS IAM & EMM user portal and Admin Portal login prompts. In addition, you use this tab to specify the company name in your organization's implementation of the Samsung SDS IAM & EMM clients and specify the welcome screen text and company logo displayed when a user enrolls an iOS device.

You can restore the defaults for most options by clicking the Reset button. The exception is the Account Name field—Reset does not change this field’s contents.

Note The first time a user logs in to the user portal or Admin Portal, the default colors might be displayed. However, as soon as they complete user authentication—and in each subsequent login—the customized colors and images are displayed.

The following properties are available for customizing:

<table>
<thead>
<tr>
<th>Property</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Options</td>
<td><strong>Portal ribbon color</strong> Set the color for the narrow banner across the top of the login prompts. Enter the color’s hexadecimal color number or use the Select Color drop-down list to specify the color. Do not use RGB values to specify the color.</td>
</tr>
<tr>
<td>Login Image</td>
<td>Change the image that appears in the login prompts. Click the Browse button to select the image file. The image size is 137 pixels wide by 35 pixels high. Admin Portal automatically scales the image you upload to these dimensions, using the height as the base property. If your image cannot be scaled down exactly to 137x35, Admin Portal crops the width to be consistent with the equivalent aspect ratio.</td>
</tr>
<tr>
<td>Portal Image</td>
<td>Change the image in the user portal and Admin Portal banners. Click the Browse button to select the image file. The image size is 160 pixels wide by 36 pixels high. Admin Portal automatically scales the image you provide to these dimensions, using the height as the base property. If your image cannot be scaled down exactly to 160x36, Admin Portal crops the width to be consistent with the equivalent aspect ratio.</td>
</tr>
<tr>
<td>User Name Hint Text at Login</td>
<td>Change the hint text associated with the user name login text box. Click the associated Reset button to use the default hit text.</td>
</tr>
<tr>
<td>Device Enrollment options</td>
<td><strong>Welcome Text</strong> Enter the text to display in the welcome screen when a user enrolls an iOS device. The text is only displayed in the iOS version of the Samsung SDS IAM &amp; EMM client when the user enrolls the device. The Welcome Text is not used when users enroll an Android device.</td>
</tr>
</tbody>
</table>
To configure the Admin Portal and the User Portal windows and portal login screens:

1. In Admin Portal, click **Settings**, **Customization**, and **Account Customization**.
2. Select the Portal Ribbon Color.
   - To select a specific color, enter the color’s hexadecimal color code. Do not enter the color’s RGB value.
   - To use a pre-configured color, click the Select Color drop-down list and select the color.
3. Browse to and select the image file for the Login Image and click **Open**.
4. Browse to and select the image file for the Portal Image and click **Open**.
5. Set the company name displayed in the Samsung SDS IAM & EMM client home screens.
   - In the **Company Name** field, enter the name you want to appear.
6. Click **Save** to exit.

### Configuring the Admin Portal and Samsung SDS IAM & EMM User Portal login screens

<table>
<thead>
<tr>
<th>Property</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td>Enter the name of your organization as you want it to appear on the Samsung SDS IAM &amp; EMM client. The Account Name is displayed just above the user name in the application’s home screen.</td>
</tr>
<tr>
<td>Company logo</td>
<td>Browse to and select the logo displayed on the welcome screen when the user enrolls an iOS device. Admin Portal automatically scales the image you provide to a square. If the image is not square, it crops the image from the left side, removing pixels from the right side. The company logo is not used when the user enrolls an Android device.</td>
</tr>
</tbody>
</table>
| Email customization   | **MFA Challenge**  
|                       | **Device Enrollment**  
|                       | **Bulk User Import Report**  
|                       | **Invite User**  
|                       | **Invite User with OTP**  
|                       | **Directory**  
|                       | **Synchronization Report**  
| Email                 | **Company logo**  
|                       | Browse to and select the logo displayed in the email messages.                                                                                                                                              |

**Property**

- **MFA Challenge**
- **Device Enrollment**
- **Bulk User Import Report**
- **Invite User**
- **Invite User with OTP**
- **Directory**
- **Synchronization Report**

**To do this**

- Click the option to modify the letter sent for each communication with end users.
Configuring the device welcome and home screens

To configure the device’s welcome screen properties and home screen company name:

1. In Admin Portal, click **Settings, Customization, and Account Customization**
2. Enter the text that you want to appear in the welcome text in the Samsung SDS IAM & EMM client when the user enrolls the device.
   You can enter up to 2048 characters.
3. Fill in the **Company Name** field with the name you want displayed in the home screen in the Samsung SDS IAM & EMM client.
4. Browse to and select the image file for the Company Logo and click **Open**.
5. Click **Save** to exit.

Customizing the email messages contents and logos

The Samsung service uses email messages to simplify login and device enrollment for users. In addition, it sends an email after you use bulk enrollment or directory synchronization to indicate the results. You can customize the wording and styles for all of these email messages.

To modify a message scroll down to **Email Customization** and double-click the template. The pop up window has two tabs:

- **Preview**: Shows the message as it will appear to the reader.
- **Script Editor**: Contains the html tags and content. Use this tab to change the wording and modify the text styles.
  Click **OK** to save your changes.

To restore the template to its original content, right-click the template and click **Reset**.
Click the **Browse** button underneath **Email Image** to upload a logo or other image to replace the `<img src>` in the template.
The templates are used for the following events:

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Used for this purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFA Challenge</td>
<td>An email message sent to users when they log in to the user portal or Admin Portal when you enable authentication policy controls and select “Email Confirmation code” as one of the multifactor authentication options (see “Authentication - Setting authentication policy controls” on page 193). When users get this email, they click “here” to supply the second factor and complete the log in. Do not change href='{AuthLink}'.</td>
</tr>
<tr>
<td>Device Enrollment</td>
<td>An SMS message sent to the user’s mobile phone number to help them enroll the device in the Samsung service when you Invite users and select “Send SMS invites for device enrollment” (see “Sending invitations to users” on page 110) When users get this message on their phone, the click the link to download and install the Samsung SDS IAM &amp; EMM client. Do not change {EnrollLink}.</td>
</tr>
<tr>
<td>Bulk User Import Report</td>
<td>An email message sent after a bulk enroll that indicates how many accounts were created out of the total requested and lists the names from the file for whom accounts could not be created (see “Bulk import user accounts” on page 8). Do not change {CreatedUsers}, {TotalUsers}, or {FailedSummary}.</td>
</tr>
<tr>
<td>Invite User</td>
<td>An email sent to the users you selected in the Invite users procedure to simplify logging in to the user portal (see “Sending invitations to users” on page 110). Note: This message is sent only to users who have an Active Directory/LDAP account. This message uses the user’s company account (that is, Active Directory/LDAP) credentials to authenticate the user. Do not change href='{LoginLink}'.</td>
</tr>
</tbody>
</table>
### Invite User with OTP

An email sent to the users you selected in the Invite users procedure to simplify logging in to the user portal (see “Sending invitations to users” on page 110). The user can also use this message to enroll a device.

Note: This message is sent only to users who have a Samsung directory account.

This message contains the users’ Samsung directory account name and uses it and a one-time passcode to authenticate the user. If the user chooses to enroll a device, the link takes them to the Add Device screen in the user portal.

Do not change the following:
- `login name: {UserName}`
- `href='{LoginLink}'`
- `href='{UploadLink}'`

### Directory Synchronization Report

An email message sent to the recipients specified in the Email address for report delivery field in the Admin Portal Settings > Provisioning page. The email includes information for new users or a change in status to existing users that are synchronized with the source directory for specified applications.

The email message is sent once a synchronization job is complete. The progress of the job can be viewed in the Job History page (Status column).

Do not change the following:
- `{ReportURL}`
- `{AllProvJobsURL}`
- `{PreviewReport}`

Also see Application Configuration Help for more information on synchronization job reports.
Configuring connectors

The Samsung SDS IAM & EMM connector tab lists the connectors you have installed. You right-click an entry to perform the following operations:

- Change the connector log file settings.
- Ping the connector. This confirms that the Samsung SDS IAM & EMM User Suite can communicate with the connector.
- Configure or disable the web server—see How to configure Integrated Windows authentication.
- Delete the connector—see “Deleting a Samsung SDS IAM & EMM connector” on page 296.

You also use this tab to initiate the procedure for adding a new connector—see How to install a Samsung SDS IAM & EMM connector.

The columns indicate the following:

<table>
<thead>
<tr>
<th>Column header</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung SDS IAM &amp; EMM connector</td>
<td>The name of the computer</td>
</tr>
<tr>
<td>Forest</td>
<td>The domain name for the domain controller to which the connector is joined.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the connector software. You can configure the connector to update automatically—see “Configuring the connector to install updates automatically” on page 374</td>
</tr>
<tr>
<td>Last ping</td>
<td>The last time the Samsung service successfully pinged the connector.</td>
</tr>
<tr>
<td>Hostname</td>
<td>The DNS short name. You can also enter a fully qualified domain name to the IE local intranet zone. See Configuring IWA to change this name.</td>
</tr>
<tr>
<td>Status</td>
<td>Active indicates that the Samsung SDS IAM &amp; EMM User Suite can communicate with the connector. Inactive indicates that the Samsung service cannot communicate with the connector.</td>
</tr>
</tbody>
</table>

Deleting a Samsung SDS IAM & EMM connector

You can delete an inactive connectors. You cannot delete an active connector. An inactive connector is one that is offline. To take a connector offline, open the Samsung SDS IAM & EMM connector configuration program on the computer, click the connector tab, and click Stop. When the connector is offline, there is no communication between it and the Samsung service.

To delete a connector, right click the listing and click Delete. Alternatively, you can click the check box and click Delete. The connector listing is removed from the page.
Deleting a connector removes the listing from the Admin Portal page. It does not, however, uninstall the Samsung SDS IAM & EMM connector software from the computer. You can re-activate the connector by re-registering it.
Configuring Samsung SDS IAM & EMM RADIUS Support

Samsung SDS IAM & EMM supports RADIUS in two ways. The first is to use the Samsung SDS IAM & EMM connector as a RADIUS server for clients that support RADIUS authentication, such as VPNs. Using Samsung SDS IAM & EMM User Suite with your RADIUS client, you can provide a second authentication layer for added security. For example, if a VPN concentrator uses RADIUS for authentication, you can configure email as a secondary authentication requirement. A typical work flow is when a RADIUS client (like a VPN server) uses the Samsung SDS IAM & EMM connector as a RADIUS server to authenticate an incoming user connection. Depending on the user type, the connector authenticates the credentials either through Active Directory or the Samsung SDS IAM & EMM User Suite and returns the authentication result to the RADIUS client. This diagram shows the work flow. See Configuring the Samsung SDS IAM & EMM connector for use as a RADIUS server for configuration details.

The second way to use RADIUS with Samsung SDS IAM & EMM is use your existing RADIUS server for user authentication into Samsung SDS IAM & EMM by defining the Samsung SDS IAM & EMM connector as a RADIUS client. When users attempt to log in to Samsung SDS IAM & EMM and selects an external RADIUS server as a multi-factor authentication (MFA) mechanism, we send the user credentials (username and passcode) to the connector, which validates them against the configured RADIUS server, and returns the result of that validation to Samsung SDS IAM & EMM. This diagram shows the work flow. See Configuring the Samsung SDS IAM & EMM connector for use as a RADIUS client for configuration details.
Configuring Samsung SDS IAM & EMM connector for use as a RADIUS server

To enable communication between your RADIUS client and the connector (acting as a RADIUS server), do the following:

1. Make configuration changes in Admin Portal to designate the connector as a RADIUS server, add the RADIUS client information, and define the requirement for a secondary authentication mechanism. See Configuring Admin Portal (connector as a RADIUS server).

2. Configure the RADIUS client (for example Cisco VPN, Juniper VPN, and Palo Alto VPN). See Setting up a RADIUS client for client configuration details.

Configuring Admin Portal (connector as a RADIUS server)

Make configuration changes in Admin Portal to designate the connector as a RADIUS server, define the RADIUS client information, and define the requirement for a secondary authentication mechanism.

To configure Admin Portal:

1. Log in to the Admin Portal and click Settings > Network > Samsung SDS IAM & EMM connector.

2. Select an existing connector or add a new one.

3. Click RADIUS.

4. Select the Enable RADIUS Server checkbox.

5. Provide the port number in which the Samsung SDS IAM & EMM connector talks to the Samsung service. The default port number is 1812.
6 Click Save.

7 Click Authentication > RADIUS Connections > Client tab > Add to configure your RADIUS client.

A RADIUS client can be VPN server, wireless access point, etc.

8 Enter the required information.

![RADIUS Client Settings](image)

The **Client Hostname or IP Address** field is expecting the hostname or IP address of the RADIUS client.

The **Client Secret** field is expecting a shared secret key for the RADIUS client and Samsung service. If you have entered a secret key on your RADIUS client, then enter that same key here. The keys must match to enable authentication. If you are creating a new secret key, best practices recommend 22 or more characters in length.

9 *(Optional)* The “Include new-line characters in the mechanism selection list prompt” option controls how the mechanism list is displayed. This screenshot below shows the list when this option is enabled.
This screenshot below shows the list when this option is disabled.

10 Click Save.

11 Click Policies and either select an existing policy set or add a new one.

12 Click User Security Policies > RADIUS.

13 Select Yes in the Allow RADIUS client connections dropdown.

   This setting allows users to authenticate with the RADIUS client.

14 Select the Require authentication challenge checkbox to require that users provide a secondary authentication mechanism to log in via the RADIUS client.

15 Select the authentication profile from the dropdown.
**Important:** We recommend that you select a profile where the first challenge is Password because the user prompt from the RADIUS client defaults to Username/Password, regardless of the authentication mechanism(s) you choose for the first challenge. If you select a profile where the first challenge is not Password, for example it is Mobile Authenticator, then users may not successfully authenticate with the RADIUS client because we are expecting a mobile authenticator code but users enter their username/password based on the UI prompt.

See “Creating authentication profiles” on page 30 for information on authentication profiles.

16 Click **Save**.

Next step: You now need to configure your RADIUS client. See **Setting up a RADIUS client**.

**Setting up a RADIUS client**

The steps for configuring a RADIUS client to work with the Samsung SDS IAM & EMM connector vary for each client. Refer to your RADIUS client documentation for the configuration procedure and guidelines.

At a high level, you consistently need the following information regardless of the RADIUS client device:

- IP address of the Samsung SDS IAM & EMM connector
- The secret key you provide to the RADIUS client and Admin Portal must match exactly

**Important:** For Open VPN, the Samsung SDS IAM & EMM connector only supports the PAP authentication method.

Below are configuration examples for Cisco VPN, Juniper VPN, and Palo Alto VPN.

**Configuring Cisco VPN**

This topic provides general instructions for enabling RADIUS authentication on a Cisco ASA device. Refer to the Cisco ASA documentation for more detailed information.

To configure RADIUS authentication on a Cisco ASA device:

1. On the Cisco ASDM for ASA interface, create an IP Name object for the target by doing the following:
   a. Navigate to **Firewall**, expand **Objects**, and select **IP Names**.
   b. Click **Add** and enter a descriptive name (for example, Samsung SDS IAM & EMM RADIUS), the IP address of the Samsung SDS IAM & EMM connector, and a description (for example, Samsung SDS IAM & EMM RADIUS Bridge).
   c. Click **OK** then **Apply**.

2. Create a AAA server group by doing the following:
   a. Click **Remote Access VPN**.
b Click **AAA Setup, AAA Server Group**, then **Add**.

c Enter a server group name, for example “Samsung SDS IAM & EMM”.

d Confirm that the RADIUS protocol is selected.

e Accept the default for the other settings and click **OK**.

3 Add the RADIUS server to the server group by doing the following:

a Select the newly created server group.

b Click **Add**.

c Under the Interface Name, select the interface on the ASA that will have access to the RADIUS server.

d Under "Server Name or IP Address" enter the IP Name you created for the RADIUS server (i.e. Samsung SDS IAM & EMMRADIUS).

e In the Server Secret Key field, enter the secret key that you entered in the Samsung SDS IAM & EMM Admin Portal interface.

f In the Common Password field, re-enter the pass phrase/secret key.

g Accept the default for the other settings and click **OK**.

### Configuring Juniper VPN

This topic provides general instructions for enabling RADIUS authentication on a Juniper device. Refer to the Juniper VPN documentation for more detailed information.

To configure RADIUS authentication on a Juniper device:

1 Open the Juniper Secure Networks Secure Access SSL-VPN Central Manager.

2 Navigate to **Authentication, Authentication Servers, New RADIUS Authentication Server**.

3 Provide the following information:

   - Name: Descriptive name such as Samsung SDS IAM & EMMRADIUS.
   - NAS-Identifier: Descriptive name such as Juniper.
   - Radius Server: IP address of the Samsung SDS IAM & EMM connector.
   - Authentication port: 1812
   - Shared Secret: The secret key that you entered in the Samsung SDS IAM & EMM Admin Portal interface.
   - NAS-IP-Address: IP address of the Juniper device.
   - Timeout: 15 seconds
   - Retries: 0
   - Users authenticate using tokens or one-time password: leave unchecked.

4 Click **OK**.
5 Click **Add Custom RADIUS Challenge Rules** and provide the following information:
   - Incoming Packet Type: Access-Challenge
   - Reply-Message - matches the expression: (.*)
   - Show GENERIC LOGIN page: Enable the checkbox

6 Click **OK**.

7 Set up the same rule for the Access Reject packet type.

8 When you are done configuring the authentication rules, they should look similar to the following:
   - rule_1 - Access Challenge - (Reply-Message matches the expression "(.*)")
   - rule_2 - Access Reject - (Reply-Message matches the expression "(.*)")

**Configuring Palo Alto Networks**

This topic provides general instructions for enabling RADIUS authentication on a Palo Alto Networks device. Refer to the Palo Alto Networks VPN documentation for more detailed information.

To configure RADIUS authentication on a Palo Alto Networks device:

1 Open the Palo Alto Networks administration interface.

2 Navigate to **Device, Server Profiles, RADIUS**.

3 Click **Add** to add a new RADIUS server profile.

4 Provide the following information:
   - Name: Enter a descriptive name, such as Samsung SDS IAM & EMMRADIUS.
   - Timeout: 10
   - Retries: 0

5 Click **Save**.

6 Navigate to **Servers** and click **Add** to add a RADIUS server.

7 Provide the following information:
   - Server: Enter Samsung SDS IAM & EMMRADIUS.
   - IP Address: The IP address of the Samsung SDS IAM & EMM connector.
   - Secret: The secret key that you entered in the Samsung SDS IAM & EMM Admin Portal interface.
   - Port: 1812

8 Click **Save**.
9 Navigate to Device, Authentication Profile.

10 Click New to add a new authentication profile.

11 Provide the following information:
   - Profile Name: Enter Samsung SDS IAM & EMM RADIUS.
   - Authentication: RADIUS
   - Server Profile: Enter Samsung SDS IAM & EMM RADIUS.

12 Click Save.

13 Navigate to Network, SSL-VPN to configure your VPN with Samsung SDS IAM & EMM.

14 Edit your VPN profile or create a new one.

15 Set the Authentication Profile to “Samsung SDS IAM & EMM RADIUS”.

16 Click Save.

17 Click Commit to apply the new configurations.

Configuring the Samsung SDS IAM & EMM connector for use as a RADIUS client

You can use your existing RADIUS server for user authentication into Samsung SDS IAM & EMM by enabling communication between your RADIUS server and the Samsung SDS IAM & EMM connector (acting as a RADIUS client). The high level steps are:

1 Configure the RADIUS server to recognize the connector as a valid RADIUS client. See Configuring a RADIUS server.

2 Make configuration changes in Admin Portal to add the RADIUS server information, designate the connector as a RADIUS client, and define your authentication requirements to include RADIUS. See Configuring Admin Portal (connector as a RADIUS client).

Configuring a RADIUS server

You configure the RADIUS server to recognize the connector as a valid RADIUS client. The following RADIUS server configuration procedures use the RSA Authentication Manager’s RADIUS interface as an example. Your procedure will differ slightly if you are using a different RADIUS server.

At a high level, you consistently need the following information regardless of the RADIUS server:

- IP address of the Samsung SDS IAM & EMM connector
- The secret key you provide to the RADIUS server and Admin Portal must match exactly
To configure the RADIUS server (using the RSA Authentication Manager’s RADIUS interface):

1. Log in to the Authentication Manager Security Console with “SuperAdmin” or “Auth Mgr Radius Admin” rights.
2. Click **RADIUS Clients > Add New** in the RADIUS area.
3. Provide the required information.
4. Click **Save and Create Associated RSA Agent**.

**Configuring Admin Portal (connector as a RADIUS client)**

Make configuration changes in Admin Portal to add the RADIUS server information, designate the connector as a RADIUS client, and define your authentication requirements to include RADIUS.

To configure the connector and other Admin Portal settings:

1. Log in to Admin Portal.
2. Click **Settings > Authentication > RADIUS Connections > Servers > Add** to define the RADIUS server information.

   The server name will be displayed to users as one of their MFA mechanism options.

   **Note** The Server Secret field is asking for the secret that is shared between the RSA server and Samsung service. If you have entered a secret key on your RADIUS server, then enter
that same key here. The keys must match to enable authentication. If you are creating a new secret key, best practices recommend 22 or more characters in length.

3 Click **Save**.

4 Click **Network > Samsung SDS IAM & EMM connector** > select an existing connector or add a new one.

   The Samsung SDS IAM & EMM connector Configuration page opens.

5 Click **RADIUS** and select the **Enable RADIUS Client** checkbox to configure the connector for use as a RADIUS server.

6 (Optional) Select **Override server secret for this connector** checkbox.

   If you do not want all your proxies to have the same shared secret, you can override the secret here and enter a different secret.

7 Click **Save**.

8 Click **Policies** and either select an existing policy set or add a new one.
9 Click **User Security Policies > RADIUS**.

10 Select **Yes** in the Allow 3rd Party RADIUS Authentication dropdown.

   This setting allows users to authenticate using the RADIUS server.

11 Click **Save**.

12 Define your authentication requirements to specify when and under which conditions your users will authenticate using the RADIUS server. See How to define authentication requirements. Users will not be able to authenticate using the RADIUS server until you define the authentication requirements.

Users can now log in to Samsung SDS IAM & EMM by selecting the RADIUS server authentication method and entering the passcode generated by the RADIUS token container application -- which mirrors a hardware token or a token container running on a mobile device.
Adding LDAP as a directory service

LDAP communicates with the Samsung SDS IAM & EMM connector over TLS/SSL on port 636. As part of the client/server handshake between the connector and the LDAP server, the LDAP server must present the connector with an X.509 certificate. To establish a trust relationship between the connector and the LDAP server, you must install the CA certificate that issued the LDAP server’s Server Authentication certificate on the machine running the connector (specifically, the Local Computer Trusted Root Certification Authorities certificate store).

To add LDAP for the connector:

Possible Explanations
- The DNS name cannot be resolved by the machine.

Note: The Memory property is only available if the device was enrolled through the Mac cloud agent.

- There is no network route to the LDAP server from the Samsung SDS IAM & EMM connector machine, possible because of firewall rules or other routing issues.
- The LDAP server is not listening on port 636.

Verification Steps

Perform the following steps to verify the possible explanations:

1. From the Samsung SDS IAM & EMM connector machine, confirm that the DNS name can be resolved with nslookup.

2. If the above confirmation is successful, confirm that there is a network path to the LDAP server by telneting to it on port 636. If the screen goes blank, it means we can connect. Use `ctrl ]` and type `quite` to exit.

Solutions

Possible Explanations
- The DNS name cannot be resolved by the Samsung SDS IAM & EMM connector machine.
- There is no network route to the LDAP server from the Samsung SDS IAM & EMM connector machine, possible because of firewall rules or other routing issues.

If the name cannot be resolved, try to enter the name in the hosts table or use the IP address of the machine. If the latter, you will likely need to un-check Verify Server Certificate on the Add LDAP Directory page.

If the server is NOT listening on port 636, append the port to the DNS hostname; for example: `<dns hostname>:3269`
Adding LDAP as a directory service

Note: We only support LDAP over SSL. We do not support clear LDAP.
Adding Google as a directory service

If you are using the Google Apps for Work to store and manage your user information, you can configure the Samsung SDS IAM & EMM identity platform to recognize it as a directory service.

To add Google Apps for Work as a directory service:

1. Log in to Admin Portal as a system administrator, click **Settings, Users, Directory Service, Add Google Directory**.
2. Click **Authorize** and enter your Google Apps for Work administrator credentials.
3. (Optional) Click **Add** to enter a redirect URI if you want your users to use a more recognizable URI that is specific to your organization.
4. Click **Save**.
Managing Business Partner Federation

Business Partner Federation establishes a trust relationship between the Service Provider (SP) and Identity Provider (IDP) using SAML tokens. By establishing this trust relationship, you can provide access to the resources that you want to share. There are two use cases for Business Partner Federation.

**Use case 1:**

In this use case, you share your Samsung tenant (Samsung SDS IAM & EMM User Suite) with your business partners. Your Samsung tenant (which hosts the services) serves as the SP and your partner serves as the IDP. Your business partners access the tenant and its associated resources by passing a SAML token obtained from their IDP service. This use case applies to any IDP (ADFS or other kinds of IDPs).

**Use case 2:**

In this use case, you share a third party's services with your partners. Your Samsung tenant serves as the IDP and your partner serves as the SP. Your business partners access the third party's services by passing a SAML token obtained from the Samsung tenant.
Responsibilities

Partners are responsible for the following:

- Providing you with their IDP metadata.
- Providing you with the group attribute value(s) that they will pass in their SAML tokens. See “Understanding group attribute values to roles mapping” on page 314.
- Configuring their IDP to pass SAML tokens to you:
  - If your partner is using an external IDP, see our support Knowledge Base article for ADFS configuration information.
  - If your partner is using another Samsung tenant, they can easily do this by deploying the Samsung B2B SAML application. See Creating a Custom SAML application.

Service Providers (SPs) are responsible for the following:

- Providing the SP metadata to your partner. See “Providing the Service Provider metadata” on page 316.
- Adding the partner in Admin Portal. See “Adding a partner” on page 314. You will need the IDP metadata and the group attribute value from your partner before you can complete this task.
- Assigning your groups to roles in Admin Portal. See “Assigning host groups to roles” on page 315.
• Mapping of the global group attribute (for all your partners) to your groups. See “Mapping of global group attributes” on page 315.

Understanding group attribute values to roles mapping

As part of managing their users, partners typically assign them role-based values (also known as group attribute values), such as Sales Managers, Service Managers, etc. However, we do not have visibility into their user directories and one partner may name the value "Sales Managers" while another partner may name it "SalesTeamManagers". To organize these group attribute values, we have created a group construct in the federated directory service. As the systems administrator in the host tenant, you can create host groups (for example "Mgrs-Sales" group) in which to map the group attribute values (for example the "Sales Managers" and "SalesTeamManagers" values). This host group can then be added to roles in your tenant. The diagram below demonstrates this flow.

Adding a partner

You add the partner in Admin Portal to enable sharing on your end. You will need the group attribute values and IDP metadata from your partner to finish the configuration.

To create a partner:

1. Log in to Admin Portal.
2. Click Settings, Users, Partner Management, Add.
3. Enter a unique partner name.
4. SAML 2.0 is automatically selected because we currently only support this federation type.
5. Click Add associated with the Domain Name field to enter a unique domain name.

This domain name will be used as the login suffix for all partner users. It allows Samsung to recognize users as coming from a specific IDP and redirects them accordingly. For example, you may want to use the business partner company name (for example companyABC.com) as the domain name.
6 Click **Add** to add the domain name to the table.

7 Click **Group Mappings, Add** to create a mapping of the group attribute values (i.e. partner roles for other Samsung tenants, or groups for partners using ADFS) to your groups.

8 Enter the partner role or ADFS group (ADFS federation) into the Group Attribute Value column, then either select an existing group in the Group Name column or enter a new name.

   You do this to map the partner roles/ADFS groups (information you should have received from your partner) to your groups. Each group needs to be a member of at least one role in your tenant. See “Assigning host groups to roles” on page 315.

9 Click Inbound Metadata to configure IDP settings (using the IDP metadata you received from your partner) for this partner using one of the following options:
   a Option 1: Upload the IDP configuration from URL. To use this option, paste the Identity Provider SAML Metadata URL provided by your partner.
   b Option 2: Upload IDP configuration from a file. If your partner provided the Identity Provider SAML Metadata in an XML file, you can upload it here.
   c Option 3: Manual Configuration. Manually enter the relevant information. This is not a recommended option.

**Assigning host groups to roles**

For the host groups (those listed in the Group Name column of the Settings, Users, Partner Management, Group Mappings page) to have access to relevant applications and rights, you need to assign them to the relevant roles.

To assign the groups to roles:

1 Log in to Admin Portal.

2 Click **Roles** and select an existing role or create a new one.

3 Click **Members, Add** and search for the group.

   In the Source area, you must have the FDS user source selected to see the federated users/groups. Groups from federated services have the icon/FDS label associated.

4 Select the group and click **Add**.

5 Click **Save**.

**Mapping of global group attributes**

You can create a mapping of global group attributes values (i.e. partner roles for Samsung SDS IAM & EMM tenants, or groups for partners using ADFS) for all your partners to your
specified groups. If the system encounters conflicts, the individual group attribute mapping takes priority.

To map global group attributes to your specified groups:

1 Log in to Admin Portal.
2 Click **Settings, Users, Partner Management, Global Mappings**.
3 Enter the global partner role or ADFS group (ADFS federation) into the Group Attribute Value text box, then either select an existing group in the Group Name text box or enter a new name.

You do this to map global partner roles/ADFS groups (information you should have received from your partners) to your groups. Each group needs to be a member of at least one role in your tenant. See “Assigning host groups to roles” on page 315.

4 Click **OK**.

**Providing the Service Provider metadata**

Provide your partner with your service provider metadata.

To get the service provider metadata:

1 Click **Settings** in Admin Portal.
2 Click **Users, Partner Management**.

If you have not started creating the partner profile, then click **Add** to access the necessary information. If you have an existing partner, you can look at that partner's information for the service provider metadata. This information stays consistent across all partners. In other words, you provide the same metadata information to all your partners.

3 Click **Outbound Metadata** and use one of the three options to get the metadata information.
Managing social login users

You can enable your external users (such as customers or temporary contractors) to use their existing social media credentials to access assigned applications via the Samsung SDS IAM & EMM user portal or your own portal. Additionally, you can customize the user experience by rebranding the access request page with our company name and logo.

When users access their application using the Samsung SDS IAM & EMM user portal, users can do the following:

- Access assigned applications
- Add applications to the Apps page
- View their account information and user portal activity history

When users log in, they are automatically added to the Everybody role and External Users group upon log in. This group can then be added to roles and you assign applications to the roles.

See “Configuring social media access without customized branding” on page 317 for information about using the Samsung SDS IAM & EMM user portal without your company branding.

See “Customizing the social login user experience” on page 317 for information about rebranding the access request page and redirecting users to your own portal.

Configuring social media access without customized branding

You can enable your external users to use their existing social media credentials for single-sign-on access to assigned applications via the Samsung SDS IAM & EMM user portal. These instructions do not include any customization or branding. Users will see the Samsung SDS IAM & EMM name and logo on the access request page.

To configure social media access to the Samsung SDS IAM & EMM user portal without customized branding:

1. Log in to Admin Portal and click Settings, Users, Social Login.
2. Select the social identity that you want users to have from the user portal.
3. Click Save.

Customizing the social login user experience

You can customize the social media log in experience by rebranding the access request page (see screenshot below) to display your company logo and name. Additionally, if your company has its own portal for application access, you can redirect users to that portal after they log in using their social media credentials.
Managing social login users

The high-level procedures for customizing the social media log in experience are:

1. Use the social media developer toolkit to create a social media application with your organization's branding. You need to create an application for each of the social identity that you want users to have access. Instructions differ based on the social identity:
   - Facebook -- See “Creating a Facebook application” on page 318.
   - Google -- See “Creating a Google application” on page 320.
   - LinkedIn -- See “Creating a LinkedIn application” on page 321.
   - Microsoft -- See “Creating a Microsoft application” on page 322.

2. Use Samsung SDS IAM & EMM Admin Portal to configure the integration to your social media application (for a branded access request page) and redirect to your company portal (if you have your own portal). See “Configuring the integration to your social media application” on page 323.

Creating a Facebook application

You need to create a Facebook application if you want users to see your company name and logo when they choose to log in using their Facebook credentials.

To create a Facebook application:

1. Create a Facebook account and log in.
2. Register as a developer if you have not done so.
4. Click My Apps and select Add a New App.
5. Click www Website, specify a name for the application, and click Create New Facebook App ID.
6. Select Skip and Create App ID.

The Create a New App ID page displays.
7 In the **Display Name** field, enter your company name.

This is the name that will appear on the access request page where it completes a sentence similar to “<Your company name> would like to access some of your Facebook information.”

8 Select **Productivity** in the **Category** drop down.

9 Click **Create App ID**.

The following configuration page displays:

10 Click **Settings** on the side panel.

11 On the **Basic** tab, specify the **Contact Email** and click **Save Changes**.

12 On the **Advanced** tab, enter your Samsung SDS IAM & EMM Identity Service pod URI into the **Valid OAuth redirect URIs** field and click **Save Changes**.

For example, enter `https://<pod_abcd>.centrify.com`.

13 Click **App Details** on the side panel.

14 Enter a description that includes your pod name in the **Short Description** field.

For example, *Company XYZ - Pod123*.

15 In the Contact Info section, enter your company information for the following:

- Privacy Policy URL -- For example `https://www.companyABC.com/privacy/`
- Terms of Service URL -- For example `https://www.companyABC.com/eula/`
- User Support URL -- For example `https://www.companyABC.com/support/`
- Marketing URL -- For example `https://www.companyABC.com/products/`

16 In the **Icons** section, upload your company logo using the appropriate size.

This logo will appear on the access request page when users log in.

17 Click **Save Changes**.

18 Click **Status & Review** on the side panel.

19 Toggle **Yes** for the “Do you want to make this app and all its live features available to the general public?” question.
20 Confirm the selection to make the application public.

21 Click Dashboard on the side panel.


You will need this information when you configure the integration to your social media application. See “Configuring the integration to your social media application” on page 323.

Creating a Google application

You need to create a Google application if you want users to see your company name and logo when they choose to log in using their Google credentials.

To create a Google application:

1 Create a Google account and log in.


   The Google Developers Console page displays.

3 In the Select a project drop down, select Create a project.

   The New Project page displays.

4 Enter a project name that includes your pod name.
   For example, Project XYZ · Pod123.

5 Respond to the other fields as appropriate.

6 Click Create.

   You must agree to the terms of service to enable this button.

7 Click the side panel expander icon (three stacked lines) to expand the side bar.

8 Click API Manager and Overview.

    The Overview page displays.

9 In the Social APIs section, click Google+ API.

10 Click Enable API.

11 Click Credentials in the side panel.

12 In the New Credentials drop down, select OAuth Client ID.

13 Click the Configure consent screen button.

14 In the Product name shown field, enter the your product/company name.
This is the name that will appear on the access request page where it completes a sentence similar to “<Your company name> would like to access some of your Google information.”

15 Enter your company URL into the **Homepage URL** field.

16 Enter the URL where your company logo resides.
   This logo will appear on the access request page when users log in.

17 Enter the Privacy policy URL and Terms of service URL for your company.

18 Click **Save**.

   The Create client ID page displays.

19 Select **Web application** as the application type.

20 Enter your Samsung SDS IAM & EMM Identity Service pod URI into the **Authorized redirect URIs** field and click **Create**.
   For example, enter `https://<pod_abcd>.centrify.com`.

   The OAuth client window displays.

21 Copy/paste the **Client ID** and **Client Secret** for future use in the Admin Portal.
   You will need this information when you configure the integration to your social media application. See “Configuring the integration to your social media application” on page 323.

### Creating a LinkedIn application

You need to create a LinkedIn application if you want users to see your company name and logo when they choose to log in using their LinkedIn credentials.

To create a LinkedIn application:

1 Create a LinkedIn account and log in.


3 Click **My Apps**.

4 Click **Create Application**.

5 Enter your company name.
   This is the name that will appear on the access request page where it completes a sentence similar to “<Your company name> would like to access some of your LinkedIn information.”

6 Enter your application name into the **Name** field.
7 Enter a description that includes your pod name in the Description field.
   For example, Company XYZ - Pod123.

8 Click the Select File to Upload button to upload your company logo.
   This logo will appear on the access request page when users log in.

9 Provide the remaining required information as appropriate.

10 Click Submit.
   The Test Applications page displays.

11 In the Default Application Permissions area, enable the r_basicprofile and
    r_emailadress check boxes.

12 Enter your Samsung SDS IAM & EMM Identity Service pod URI into the Authorized
    Redirect URLs field and click Add.
   For example, enter https://<pod_abcd>.centrify.com.

13 Click Update.

14 Copy/paste the Client ID and Client Secret for future use in the Admin Portal.
   You will need this information when you configure the integration to your social media
   application. See “Configuring the integration to your social media application” on
   page 323.

15 Click Settings in the side panel.

16 Select Live in the Application Status drop down.

17 Click Update.

Creating a Microsoft application

You need to create a Microsoft application if you want users to see your company name and
logo when they choose to log in using their Microsoft credentials.

Note: The first few steps of this procedure may vary if you already have a Microsoft account and
Windows Live ID.

To create a Microsoft application:

1 Create a Microsoft account and log in.


3 Read the information in the Before You Register section then click Register to obtain a
   Windows Live ID.

4 Click the application management site link in step 1 of the procedure.

5 Enter you application name.
This is the name that will appear on the access request page where it completes a sentence similar to “<Your company name> would like to access some of your Microsoft information.”

6 Set the language and click I accept.

The application configuration page opens.

7 Click Basic Information in the side panel.

8 Click the Browse button to upload your company logo.

This logo will appear on the access request page when users log in.

9 Enter the following URL information:
   • Terms of Service URL -- For example https://www.companyABC.com/eula/
   • Privacy URL -- For example https://www.companyABC.com/privacy/

10 Click Save.

11 Click API Settings in the side panel.

12 Enter your Samsung SDS IAM & EMM Identity Service pod URI into the Redirect URLs field and click Add.

   For example, enter https://<pod_abcd>.centrify.com.

13 Click Save.

14 Click App Settings in the side panel.

15 Copy/paste the Client ID and Client Secret for future use in the Admin Portal.

You will need this information when you configure the integration to your social media application. See “Configuring the integration to your social media application” on page 323.

Configuring the integration to your social media application

After you have created the social media applications, you now have the necessary information to configure the integration to those applications.

To configure the integration to your social media application:

1 Log in to Admin Portal and click Settings, External Users.

2 Select the social identity that you want users to have from the user portal.

3 Select the Use custom settings link associated with the relevant social identity.

   The <social identity> Custom Settings page opens.

4 Select the Use Custom Integration check box.
5 Enter the application ID from your social media application into the OAuth Application ID text box.

6 Enter the application secret from your social media application into the OAuth Application Secret text box.

7 Click Save.

If your company does not have its own portal for application access, then you are done.

If your company does have its own portal for application access, then continue to the next step.

8 (Optional) If your company has its own portal for application access, click Add in the “Additional OAuth Trusted Redirect URIs” to enter the redirect URI then click Add again.

This step is only required if your company has its own portal for application access and you want users to get redirected to this portal after they log in using their social media identity.

9 Click Save.
Enabling email quarantining

You use the ActiveSync Device Quarantining option to enable automatic quarantining of user accounts for iOS and Android devices when a device is not enrolled. While the device is quarantined, its user has limited access to the Exchange server account’s email, calendar, contacts, and Notes folders. When a device is enrolled, its user has full access to the folders.

The Samsung service uses the standard Quarantine and Allow List Exchange ActiveSync access states to block access except to those who enroll their device. When the device is enrolled, the connector adds it to the Allowed List; when the device is unenrolled, the connector removes it from this list. If you are unfamiliar with the quarantine and allow access states go to technet.microsoft.com for an introduction.

If you have multiple Exchange servers, you enable automatic quarantining on a server-by-server basis. As soon as you enable this feature on a server, account access from all of the mobile devices that use that Exchange server is blocked until users enroll their devices.

To specify an Exchange or Office365 server for quarantining:

1. Log in to Admin Portal and click Settings, Mobile, ActiveSync Device Quarantining, Add.
2. Select the either Exchange 2010 or Office365 as your server type.
3. Enter the host name (the URL for the Exchange Web Services endpoint for your server) for the connection endpoint.
   - For Exchange servers the connection endpoint has this form:
     https://<exchange_server_name>/PowerShell
   - For Office 365 the connection endpoint has this form:
     https://ps.outlook.com/PowerShell
4. Select the authentication type. Select Basic if you enabled Basic Authentication rather than Windows Authentication. (Office 365 always uses Basic Authentication.)
5. Enter the user name and password for an account that has permission to modify the Exchange or Office 365 server settings.
6. Click OK.

To manually remove a quarantine from an account:

1. Log in to the computer on which you installed the Samsung SDS IAM & EMM connector.
2. Find the device ID of the quarantined device.
   The device ID is generated by the mail client (for example, iOS Mail or Touchdown).
   You unblock a device by adding its device ID to a list of devices that are not quarantined.
   The following PowerShell script retrieves the device ID
Enabling email quarantining

Get-ActiveSyncDeviceStatistics -mailbox <username> | where {$_.DeviceAccessState -eq 'Quarantined'} | select DeviceID

3 Add the device ID to the list of devices that are allowed access.

Admin Portal quarantines all devices when you enable blocking except for those devices identified in -ActiveSyncAllowedDeviceIDs. Use the following PowerShell script to update the list.

Set-CasMailbox -identity <username> -ActiveSyncAllowedDeviceIDs <device IDs>

To specify multiple devices, separate each device ID with a comma.

To re-enable blocking, update the list again but remove the device ID.

Note This procedure is required for Exchange Servers only if you want to use the account quarantining feature. Quarantining blocks user access to the email account when the device is not enrolled in the Samsung service. See “Enabling email quarantining” on page 325 for the details. Skip this procedure if you do not plan to enable quarantining.

Blocking is available to Exchange 2010 and Office 365 servers. It is not available to Exchange 2007 servers. Exchanges 2010 servers must have SP1 installed.

You must enable Remote PowerShell on the Exchange or Office 365 server. After you enable Remote PowerShell, the Exchange server creates an Internet Information Services (IIS) application named PowerShell. You need to enable an authentication method for this application. (By default no authentication method is selected.) Use the following procedure to enable an authentication method for the PowerShell application.

To enable the authentication method for the PowerShell application:

1 Start IIS Manager.

2 On the left pane, select Site > Default Web Site > PowerShell.

3 On the right pane, select IIS > Authentication, right-click, click and select Open Feature.

4 Select either Windows Authentication or Basic Authentication, right-click, and select Enable.

   If you select Basic Authentication, be sure to select the check box when you enable the Exchange server in the Admin Portal settings.

5 Back up your original settings. In this case, you would use a PowerShell script to extract the original settings.
Using Apple Configurator to mass deploy iOS devices

You use the Apple Configurator option to preconfigure iOS devices with a base security policy before you distribute them to your users. The Apple Configuration page provides a wizard which builds iOS profiles that contain the base security policy settings and stores them in a zip file. You then import the zip file into Apple Configurator to install the profiles in the devices. During the profile installation process, the devices are also enrolled in the Samsung service.

See Apple Configurator Help for more information about this program.

Note This feature is available with a Premium or EMM license only. If you do not have either license, you cannot download the iOS device profile. If the license expires before the user personalizes a bulk-enrolled device, an error message is displayed to the user indicating that the license requirements have not been met.

When the user enrolls the device, the Samsung service installs additional profiles which contain the remainder of the policy settings for the device. If the user logs out of the Samsung service, the additional policy profiles are removed and only the base security policy profiles remain in place.

You create the full mobile device policy for the iOS devices before you use this wizard. You can use either the Active Directory Group Policy Object Editor to create a group policy object or Admin Portal to create a policy set. Which tool you use depends upon whether you use Active Directory or Samsung SDS IAM & EMM policy service to define the mobile device policies (see “Selecting the policy service for device policy management” on page 345). See “Common Mobile Settings” on page 378, “iOS Settings” on page 380, and “Additional iOS Settings” on page 383 for a summary of the mobile device policies for iOS devices. The Samsung service creates multiple profiles to install the full set of policies in the device. The profiles are listed in the device’s Settings > General > Profiles screen.

The Apple Configurator wizard builds the base security policy profiles from the passcode and restrictions policies from the group policy object or policy set you created. In addition, the base security policy profiles contain the wi-fi profiles you created in the Common Mobile Settings, excluding any WEP or WPA/WPA2 Enterprise profiles.

Notes

- Preconfiguring iOS devices is a Samsung service licensed feature. However, pre-configuring is also available for 30 days after receiving your customer ID during your Samsung SDS IAM & EMM User Suite evaluation period. If your license expires, you can no longer pre-configure iOS devices for bulk enrollment.

- When you receive preconfigured devices back from users, instruct them to click the Logout button on the Settings screen in the Samsung SDS IAM & EMM client. This removes the additional policy profiles installed when the user logged in. This process leaves the base security policy profiles installed using Apple Configurator in place.
The wizard’s user interface is different for Active Directory and Samsung SDS IAM & EMM directory services. The interface displayed depends upon whether you selected “Active Directory group policy” or “Samsung SDS IAM & EMM policy service” on the Device Policy Management page on the Settings page in Admin Portal (see “Selecting the policy service for device policy management” on page 345).

Download profiles from a group policy object

You use this procedure only if you are using Active Directory group policy for device policy management (see “Selecting the policy service for device policy management” on page 345). This procedure installs the base security policy profiles in the iOS devices from the group policy object linked to an organizational unit. Before you begin the procedure, do the following:

- Create an Active Directory organizational unit for these devices.
- Create the group policy object for these devices and link it to the organizational unit you created for these iOS device.
- Specify the organizational unit when you configure the device enrollment settings in the policy set for the iOS device users—see “Enabling users to enroll devices” on page 22.

To install the base security policy profiles:

1. Log in to Admin Portal and click Settings, Mobile, Apple Configurator.
2. In Step 1, select the organizational unit associated with the policy set for the role with the accounts for the users who will be enrolling the devices.
   The drop-down list contains only the organizational units you have specified in the the device enrollment settings.
3. Perform Step 2.
   Click Download to create and download the file mass_enrollment.zip containing the base security policy settings.
4. Unpack mass_enrollment.zip and transfer the files to a location from which you can import them into Apple Configurator.
5. Perform Step 3.
   Follow the Apple Configurator instructions to import the files and then use the Apple Configurator Prepare function to install the profiles in the devices.

After the profiles have been installed, each device initiates contact with the Samsung service to enroll the devices. When enrollment completes, the device is listed in the Active Directory organizational unit you selected and on the Devices page in Admin Portal. The computer object name in the Active Directory listing contains “companyOwned.”
6 When you hand over the devices, instruct the users to install the Samsung SDS IAM & EMM client and log in to the Samsung service to install the additional profiles with the remaining policy settings.

Download profiles from a Samsung SDS IAM & EMM policy service policy set

The following procedure installs the base security policy profiles in the iOS devices from the policy sets assigned to one or more roles. Before you begin the procedure, do the following:

- Create roles for all the users who will be enrolling these iOS devices and add the user accounts to the roles.
- Create one or more policy sets for these devices.
- Apply the policy set(s) to the role(s).

To install the base security policy:

1 Log in to Admin Portal and click Settings, Mobile, Apple Configurator.

2 In Step 1, select the role or roles that contain the accounts for the users who will be enrolling the devices.

3 Perform Step 2.
   
   Click Download to create and download the zip file mass_enrollment.zip containing the base security policy settings.

4 Unpack mass_enrollment.zip and transfer the files to a location from which you can import them into Apple Configurator.

5 Perform Step 3.
   
   Follow the Apple Configurator instructions to import the files and then use the Apple Configurator Prepare function to install the profiles in the devices.

   After the profiles have been installed, each device initiates contact with the Samsung service to enroll the devices. When enrollment completes, the device is listed on the Devices page in Admin Portal.

6 When you hand over the devices, instruct the users to install the Samsung SDS IAM & EMM client and log in to the Samsung service to install the additional profiles with the remaining policy settings.
Using DEP with Apple Configurator to mass deploy iOS devices

You can use Device Enrollment Program (DEP) with Apple Configurator to mass deploy iOS devices not purchased directly from Apple.

Before you start configuring Apple Configurator, confirm that you have the following:
- A MAC with Apple Configurator 2 or newer installed.
- An iOS device connected to the MAC.

To configure Apple Configurator for device enrollment:

1. On the MAC, run Apple Configurator.
2. Click Prepare on the All Device window.
   The Prepare iOS Devices window opens.
3. Select Manual in the Configuration drop down and click Next.
   The Enroll in MDF Serve window opens.
4. Select New Server in the Server dropdown and click Next.
   The Define an MDM Server window opens.
5. Enter your company name in the Name field.
6. Enter the Samsung SDS IAM & EMM specific URL (for example, //id.my.Samsung SDS IAM & EMM.com) in the Enrollment URL field.
7. Click Next.
8. The MDM server automatically provides an anchor certificate. You can add additional certificates if you want.
9. Decide if you want to supervise/manage the iOS device, then click Next.
   The Assign to Organization window opens.
10. Select your company name from the Organization drop down and click Next.
    The iOS Setup Assistant window opens.
11. Select the steps you want to skip during the device setup and click Prepare.
    Look at your attached iOS device. It begins to prepare.
12. Finish the configuration on the attached iOS device.

To finish the configuration on the iOS device:

1. Set the keyboard language and Wifi if required.
2 The DEP profile becomes available for installation.
3 Click **Apply Configuration** on the About page.
4 Provide your Samsung service credentials to log in.
   The DEP profile begins to install.
5 Accept the terms and conditions.
6 Verify that the MDM profile installs successfully on the iOS device.
Generating an APNS certificate

For the Samsung service to communicate securely with Apple iOS devices, both the Samsung service and the devices and computers need a trusted, SSL certificate that is signed by both Samsung service and Apple certification authorities. This certificate is called an *Apple Push Notification Service (APNS) certificate*. This section describes how to get this certificate and upload it to the Samsung service.

What to do before creating or updating an APNS certificate

To get your APNS certificate, you need to have the following:

- The proper Admin Portal permissions.
  
  Only the users who are authorized to manage enrolled devices can create or update APNS certificates. This includes administrators in the sysadmin role and roles that can manage devices.

- An Internet connection.

- An iTunes App Store Apple ID that can be used to obtain updated APNS certificates from Apple.
  
  You need to use this same Apple ID in the future to renew your APNS certificate. It might make future updates simplest if you create a generic Apple ID to use solely for APNS certificate creation.

How often you should create an APNS certificate

You need to create an APNS certificate once before users start enrolling devices. After that, you’ll need to renew it every year. You do not need to re-enroll devices after updating an APNS certificate. The expiration date for the APNS certificate you are using is listed at the top of the page.

You can find more information about APNS certificates on Apple’s website:


What happens when the APNS certificate expires

If the APNS certificate expires, users can no longer enroll devices. In addition, the services available to enrolled iOS devices is limited as follows:

- Users and administrators cannot send commands to the devices from the user portal and Admin Portal.

- Administrators cannot install native applications.

Initially, enrolled devices remain enrolled and Status in the user portal and Admin Portal shows Enrolled. In addition, users can open the Samsung SDS IAM & EMM client and launch the web applications with silent authentication. However, at the end of the ‘Mark
Generating an APNS certificate

You use Admin Portal to generate and download the Certificate Signing Request file, and then upload that file to the Apple Push Certificates Portal. Apple generates the completed APNS certificate, which you then upload to Admin Portal.

The following figure illustrates the procedure.

To create or update your APNS certificate for iOS devices:

1. In Admin Portal, click Settings, Mobile, APNS Certificate.

   If you haven’t yet uploaded an APNS certificate to the Samsung service, the expiration date at the top of the page appears as unconfigured.

2. Click Generate Request to create the Certificate Signing Request (CSR) file.

   Admin Portal downloads the CSR file—mdm_csr.pem—to your system. Depending on your web browser’s settings, your web browser may automatically save the file in a predetermined location or it may prompt you to save the file.

3. Create the APNS certificate:
Generating an APNS certificate

1. Click the link to https://identity.apple.com/pushcert and login to your Apple iTunes App Store account. This opens the Apple Push Certificates Portal. This page contains all of the APNS certificates you have created under this account.

2. Click Create a Certificate.

3. Read and accept the terms and conditions.

4. Click Choose File to select the Certificate Signing Request (mdm_csr.pem) file just generated and then Upload to import the file into the Apple Push Certificates Portal.

5. Click Download. Depending on your web browser’s settings, your web browser may automatically save the file in a predetermined location or it may prompt you to save the file. The certificate created by Apple is named MDM_Samsung Electronics Co., Ltd._Certificate.pem.

4. Click Upload Apple Response and select the APNS certificate just downloaded.

Renewing an APNS Certificate

The expiration date for an APNS certificate is shown at the top of the page. You can renew it any time before the expiration. The new certificate is valid for one year from the date of renewal.

To renew an APNS certificate:

1. In Admin Portal, click Settings, Mobile, APNS Certificate.

   Make note of the certificate’s expiration date. You will need this date when you renew the certificate on the Apple Push Certificates Portal.

2. Click Generate Request to create the Certificate Signing Request (CSR) file.

   Admin Portal downloads the CSR file—mdm_csr.pem—to your system. Depending on your web browser’s settings, your web browser may automatically save the file in a predetermined location or it may prompt you to save the file.

3. Click the link to https://identity.apple.com/pushcert and login to your Apple iTunes App Store account.

   This opens the Apple Push Certificates Portal. This page contains all of the APNS certificates you have created under this account.

4. Click Renew for the certificate with the expiration date that matches the date on the APNS Certificates page in Admin Portal.

5. Click Choose File to select the Certificate Signing Request (mdm_csr.pem) file just generated and then Upload to import the file into the Apple Push Certificates Portal.

6. Click Download. Depending on your web browser’s settings, your web browser may automatically save the file in a predetermined location or it may prompt you to save the
file. The certificate created by Apple is named
MDM_Samsung Electronics Co., Ltd._Certificate.pem.

7 Click **Upload Apple Response** and select the APNS certificate just downloaded.

The Current Expiration Date at the top of the page should show the new date.

**Managing your Samsung Knox licenses**

The Samsung Licenses page contains all of the Samsung Knox licenses you have purchased. The columns contain the license key, the date the license was issued, the date it expires, the total licenses purchased, the number of licenses in use (Activations), and the current state of the license key.

The license states are dependent upon the type of license:

- **Active**: License is validated with license server and available
- **De-active**: License is validate, however, it has been suspended. Registration on a new device is not allowed
- **Expired**: Contract expiration on license KLM server. Registration on a new device is not allowed
- **None**: Registration on a new device is not allowed
- **Terminated**: License period has expired and the license is no longer available. Registration on a new device is not allowed.
- **Valid**: Registration on a new device is allowed.

The licenses you purchase affect which mobile device policies are available to you. See "Understanding licensing" on page 377 for an overview.

The Samsung service posts a message when you log in to Admin Portal that indicates if you have any licenses that will be expiring in the next 10 days or have expired.
Enabling automatic log out from the Samsung SDS IAM & EMM user portal and Admin Portal

You can automatically log out users from Admin Portal or the user portal after a period of inactivity. You enable this policy using the Idle User Session Timeout tab and then set the inactivity time period. The default is five minutes.

This policy has no effect on mobile device users.

To enable automatic user log out:

1. Open Admin Portal and click **Settings, Users, Idle User Session Timeout**.
2. Select “Automatically log out idle users.”
3. Enter the time period.
4. Click **Save Changes**.
Using login suffixes

The login suffix is that part of the login name that follows @. For example, if the login name is bob.jones@acme.com, the login suffix is “acme.com.” The login suffix identifies for the Samsung service which ID repository has the user’s account when the user logs in to the Samsung service portals or enrolls a device. If the login suffix is not listed on this page, the user cannot be authenticated.

Normally, the Samsung service automatically creates a default login suffix for your organization based on the login suffix in the work email account entered in the Samsung service sign-up form. However, if that login suffix is already in use, the Samsung service appends a one- or two-digit number to the end. For example, if the email address entered when the Samsung service account had the login suffix acme.com but “acme.com” was already used by another organization, the Samsung service would create the login suffix acme.com.4.

You can create more login suffixes for Samsung SDS IAM & EMM directory accounts. You assign a new Samsung directory to a login suffix when you create the account.

Samsung SDS IAM & EMM directory specific information

For Samsung SDS IAM & EMM directory users, the customer ID in the URL can be a ID or a login suffix.

However, if you use a login suffix and the user name that is specified is a short name (without a login suffix), then the customer ID in the URL must be a login suffix. The login suffix should not look like a ID.

The following are examples of using a short name (without login suffix) user name to log in to the Samsung SDS IAM & EMM User Suite

<table>
<thead>
<tr>
<th>URL</th>
<th>User name used for logging in is a short name without a login suffix</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://companyXYZ/my?custome-rid=myorg.com">https://companyXYZ/my?custome-rid=myorg.com</a></td>
<td>jane</td>
<td>You must have a user account <a href="mailto:jane@myorg.com">jane@myorg.com</a>.</td>
</tr>
<tr>
<td><a href="https://cloud.centrify.com/my?custome-rid=myorg">https://cloud.centrify.com/my?custome-rid=myorg</a></td>
<td>jane</td>
<td>You must have a user account jane@myorg</td>
</tr>
<tr>
<td><a href="https://cloud.centrify.com/my?custome-rid=AAA0001">https://cloud.centrify.com/my?custome-rid=AAA0001</a></td>
<td>jane</td>
<td>Even though AAA0001 is a valid login suffix, this log in fails because the customer ID in the URL looks like a ID. For this log in to succeed, the user name should have a login suffix (for example jane@AAA0001).</td>
</tr>
</tbody>
</table>

Chapter 24 • Configuring Samsung service settings
Active Directory specific information

If you are using an Active Directory domain as an ID repository, the Samsung service adds the following login suffixes when the connector is installed:

- The login suffix in the installer’s account name. This allows the administrator to log in to Admin Portal right after installing the connector.

  Note If the login suffix in the connector installer’s account is already in use in the Samsung service, an error message is displayed and you cannot use that domain name as a login suffix. (This occurs rarely but can happen.) Contact support if this happens to your account.

- The domain name of the domain controller to which the host computer for the connector is joined.

- If that domain controller is part of a tree or forest, the Samsung service adds a login suffix for all other domains in the tree or forest it can locate.

  If you have users with Active Directory accounts in domains in a tree or forest that was not found or users who log in with their Office 365 account, you must add those login suffixes before these users can log in to Admin Portal or the Samsung SDS IAM & EMM user portal, and enroll a device.

  You can also create an alias for an Active Directory domain name. You would use an alias to simplify login for users with a long or complicated Active Directory login suffix. See “Creating an alias for long Active Directory domain names” on page 339 for the details. You cannot create an alias for Samsung SDS IAM & EMM directory login suffixes.

Creating a login suffix

You can create as many login suffixes as you want for Samsung SDS IAM & EMM directory accounts. The login suffix can be composed of any of the UTF8 alphanumeric characters plus the symbols + (plus), - (dash), _ (underscore), and . (period). You can, but are not bound to, use the form label.label for your login suffixes; however, a login suffix can be composed of a single label—for example, ACBCorp.

Login suffixes must be unique in the Samsung service (not just within your Samsung service account). If you enter a login suffix that is already in use, you get an error message.

You can select any login suffix when you create new Samsung directory accounts.

To create a login suffix:

1. Log in to Admin Portal and click Settings, Customization, Suffix, Add.
2. Enter the suffix in the text box and click Save.
Deleting a login suffix

You cannot delete a login suffix that has any user accounts. Admin Portal displays an error message if you try to delete a login suffix that still has user accounts. To delete a login suffix, remove all of its user accounts.

Modifying a login suffix

You can rename a login suffix. If you do, the accounts that had the original login suffix are automatically updated to the new one. Be sure to notify the users affected that they have a new login suffix. They will not be able to log in using the original suffix.

To modify a login suffix:

1. Open Admin Portal and click Settings, Customization, Suffix.
2. Right-click the login suffix and click Modify.
3. Make your changes in the text box and click Save.

Creating an alias for long Active Directory domain names

Best practice dictates that you use a login suffix for Active Directory users that they are already using. For example, if they’re using your organization’s domain name to open their email account, it would help them remember their Samsung service user name if you used the same login suffix.

However, this is not a requirement. For example, if you have a long or complex Active Directory domain name, you can create a mapped login suffix for Active Directory accounts using the Advanced option. For example, if your login suffix is abc.bigcorp.com, you could define another login suffix, such as “abc.” A user could then log in to the user portal using just <username>@abc.

To map an Active Directory login suffix:

1. Open Admin Portal and click Settings, Customization, Suffix, Add.
2. Enter the alias in the Login suffix text box.
3. Expand Advanced.
4. Reset the Keep Login Suffix and Mapped Suffix the same checkbox.
5. Backspace over the login suffix in the text box below the checkbox and enter the Active Directory domain name.
6. Click Save.
Linking to the Apple Device Enrollment Program

You use this setting to link the Samsung service as an MDM server in the Apple Device Enrollment Program, upload the Samsung service token, and define the initial profile configuration settings. The Device Enrollment Program is an Apple Deployment Program that helps businesses and education institutions easily deploy and manage iPad and iPhone devices.

Note This feature is available to users with Knox Premium or EMM licenses only. You must have one of the license to see this option on the Settings page. If the license expires before the user enrolls the device, DEP enrollment does not complete and an error is entered in the log file.

When you use the Device Enrollment Program and the device has a network connection, the Apple Device Enrollment Program server installs an initial profile in specified devices. You use the Apple DEP Configuration page in Admin Portal to define the initial profile’s configuration settings, including the device enrollment options, your user support phone number, and the device setup items the user must complete when they first receive the device. Depending upon which enrollment options you select, the Samsung SDS IAM & EMM client can be automatically installed on the device. Thus, users do not need to install it from the Apple App Store.

To use the Apple Device Enrollment program, you need to enroll your organization first. Go to https://deploy.apple.com to learn about the program and to enroll your organization. Return to this section after you have completed enrollment, reviewed the restrictions, and configured your account.

Linking to the Apple Device Enrollment Program is a two part process from the Admin Portal:

- Creating a link between the Samsung service and the Apple Device Enrollment Program.
  
  In this step you create a service token for the Samsung service and upload it to Admin Portal.

- Configuring the initial profile.
  
  These options and properties are displayed on this page after you successfully upload the service token.

The profile is installed only in the devices that are assigned to the Apple Device Enrollment program.

This profile does not replace the profiles that are installed by the Samsung SDS IAM & EMM client after the user enrolls the device in the Samsung service. The profile you define in this procedure just controls the user’s device set up options.
Important: When the serial number for a new device is added to the Apple Device Enrollment Program server, you must click the Push Profile button in Admin Portal, Settings, Apple DEP Configuration.

As a rule of thumb, you should wait 24 hours after you assign the device before giving it to the user to enroll.

To create the link to the Apple Device Enrollment program:

1. Open Admin Portal and click Settings, Mobile, Apple DEP Configuration.
2. Generate a public key.
   - Click Download to generate the public key. In most browsers, this file is written to your Downloads folder.
   - Click the link and enter your user name and password.
   - In your Apple Device Enrollment Program screen, click Add an MDM server and specify the file with the public key you just created.
   - The server token file is downloaded by your browser. In most browsers, this file is written to your Downloads folder.
5. In Admin Portal, upload the server token file.
   - Click Upload and specify the file just downloaded.
   - Once the file has been uploaded, the Apple DEP Configuration page expands to add the Configuration settings.

To configure the initial profile:

1. Enter the profile name.
2. Select the Device enrollment options
   - Minimally, you should select Make device supervised and Require device enrollment. When you select these options, users can enroll with the Active Directory/LDAP or Samsung SDS IAM & EMM directory user name and password and the Samsung SDS IAM & EMM client and Company Apps applications are installed automatically on the device. (Otherwise, the user would have to install the Samsung SDS IAM & EMM client from the Apple App Store.)
3. Enter the Customer support phone number.
   - This is the number for your IT or Help department that you want your users to call if they have a problem or are confused while enrolling the device.
4 Enter a Department or location.

5 Select which setup items to skip when the user enrolls the device.

    By default, the user is prompted for all of the setup items. Check the items you do not require.

6 Click Save.
Setting Corporate IP ranges

You use the Corporate IP Range feature to define IP ranges for your internal network and external network. Connections that are made from inside the corporate IP range have the following privileges:

- Active Directory users can log in to Admin Portal and the Samsung SDS IAM & EMM user portal with silent authentication. (This requires Integrated Windows authentication—see “Configuring connectors” on page 296.)
- If you enable authentication policy controls, these users can be exempt from the additional authentication requirements. (See “Authentication - Setting authentication policy controls” on page 193 for the details.)

There are two Samsung service features that look to the Corporate IP range:

- Silent authentication for Admin Portal and user portal logins: If the computers’ address is outside the IP range you specify here, Active Directory users are prompted to enter their credentials. This feature is not available to users with Samsung SDS IAM & EMM directory accounts.

  If you do not specify a range, all IP addresses are treated as possibly inside your network.

  **Note** This feature uses Integrated Windows authentication. See “Configuring connectors” on page 296 for more about Integrated Windows authentication.

- multifactor login authentication: Users logging in to the portals from computer’s with an address that is outside the IP range are prompted to provide an additional authentication factor.

  If you do not specify an IP range, all IP addresses are treated as outside your network and all users—including those users within your network—are prompted for an additional authentication factor.

  See “Authentication - Setting authentication policy controls” on page 193 for the details on multifactor authentication.

To specify external IP addresses for silent authentication and access control:

1. Open Admin Portal and click **Settings, Network, Corporate IP Range, Add**.
2. Enter an IP address or a range of addresses in the form `<network>/<subnet mask>`.
   
   Admin Portal shows your current external IP address under the text box.
3. Click **OK**

Repeat to specify additional addresses or ranges.
Tag devices as corporate owned

The Samsung SDS IAM & EMM identity platform assigns all enrolled devices with the Personal Owned or Corporate Owned ownership attribute. Devices that are enrolled in the Samsung SDS IAM & EMM identity platform using the following methods are automatically tagged as corporate owned:

- Bulk enrollment
- Device enrollment program (DEP)
- Android for Work in device owner mode

Corporate owned devices can be assigned specific policies that may differ from personal owned devices. For information on policy assignment, see How to create a policy set and assign it to users.

You can only re-tag corporate owned devices as personal owned by un-enrolling and then re-enrolling them. To re-tag devices that have been automatically tagged as corporate owned:

1. Unenroll the devices from the Samsung SDS IAM & EMM identity platform.
2. Re-enroll the devices without using one of the above listed methods.

Change ownership attribute to Personal Owned

You can retag "personal owned" labeled devices with "corporate owned" labels by uploading the device serial numbers onto Samsung service. You must have the serial numbers in a .csv flat file with one serial number and associated device types per line. Device type assignments must be A, I, or M (Android, iOS, or Mac).

To upload the serial numbers:

1. Log in to Admin Portal.
2. Click Settings > Mobile > Corporate-owned Devices > Import.
   
   The Corporate-owned Devices Import window opens.
3. (Optional) Click the Corporate-owned devices import template link if you need to create the CSV file.
4. Click Browse, navigate to your CSV file, upload the file.
5. Click Next.
6. Review the data fields and click Next.
7. Verify the email address for report delivery and click Confirm.
Selecting the policy service for device policy management

You use Device Policy Management to select whether you use Samsung SDS IAM & EMM policy service or Active Directory Group Policy Management to set device configuration policies. After you select the policy management tool, you can set the policy update schedule and certificate authority.

**Note** You must select the Samsung service for mobile device management if you want to set the mobile device policies and install them in the device (see “How to configure Mobile Device Management or single sign-on only” on page 18).

When you select the Samsung SDS IAM & EMM policy service, you use policy sets created in Admin Portal to set device configuration policies. When you use Active Directory group policy you create group policy objects and edit them with the Group Policy Management Editor to set device configuration policies. See “Managing device configuration policies” on page 221 for the details. You use roles to apply the policies to sets of users by linking the group policy object to an Active Directory organizational unit and then specify that organizational unit in the device enrollment settings.

Both methods provide largely the same policies—see “List of device configuration policies” on page 376 for a summary of the policies available in each one. The method you select depends upon the types of accounts (Samsung SDS IAM & EMM directory or Active Directory) used for enrolling devices. Use the following guidelines to select the proper method for your organization:

<table>
<thead>
<tr>
<th>You have devices enrolled by users with the following types of accounts</th>
<th>Select this method</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both users with Samsung SDS IAM &amp; EMM directory and Active Directory accounts</td>
<td>Samsung SDS IAM &amp; EMM policy service</td>
<td>If you select Active Directory, the Samsung service does not install the policies in devices enrolled by users with Samsung SDS IAM &amp; EMM directory accounts.</td>
</tr>
<tr>
<td>Only users with Active Directory accounts</td>
<td>Either Active Directory or Samsung SDS IAM &amp; EMM policy service</td>
<td>Select the method that is most convenient to you.</td>
</tr>
<tr>
<td>Only users with Samsung SDS IAM &amp; EMM directory accounts</td>
<td>Samsung SDS IAM &amp; EMM policy service</td>
<td></td>
</tr>
</tbody>
</table>

**Note** If you select Active Directory group policy, you still use policy sets to configure the Device Management Settings, Device Enrollment Settings, Account Security Policies, and Application Policies. You use the group policy object just to set the device configuration policies.
Selecting the Samsung SDS IAM & EMM policy service

If you select Samsung SDS IAM & EMM policy service, the Samsung service uses the policy sets assigned to each role to set the device configuration policies. See “Using Admin Portal to set device configuration policies” on page 222 for the details.

When you select the Samsung SDS IAM & EMM policy service, you configure the policy push delay and select the certification authority. The policy push delay specifies the number of minutes the Samsung service waits from the time you saved the policy set to push the changes to the devices.

You can use either the Active Directory Certificate Service or the Samsung SDS IAM & EMM CA to generate user and computer certificates to authenticate users and devices for wi-fi connections, respectively. The certificates are created and installed on the device when the user enrolls the device.

Click **Use Active Directory Certificate Service for PKI client authentication** to use the default certification authority you configured in your Active Directory Certificate Service. (You can use the default certification authority only.) If you select this option, you need to create user and computer templates on the default certification authority. There may be some additional configuration required in the connector as well. See “Using Active Directory certificates in devices for authentication” on page 365 for the details.

Click **Use Tenant Certificate Authority for PKI client authentication** to use the Samsung SDS IAM & EMM CA for your Samsung service account () to generate user and computer certificates instead. You do not need to create templates when you select this option.

The Samsung SDS IAM & EMM User Suite includes a Samsung SDS IAM & EMM CA for each customer Samsung service. When you select the certification authority, it generates certificates that can be used to authenticate users for wi-fi and VPN connections and Exchange ActiveSync server log ins. The certificates are automatically generated and installed for users who are a member of a role that has a wi-fi, VPN, or Exchange server profile in the Samsung SDS IAM & EMM policy service in which certificates are used for authentication. The certificates are installed automatically when the user enrolls the device.

Click the **Download** button to download the certificate for the Samsung SDS IAM & EMM CA for your account for installation in the Exchange server, wi-fi access point, or VPN server or concentrator. The certificate is self-signed. See the following sections to configure the use of Samsung SDS IAM & EMM CA certificates:

- “Configuring Exchange profiles” on page 239
- “Configuring VPN profiles” on page 243
- “Configuring Wi-Fi profiles” on page 246

To select Samsung SDS IAM & EMM policy service for device policy management:

1. Open Admin Portal and click **Settings, Mobile, Device Policy Management**.
2 Enable Samsung SDS IAM & EMM directory Policy Service.

3 Click the text box and enter the number of minutes for the policy push delay.

4 Click the radio button to select the certification authority.

5 Optional: If you need to install the certificate for your Samsung SDS IAM & EMM CA in a wi-fi access point, VPN server or concentrator, or Exchange ActiveSync server, click Download to download the certificate file.

6 Click Save.

Selecting Active Directory group policy

If you select Active Directory group policy, the Samsung service uses the group policy object you linked to the organizational unit specified in the Device Enrollment Settings for each role to set the device configuration policies. See “Using the Group Policy Management Editor to set mobile device policies” on page 223 to specify the organizational unit; see “Configuring group policy objects and organizational units” on page 348 to link the group policy object to the organizational unit.

When you select the Active Directory group policy, you set the update interval and select the certification authority used to generate certificates for users and devices when they enroll on the Settings page. The update interval sets how often the Samsung service polls the domain controller for changes to the group policy objects. If the Samsung service finds a group policy object has changed, it pushes the policy changes to the devices. Otherwise, it takes no action.

The certification authority you select generates certificates that can be used to authenticate users for wi-fi and VPN connections and Exchange ActiveSync server log ins. The certificates are automatically generated and installed for users who are a member of a role that has a wi-fi, VPN, or Exchange server profile in the group policy object linked to their organizational unit. The certificates are installed automatically when the user enrolls the device.

When you install the connector, it searches the Active Directory forest for the certification authorities you have configured in your Active Directory Certificate Service. You can select any certificate authority it finds to generate certificates.

Note When you use an Active Directory certification authority, you need to create user and computer templates on the certification authority you select. There may be some additional configuration required in the connector as well. See “Using Active Directory certificates in devices for authentication” on page 365 for the details.

To select Active Directory for device policy management:

1 Open Admin Portal and click Settings, Mobile, Device Policy Management.

2 Enable Active Directory group policy.
3 Set the update interval.
   Enter the number of minutes to set the period between polling events.

4 Select the certificate authority.
   If you do not want to use the default certification authority, use the drop-down menu to select another.

5 Click Save.

Configuring group policy objects and organizational units

When you use Active Directory group policy to set device configuration policies, you use group policy objects that you edit with the Group Policy Management Editor to set the policies. Next, you link that group policy object to an organizational unit. Finally, you specify the organizational unit to use for a given policy set when you configure the Device Enrollment Settings (see “Enabling users to enroll devices” on page 22).

The organizational unit you specify in the Device Enrollment Settings is also the organizational unit in which the Samsung service stores the Active Directory record when the user enrolls the device. You can use this record in Active Directory Users and Computers to get information about the device and send it commands. See “Using Active Directory Users and Computers to manage devices” on page 162 for the details.

When you select Active Directory group policy, you should plan on how you are going to apply the group policy objects to Samsung SDS IAM & EMM directory roles before you create the policy sets and assign them to the roles. Once you have your roles and policies planned, you use the following procedure to apply them to individual users’ devices:

1 Create a separate organizational unit for each role.

2 Create the group policy object for that role and set the policies.

3 Link the group policy object to the organizational unit.

4 Specify the organizational unit when you set the Device Enrollment Settings for the policy set (see “Enabling users to enroll devices” on page 22).

5 Assign the policy set to the role.

6 Add the users to the role.

You can use multiple roles or policy sets to apply different policies to users. In this case the rules for hierarchical policies are applied—see “Using hierarchical policy sets” on page 187.

Enabling Samsung Knox UMC login suffix updates

When you select the Samsung service for mobile device management and you have Samsung Workspace devices equipped with the Samsung Knox Universal Mobile Device Management Client (UMC), you should set “Enable Samsung Knox UMC” to simplify
device enrollment for users. For these users, installing the Samsung SDS IAM & EMM client and enrolling their devices uses a different procedure than users with Android and Samsung devices that are not equipped with the UMC. See “Working with UMC supported KNOX devices” on page 179 for the details.

When you enable this setting, the Samsung service automatically registers and synchronizes the login suffixes you have created. The simplified enrollment is provided to all users whose login suffix is registered in the Samsung Enterprise Gateway. The update is typically made within a minute after you add, delete, or modify the login suffix.

To update the Samsung Enterprise Gateway with your login suffix changes:

1. Log in to Admin Portal and click the Settings, Mobile, Samsung Knox UMC.
2. Select the Enable Samsung Knox UMC checkbox.
3. Click Save.
Managing security settings

You use the security settings to:

- Capture users’ passwords using strong encryption that is unique to your company. See Capturing users’ passwords securely.
- Enable users to retrieve their forgotten username. See Retrieving forgotten username self-service.
- Configure additional attributes for multi factor authentication (MFA). See Configuring additional attributes for MFA.

Capturing users’ passwords securely

By default, the Samsung service does not capture users’ passwords. However, you might want to capture users’ passwords to support account mapping options for user password apps or to provision user passwords to supported applications.

To capture users’ passwords, enable Securely capture users’ passwords at login. Once this option is enabled, the Samsung service captures users’ passwords the next time they log in.

Tip Unless capturing users’ passwords is required for a specific feature, Samsung recommends leaving this feature disabled.

Retrieving forgotten username self-service

Enable this setting if you want users to have the option to retrieve their forgotten username at login. Users will be prompted to enter an email address to which the username will be sent if a Samsung SDS IAM & EMM account is found that matches the email address.

Configuring additional attributes for MFA

You can use additional Active Directory/LDAP attributes (such as other mobile phone, other home phone, other office phone and other email addresses) for multi factor authentication (MFA). The Samsung service maps these additional attributes to Admin Portal and uses their values for MFA notification.

Regardless of the attribute you select, only the Mobile Phone type will receive a text message notification.

Use the Custom attribute for other phone numbers, such as fax or IP phone. When you use the Custom attribute, the attribute name must match one in the Attr LDAP Name column as shown here.

We import all Active Directory user attributes, but we only monitor and accept updates for the attributes listed in the following table.
This table lists the Active Directory user attributes used by Office 365 for which we monitor and accept updates. Some of these attributes are duplicated in the above table.

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Attributes</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountExpires</td>
<td>lockoutTime</td>
<td>otherMobile</td>
</tr>
<tr>
<td>c</td>
<td>mail</td>
<td>pager</td>
</tr>
<tr>
<td>cn</td>
<td>manager</td>
<td>primaryGroupID</td>
</tr>
<tr>
<td>co</td>
<td>member</td>
<td>postalCode</td>
</tr>
<tr>
<td>countryCode</td>
<td>memberOf</td>
<td>postOfficeBox</td>
</tr>
<tr>
<td>directReports</td>
<td>mobile</td>
<td>pwdlastset</td>
</tr>
<tr>
<td>distinguishedName</td>
<td>name</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>displayName</td>
<td>otherPager</td>
<td>sn</td>
</tr>
<tr>
<td>givenName</td>
<td>otherTelephone</td>
<td>st</td>
</tr>
<tr>
<td>groupType</td>
<td>otherMailbox</td>
<td>streetAddress</td>
</tr>
<tr>
<td>homePhone</td>
<td>otherFacsimileTelephoneNumber</td>
<td>userAccountControl</td>
</tr>
<tr>
<td>I</td>
<td>otherHomePhone</td>
<td>userPrincipalName</td>
</tr>
<tr>
<td>ipPhone</td>
<td>otherIpPhone</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td></td>
<td></td>
<td>wWWHomePage</td>
</tr>
<tr>
<td>assistant</td>
<td>msExchArchiveName</td>
<td>msExchSenderHintTranslations</td>
</tr>
<tr>
<td>authOrig</td>
<td>msExchAssistantName</td>
<td>msExchTeamMailboxExpiration</td>
</tr>
<tr>
<td>c</td>
<td>msExchAuditAdmin</td>
<td>msExchTeamMailboxSharePointU rl</td>
</tr>
<tr>
<td>cn</td>
<td>msExchAuditDelegate</td>
<td>msExchUsageLocation</td>
</tr>
<tr>
<td>co</td>
<td>msExchAuditDelegateAdmin</td>
<td>msExchUserHoldPolicies</td>
</tr>
<tr>
<td>company</td>
<td>msExchAuditOwner</td>
<td>msRtcSip-ApplicationOptions</td>
</tr>
<tr>
<td>countryCode</td>
<td>msExchBlockedSendersHash</td>
<td>msRtcSip-DeploymentLocator</td>
</tr>
<tr>
<td>department</td>
<td>msExchBypassAudit</td>
<td>msRtcSip-Line</td>
</tr>
<tr>
<td>description</td>
<td>msExchBypassModerationFromDLMembersLink</td>
<td>msRtcSip-OptionFlags</td>
</tr>
<tr>
<td>displayName</td>
<td>msExchBypassModerationLink</td>
<td>msRtcSip-OwnerUrn</td>
</tr>
<tr>
<td>dLMemRejectPerms</td>
<td>msExchDelegateListLink</td>
<td>msRtcSip-PrimaryUserAddress</td>
</tr>
<tr>
<td>dLMemSubmitPerms</td>
<td>msExchElecExpirySuspensionEnd</td>
<td>msRtcSip-UserEnabled</td>
</tr>
<tr>
<td>Attributes</td>
<td>Attributes</td>
<td>Attributes</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>extensionAttribute1</td>
<td>msExchElcExpirySuspensionStart</td>
<td>objectGUID</td>
</tr>
<tr>
<td>extensionAttribute2</td>
<td>msExchElcMailboxFlags</td>
<td>objectSid</td>
</tr>
<tr>
<td>extensionAttribute3</td>
<td>msExchEnableModeration</td>
<td>otherFacsimileTelephoneNumber</td>
</tr>
<tr>
<td>extensionAttribute4</td>
<td>msExchExtensionCustomAttribute1</td>
<td>otherHomePhone</td>
</tr>
<tr>
<td>extensionAttribute5</td>
<td>msExchExtensionCustomAttribute2</td>
<td>otherIPPhone</td>
</tr>
<tr>
<td>extensionAttribute6</td>
<td>msExchExtensionCustomAttribute3</td>
<td>otherMobile</td>
</tr>
<tr>
<td>extensionAttribute7</td>
<td>msExchExtensionCustomAttribute4</td>
<td>otherPager</td>
</tr>
<tr>
<td>extensionAttribute8</td>
<td>msExchExtensionCustomAttribute5</td>
<td>otherTelephone</td>
</tr>
<tr>
<td>extensionAttribute9</td>
<td>msExchHideFromAddressLists</td>
<td>pager</td>
</tr>
<tr>
<td>extensionAttribute10</td>
<td>msExchImmutableId</td>
<td>physicalDeliveryOfficeName</td>
</tr>
<tr>
<td>extensionAttribute11</td>
<td>msExchLitigationHoldDate</td>
<td>postalCode</td>
</tr>
<tr>
<td>extensionAttribute12</td>
<td>msExchLitigationHoldOwner</td>
<td>postOfficeBox</td>
</tr>
<tr>
<td>extensionAttribute13</td>
<td>msExchMailboxAuditEnable</td>
<td>preferredLanguage</td>
</tr>
<tr>
<td>extensionAttribute14</td>
<td>msExchMailboxAuditLogAgeLimit</td>
<td>proxyaddresses</td>
</tr>
<tr>
<td>extensionAttribute15</td>
<td>msExchMailboxGuid</td>
<td>publicDelegates</td>
</tr>
<tr>
<td>facsimileTelephoneNumber</td>
<td>msExchModeratedByLink</td>
<td>pwdLastSet</td>
</tr>
<tr>
<td>givenName</td>
<td>msExchModerationFlags</td>
<td>samaaccountname</td>
</tr>
<tr>
<td>homePhone</td>
<td>msExchRecipientDisplayType</td>
<td>sn</td>
</tr>
<tr>
<td>info</td>
<td>msExchRecipientTypeDetails</td>
<td>st</td>
</tr>
<tr>
<td>initials</td>
<td>msExchRemoteRecipientType</td>
<td>streetAddress</td>
</tr>
<tr>
<td>IPPhone</td>
<td>msExchRequireAuthToSendTo</td>
<td>targetAddress</td>
</tr>
<tr>
<td>legacyExchangeDN</td>
<td>msExchResourceCapacity</td>
<td>telephoneAssistant</td>
</tr>
<tr>
<td>mail</td>
<td>msExchResourceDisplay</td>
<td>telephoneNumber</td>
</tr>
<tr>
<td>manager</td>
<td>msExchResourceMetadata</td>
<td>thumbnailPhoto</td>
</tr>
<tr>
<td>middleName</td>
<td>msExchResourceSearchProperties</td>
<td>title</td>
</tr>
<tr>
<td>mobile</td>
<td>msExchRetentionComment</td>
<td>userAccountControl</td>
</tr>
<tr>
<td>msDS-HABSeniorityIndex</td>
<td>msExchRetentionURL</td>
<td>userCertificate</td>
</tr>
<tr>
<td>msDS-PhoneticDisplayName</td>
<td>msExchSafeRecipientsHash</td>
<td>userSMIMECertificate</td>
</tr>
<tr>
<td>msExchArchiveGuid</td>
<td>msExchSafeSendersHash</td>
<td>wwwHomePage</td>
</tr>
</tbody>
</table>
Importing OATH tokens in bulk

You can authenticate the Samsung SDS IAM & EMM Identity Service using your existing third-party OATH tokens (for example, those generated by a YubiKey) by bulk uploading those tokens. Samsung SDS IAM & EMM Identity service uses those tokens to generate one-time passcodes (OTP) that users with enrolled devices can immediately use to log in to the Samsung SDS IAM & EMM user portal.

Users without enrolled devices must first log in to the user portal and scan the Samsung SDS IAM & EMM generated QR code (using a third party authenticator) to get the passcode pushed to their devices. You can direct users to Using a third party authenticator application.

When you upload these tokens, they will override any existing passcode users may have generated by scanning the Samsung SDS IAM & EMM generated QR code.

Before you start importing OATH tokens, you need a CSV file with the following column headers (header names must match exactly):

- User Principle Name
- Secret Key (HEX)
- Account Name
- Issuer
- Algorithm
- OTP Digits
- Type
- Period
- Counter

**Important:** The secret keys in the CSV file must be in HEX format.

A CSV file template is available on the bulk upload page in Samsung SDS IAM & EMM Admin Portal.

To bulk upload OATH tokens:

1. Log in to Admin Portal.
2. Navigate to Settings, Authentication, OATH Tokens.
3. Click Bulk Token Import.
4. Click Browse, navigate to your CSV file, and upload it.
5. Click Next.
6. Review the first 15 rows and if they look correct, click Next.

If you see an error, cancel the upload and fix the error.
7 Confirm the email address or enter a different one where a bulk import report will be sent.

8 Click Confirm.

A bulk import report email is sent to the specified email address.

9 Refresh the OATH Tokens page to see the uploaded instance.

If you have not configured the OATH OTP policy, you need to do so before users can use the generated passcodes. When you configure the OATH OTP policy, you can also define if users can see the QR code from the user portal. See “Configuring OATH OTP” on page 201.
Samsung SDS IAM & EMM connectors and administrator consoles

This section provides information about the Samsung SDS IAM & EMM connector, such as modifying the connector account permissions and creating certificate templates if you want to use certificates for login authentication for Wi-Fi connections, VPNs, or Exchange email accounts. Both of these are Samsung service options, and you do not need to perform these procedures if you are not using these options.

To install the connector, see “How to install a Samsung SDS IAM & EMM connector” on page 48.

The following contents are relevant to this topic:

- “Supporting user authentication for multiple domains” on page 356
- “Creating administrator consoles and adding additional connectors” on page 360
- “Modifying connector account permissions” on page 362
- “Using Active Directory certificates in devices for authentication” on page 365
- “Uninstalling the Samsung SDS IAM & EMM Management Suite software” on page 369
Supporting user authentication for multiple domains

You install the connector on a host Windows computer that is joined to a domain controller to authenticate Samsung service users who have an account in that domain. If you want the Samsung service to authenticate users in other domains, there are two connector installation models—which one you use depends upon whether the accounts are in trusted domains in a single forest or in multiple, independent domain trees or forests.

**Note** If all of your Samsung service users have their accounts in a single domain controller, you can skip this topic.

**Configuring authentication for trusted domains**

You use this model when the users’ Active Directory accounts are in domains with domain controllers that have a two-way, transitive trust relationship with the domain controller to which the connector is joined.

In this model, you have a single connector for the entire domain tree or forest. The Samsung service communicates through this connector for all authentication requests. When the user account is in another domain, the authentication requests are handled...
According to the tree-root, parent-child, forest, and shortcut trust relationship settings between the domain controllers.

**Trusted Domains Model**

If you are using Active Directory for device and policy management, all object management communications are done through the same connector as well.

By default, two-way transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain by using the Active Directory Installation Wizard. The two default trust types are parent-child trusts and tree-root trusts. When you configure the trust relationship, be sure to select Forest trust. This establishes a transitive trust between one forest root domain and another forest root domain. See *How Domain and Forest Trusts Work* in Microsoft TechNet for more about trust relationships.

After you install the first connector, you should install one or more on separate host computers. The host computer for each connector must be joined to the same Active Directory domain controller. See “Creating administrator consoles and adding additional connectors” on page 360 for the details.

The Samsung service automatically creates a login suffix for the domain to which the host computer is joined plus all of the domains that the connector can see. Which domains can be seen depends upon two criteria:

- The trust relationship between the domain controllers.
Only domain controllers with a two-way transitive trust meet this criteria

- The connector’s user account permissions.

By default the connector is installed as a Local System user account on the Windows host. (See “Modifying connector account permissions” on page 362 for more information.)

The permissions you grant to this account can affect its ability to see other domains.

**Note** When Admin Portal searches Active Directory domains for users and groups (for example, when you are adding a user or group to a role), it only searches the Active Directory Users container in the domain controllers that can be seen by the connector.

### Independent domains in multiple forests

You use this model when the users’ Active Directory accounts are in independent domain trees or forests; that is, there are domain controllers that do not have a two-way, transitive trust relationships with each other.

In this model, you have a separate connector for each independent domain tree or forest. The Samsung service picks which connector to use for the authentication request based on the login-suffix-to-domain mapping it creates and maintains. When the user account is in the connector’s domain controller, the authentication requests are handled according to the tree-root, parent-child, forest, and shortcut trust relationship settings between the domain controllers in that forest or domain tree.

After you install the first connector for each independent domain tree or forest, you should install one or more on separate host computers for each one. The host computer for each connector must be joined to the same Active Directory domain controller as the initial
connector for this tree or forest. See “Creating administrator consoles and adding additional connectors” on page 360 for the details.

The Samsung service automatically creates a login suffix for the domain to which the host computer is joined plus all of the domains that the connectors for each independent domain can see.

When Admin Portal searches Active Directory domains for users and groups (for example, when you are adding a user or group to a role), it only searches the Active Directory Users container in the domain controllers that can be seen by the connectors. Which domains can be seen depends upon two criteria:

- The trust relationship between the domain controllers.
  - Only domain controllers with a two-way transitive trust meet this criteria. When you configure the trust relationship, be sure to select Forest trust. This establishes a transitive trust between one forest root domain and another forest root domain. See How Domain and Forest Trusts Work in Microsoft TechNet for more about trust relationships.

- The connector’s user account permissions.
  - By default the connector is installed as a Local System user account on the Windows host. The permissions you grant to this account can affect its ability to see other domains. See “Modifying connector account permissions” on page 362 for more information.

If you are using this model, use the Samsung SDS IAM & EMM policy service to set mobile device policies (see “Selecting the policy service for device policy management” on page 345) and Samsung service roles to enable users to enroll devices.
Modifying the default connector settings

You use the Samsung SDS IAM & EMM connector configuration program to modify the default setting. See “Configuring the Samsung SDS IAM & EMM connector” on page 370 for the description of each tab and how to modify the default settings.

There are several default settings you may need to change right after you install the connector:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Tab</th>
<th>To do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable auto-update</td>
<td>Samsung SDS IAM &amp; EMM</td>
<td>Configure the connector to automatically poll the Samsung service for software updates and install them. You can also specify the polling-update windows.</td>
</tr>
<tr>
<td>Active Directory user verification interval</td>
<td>Samsung SDS IAM &amp; EMM</td>
<td>Set the polling period between queries for updates to active Active Directory user accounts.</td>
</tr>
<tr>
<td>Log settings</td>
<td>Logging</td>
<td>After you install a connector, you should configure the connector to log activities to help in troubleshooting in case you have any problems. Go to this tab to enable logging.</td>
</tr>
</tbody>
</table>

Creating administrator consoles and adding additional connectors

You use the same Samsung SDS IAM & EMM Management Suite installer to install the additional connectors for load balancing and failover and administrator consoles to manage Samsung service users, devices and group policy objects.

About load balancing and failover

You should configure one or more connectors to provide continuous up time for Samsung service services. Each connector you add is listed in Admin Portal on the Settings page in the Samsung SDS IAM & EMM connector tab.

The Samsung service provides load balancing among all connectors with the same services installed. For example, when a request comes in the Samsung service routes the request among the available connectors. If one connector becomes unavailable, the request is routed among the other available connectors providing automatic failover.

Installing additional connectors

You use the same procedure to download the installation wizard to the host computer and then run the wizard to install and register additional connectors. After you install and register the connector, it is added to the Samsung SDS IAM & EMM connector page.
Note  The host computer must be joined to the same Active Directory domain controller as the first connector in the same trust domain or forest.

Creating an Samsung service administrator console

You use the same procedure to download the installation wizard to the host computer and then run the wizard. However, you do not install the connector. Instead, you install either or both of the console extensions.

Note  The host computer must be joined to the same Active Directory domain controller as the connectors in the same trust domain or forest.
Modifying connector account permissions

By default, the connector service is started as a Local System account process. This account has sufficient permissions for most purposes with the following exceptions:

- If you want to give Active Directory users the ability to reset their passwords or unlock their accounts from the user portal login prompt, you will need to configure the relevant policy in Admin Portal and run the connector under an account with the necessary permissions. See “How to configure user self-service options” on page 44.

- If the host computer does not have read access to the container or organizational unit that stores the user accounts. Without read access, the connector cannot authenticate the user. Domain computers have this permission by default; however, the connector host may not. This most often occurs in multi-forest or multi-domain setups and can occur even when two-way trust is already defined. You can tell when this occurs—the connector log would show the error message, "unable to locate forest or user object."

In this case, you need to give the Local System account read access permission to the containers or organizational units.

**Note** If you change the connector’s account or modify Local System account permissions, be sure to make the same changes on all the connectors you install.

**Implementing connector on a member server**

To implement the connector on a member server:

1. On a member server, open elevated PowerShell and run the following command:
   ```
   add-windowsfeature GPMC
   ```

2. In Active Directory, create service account for the connector and assign permissions using instructions in “Permissions required for alternate accounts and organizational units” on page 362.

3. Install the connector on the member server.

4. Open Services on the connector and change the connector service “run as” account.

5. Restart the connector service.

**Permissions required for alternate accounts and organizational units**

You can also run the connector service as a Domain Admin account or an Active Directory user account instead of as a Local System account. A Domain Admin account has all of the required permissions. However, if you run as an Active Directory account, this account must be a member of the local administrators group, and you must confirm that it has the following permissions:
• At least read permission to the container that has the Samsung service user accounts.
• A broader set of permissions on the container that has the enrolled device objects.

When you designate the enrolled device object container or organizational unit in the Device Enrollment Settings, you need to set the read permission and the permissions for the Active Directory user account for the container or organizations unit that stores the enrolled device objects. Repeat the second procedure for every container or organizational unit you use to store the enrolled device objects.

To set the Read access permission to the user account container or organizational unit:

1. Open Active Directory Users and Computers, select the user account container, and open the **Properties**.
2. Select the **Security** tab and then click **Add** to add the user account you are using to run the connector service. Click **OK** after you add the user account.
3. Click the user account in **Group or User Names** and click the Allow box for the **Read** permission.
4. Click **OK**.

To set the permissions to the enrolled device object container or organization unit:

1. Open Active Directory Users and Computers, select the enrolled device object container, and open **Properties**.
2. Select the **Security** tab then the **Advanced** button to view the Advanced Security Settings.
3. Click **Add** to add a new permission entry.
4. Click **Object Types** and confirm that the object type for your connector is selected.
5. Click **OK**.
6. Navigate to Select User, Computer, Service Account, or Group window.
7. Enter the first few characters of the object name into the object name text box then click **Check Names**.
8. Select the object name for your connector and click **OK**.
9. Select **Allow** for the Create Computer objects permission.
10. Click **OK**.
11. Click **Add** to add another permission entry.
12. Click **Object Types** and confirm that the object type for your connector is selected.
13. Select the object name for your connector and click **OK**.
Modifying connector account permissions

The Permission Entry for MobileDevices window opens.

14 Click the **Allow** box for the following permissions on the Object tab:
   - Write all properties
   - Delete
   - Read permissions
   - All validated writes

15 Click **OK** on the succeeding windows to exit the Properties configuration windows.

### Setting the service connection point (SCP) object permissions

The connector creates a serviceConnectionPoint object when it is started for the first time after installation. When the connector service is started by the Local System account, it has full control over the serviceConnectionPoint object.

If you use an Active Directory account other than the Local System account, the following procedure describes how to add the additional permissions required by that user.

To set the permissions for a Service Connection Point (SCP) object for a selected user account:

1 Open ADSI Edit and open the **Properties** for the desired SCP object.

   The service connection is created when the connector is started for the first time. If the connector’s name is

   \[CN=\text{MachineA}, \text{CN=Computers}, \text{DC=domain, DC=com}\]

   the SCP object is located in ADSI Edit at the following:

   \[CN=proxy, \text{CN=MachineA}, \text{CN=Computers}, \text{DC=domain, DC=com}\]

2 Select the **Security** tab and then click **Add** to add the user account you are using to run the connector service. Click **OK** after you add the user account.

3 Click the user account in **Group or User Names** and click the **Advanced** button.

4 Click user account in the **Permission entries** tab and click the **Edit** button.

5 In the Object tab, click the Allow box for the **Write all properties** permission.

   The “Apply to” field should be set to **This object only**. This is often the default. If it is not, use the drop-down list to change it.

6 Click **OK**.

7 Click **OK** on the succeeding windows to exit ADSI Edit.
Using Active Directory certificates in devices for authentication

You can use a certificate authority in the Active Directory Certificate Service to generate user and computer certificates for user and device authentication. In turn, you can use these certificates for login authentication in the Wi-Fi, VPN, and Exchange ActiveSync server profiles rather than an account’s user name and password. (See the Wi-Fi, VPN, and Exchange server profile configuration descriptions in “Mobile device configuration policies overview” on page 227 for the details.)

**Note** This section only applies when you use Active Directory group policy for device policy management (see “Selecting the policy service for device policy management” on page 345) or you select Active Directory Certificate Service in Device Policy Management (see “Selecting the Samsung SDS IAM & EMM policy service” on page 346). If you select the Tenant Certificate Authority instead, you can skip this section.

To use certificates from your Active Directory certification authority, you must create user or computer certificate templates on the Windows Certificate Authority server used by the Samsung SDS IAM & EMM connector. In addition, you need to configure the host computer for each of your Samsung SDS IAM & EMM connectors so that it can revoke certificates.

After you create the templates, the certificates are automatically created for the Samsung service and then installed by the Samsung service when the user enrolls the device.

- If you are using Active Directory group policy for device policy management, you can select the certification authority when you configure Device Policy Management—see “Selecting Active Directory group policy” on page 347. If you are using Samsung SDS IAM & EMM policy service for device policy management and select the Active Directory Certificate Service, the Samsung service uses the default Active Directory Certificate Services certification authority only.

- In many cases, additional server configuration is required before you can use certificates for authentication. See your server’s documentation for the details.

You need to go to the user certificate template on the Windows Certification Authority server to confirm that the Domain Users group in Active Directory has the permission to auto-enroll the certificate. For specific instructions for configuring Exchange 2010 authentication using PKI, see this Exchange 2010 PKI Authentication Configuration document.

The procedures in this section assume that you have a working Active Directory Certificate Services certificate authority within your domain and you have sufficient permissions to modify the settings.
Enabling the enrollment policy to use user and computer certificates

Before you can use certificates for authentication, you need to set the enrollment policy to enable automatic enrollment and renewal. The following procedure shows you how to set the Certificate Enrollment Policy for user and computer certificates in the Default Domain Policy. However, you can also set them on a group-by-group basis.

To enable computer and user certificate enrollment policies:

1. Open the Group Policy Management plug in on the connector, right-click the Default Domain Policy, and click Edit.


4. In the Configuration Model menu, select Enabled.

5. Click OK.
6 To enable the Certificate enrollment policy for user certificates expand User Configuration > Policies > Windows Settings > Security Settings and click Public Key Policies.

7 Double click Certificate Services Client - Certificate Enrollment Policy.

8 In the Configuration Model menu, select Enabled.

9 Click OK.

Creating the certificate templates

You create either or both certificate user and computer templates on the Active Directory certificate authority server you selected in the Device Policy Management (see “Selecting the policy service for device policy management” on page 345). The template or templates you create must be named as follows, including the uppercase letters:

- Computer-ClientAuth
- User-ClientAuth

In some cases, you specify in the profile which type of certificate (user or computer) to use for authentication (for example, the iOS Wi-Fi profile) while others require you to use either the computer or the user certificate. To simplify profile configuration, we recommend creating both templates.

You use the Microsoft Management Console (MMC) on the certification authority server designated in the Samsung SDS IAM & EMM connector to create the templates.

To create computer and user certificate templates:

1 Launch certsrv.msc or the Certificate Authority console on the Windows server with the certification authority installed.

2 Expand the certification authority, right-click Certificate Templates, and click Manage.

3 Right-click Computer choose Duplicate Template.

   To create the User-ClientAuth template, you right-click User instead and then choose Duplicate Template.

4 Click the Compatibility tab, select Windows Server 2008 and click OK.

5 Click the General tab and enter Computer-ClientAuth in the Template display name text box.

   This action also automatically fills in the Template name field.

   If you are creating the user template, enter User-ClientAuth instead.

6 Set the Validity period: and Renewal period values.
7 Click the Subject Name tab and select Supply in the request.
8 Click the Security tab, select Authenticated Users and select the Enroll permission.
9 On the same tab, select Domain Computers and select the Enroll permission.
10 Click OK and close the Certificate Templates Console.
11 In the MMC, right-click Certificate Templates, click New, and click Certificate Template to Issue.
12 Click Computer-ClientAuth and click OK.
   If you are creating the user template, click User-ClientAuth instead and click OK.
   The templates you create should now appear in the Certificate Templates folder.

Revoking certificates for unenrolled devices
The certification authority does not by default revoke certificates for devices when they are unenrolled. You must give the host computer for the Samsung SDS IAM & EMM connector the "Issue and Manage Certificates" permission in the certification authority server to revoke certificates.

Note You must grant this permission in the certification authority for the host computer for each of your Samsung SDS IAM & EMM connectors.

To enable certification authority to revoke certificates when devices are unenrolled:
1 Launch certsrv.msc or the Certificate Authority console on the Windows server with the certification authority installed.
2 Right-click the certification authority and click Properties.
3 Click the Security tab.
4 Click the Add button and select the host computer for the Samsung SDS IAM & EMM connector.
   Make sure the “Computer” object type is selected (click Object Types and select Computers) and enter the first few characters of the computer name as the search filter in the Check Names field.
   Select the computer and click OK
5 Select the computer from the Group or user names list and set the Issue and Manager Certificates permission to Allow.
6 Click OK.
7 Repeat this procedure for all of your connector host computers.
Uninstalling the Samsung SDS IAM & EMM Management Suite software

You use the Uninstall command in the Windows Control Panel to remove the connector and console extensions.

All of the components are installed under the name Samsung SDS IAM & EMM Management Suite followed by the version number. Uninstalling this program removes all of the Samsung SDS IAM & EMM Management Suite components installed on the computer. You cannot, for example, delete the connector but leave the console extensions.

If you use just one Samsung SDS IAM & EMM connector, uninstalling the Samsung SDS IAM & EMM Management Settings from the Active Directory Control Panel terminates mobile device policy enforcement. However, if you uninstall the Samsung SDS IAM & EMM Management Suite from one computer but have the Samsung SDS IAM & EMM connector installed on one or more other computers, service is not interrupted. In this case, the Samsung service automatically switches to another connector.

To uninstall the Samsung SDS IAM & EMM Management Suite software:

1. On a Windows computer on which you installed Samsung SDS IAM & EMM policy service Management Suite, close any open Microsoft Management Consoles, such as Active Directory Users and Computers and Group Policy Management Editor, that may be using the components.

2. Click Start > Control Panel > (Programs) Uninstall Program, then right-click Samsung SDS IAM & EMM Management Suite version.

3. Click Yes when the confirmation message appears.

If no Microsoft Management Console applications are open, the installer finishes and removes the Samsung SDS IAM & EMM Management Suite software. If applications are open, you are prompted for how to close them.

4. If prompted to close open applications, do the following:
   - Leave the following option selected and click OK: Automatically close applications and attempt to restart them after setup is complete.
   - If prompted that a Microsoft Management Console application has stopped working, click Close the program.

The connector and, if also installed, the console extensions are now removed from your computer. However, a directory and some files will still reside on your computer. To remove these files, complete the next step.

5. To remove Samsung SDS IAM & EMM Management Suite related files, navigate to and delete the C:\Program Files\samungemm folder.
Configuring the Samsung SDS IAM & EMM connector

This section explains how to use the Samsung SDS IAM & EMM connector configuration program to configure and monitor your connector. It covers the following topics:

- About the Samsung SDS IAM & EMM connector and the configuration program
- Using the Status tab
- Using the Samsung SDS IAM & EMM connector tab

You launch the Samsung SDS IAM & EMM connector configuration program from the Start menu on the host computer. You modify settings by selecting different tabs in the window. You can see the tabs in the following figure.
About the Samsung SDS IAM & EMM connector and the configuration program

The Samsung SDS IAM & EMM connector runs on a host computer and manages communications between Active Directory/LDAP and the Samsung service. It specifies groups whose members can enroll devices and a group whose members can manage devices. It also monitors Active Directory for group policy changes, which it sends to the Samsung service to update enrolled devices.

Initial configuration of the connector follows installation with the connector configuration wizard, which launches automatically. To complete the wizard, you must identify a user group whose members can enroll devices and a container that stores accounts for enrolled devices. You must also identify a group whose users have permission to manage enrolled devices and manage the configuration.

The connector configuration application allows you to complete the initial configuration and to make changes when necessary. You can also run this application to monitor the status of your connector.

**Note** You can also monitor connectors by using Admin Portal. However, Admin Portal only allows you to monitor connectors — it does not allow you to configure a connector in any way.

The Samsung service uses all of the available connectors configured for a service. Each server has its own connector configuration program that you launch on the computer hosting the connector. However, when you make a change to any of the connectors in an installation (that is, servers registered to the same customer ID), the changes are propagated to all the servers in the installation to ensure that they are all in sync.

The Samsung SDS IAM & EMM connector configuration program is installed on any computer where a connector is installed. You can launch it from the Windows Start menu. The application appears as a window with tabbed panels:

- **Status**: Shows server name, Samsung service customer ID, and Samsung service connection status.
- **Samsung SDS IAM & EMM connector**: Provides connector controls and option settings.
Using the Status tab

The Status tab displays the following read-only information about the connector:

- **Server name** displays the assigned name of this connector.
- **Customer ID** displays the customer ID under which this connector is registered. You can install multiple connectors using the same customer ID for load balancing and failover. All active connectors are used by the Samsung service.

  **Note**  Do not change this field.

- **Samsung SDS IAM & EMM connector is started|stopped** shows whether the connector is started (running) or not.
- **Connection to Samsung service** shows the date, time, and result of the last connection to the Samsung service.

**Updating the connector to the latest version.**

You use the Status tab to update the connector to the latest version if you do not enable automatic updates (see the Samsung SDS IAM & EMM connector tab). To manually update the connector, right-click the update icon in the lower left of the Status tab and select **Update**.
Using the Samsung SDS IAM & EMM connector tab

The **Samsung SDS IAM & EMM connector** tab reports the customer ID under which the connector is registered and whether or not the server is started. It also offers the following controls:

- The **Re-register** button starts the Samsung SDS IAM & EMM connector configuration wizard and allows you to re-register this connector. Generally, you re-register the connector under the same customer ID, and then only if the connector is having difficulty communicating with the Samsung service and customer support recommends that you re-register to address the issue.

  **Note**  Re-registering under a different ID can destabilize your environment and should be done only after consulting with customer support. Changing the ID moves the connector from one installation to another. If the connector is the only server in an installation, removing the server from the installation will cause any device enrollment to the installation to fail, and enrolled devices will no longer receive policy changes.

- Click **Start** to start the connector if it’s stopped.
- Click **Stop** to stop the connector if it’s running.
- Select **Allow support to access local connector logs** to give the Samsung service provider the ability to open the connector log files. These files can help resolve a problem and are the only files the service provider can open. The default is selected.
- Click **View Log** to view the connector log.
- Use the **Settings update interval** text box to set the number of minutes this connector takes between checks on connector settings with the Samsung service. When any connector in an installation changes its settings, it sends those settings to the Samsung service. When a connector checks settings with the Samsung service, if there were new settings reported from any of the other connectors in the installation, the checking connector downloads and accepts those settings. This ensures that all connectors in an installation have the same settings.
- Use the **Active Directory user verification interval** text box to set the number of minutes this connector takes between checks for active AD user accounts. When the connector checks Active Directory user accounts, it contacts Active Directory/to see if the user account listed for each enrolled device is active. If a device’s associated user account is not active (is disabled or removed), the Samsung service unenrolls the device.
- Select the **Enable auto-update** check box to turn on automatic update for the connector. When auto-update is on, the connector checks the Samsung service periodically to see if there is a connector update. If there is, the connector downloads and installs the update, then restarts. This ensures that connector software is up-to-date. We recommend that you enable this option. See “Configuring the connector to install updates automatically” on page 374 for the details.
• Select **Use a web proxy server for Samsung service connection** check box if your network is configured with a web proxy server that you want to use to connect to the Samsung service. Note that the web proxy must support HTTP 1.1 for a successful connection to the Samsung service. After you select this option, enter the following information to enable the web proxy connection:
  - **Address** is the URL of the web proxy server.
  - **Port** is the port number to use to connect to the web proxy server.
  - Click **Credential** to enter the user name and password for an account that can log in to the web proxy server.

### Configuring the connector to install updates automatically

You can configure the connector to automatically install updates when new versions are released. When you select this option, the connector regularly polls the Samsung service and automatically installs a newer version. If you do not select this option, you use the Samsung SDS IAM & EMM connector configuration program to check for and install updates manually.

To configure connector for automatic updates:

1. Click the Windows Start menu and open the Samsung SDS IAM & EMM connector configuration program.
2. Click **Yes** to allows this program to make changes to the computer.
3. Click the **Samsung SDS IAM & EMM connector** tab.
4. Select **Enable auto-update**.
5. Click the **Schedule** button to select the times during which the connector can check for an update.
   
   To set the times when the connector can check for an update (cell is blue), click “Auto-update Allowed” or “Auto-update Denied” to start with a full or blank slate; click, drag and release to select an area of cells, and then click “Auto-update Allowed” or “Auto-update Denied” to set the periods.
6. Click **Close**.

To check for and install connector updates manually:

1. Click the Windows Start menu and open the Samsung SDS IAM & EMM connector configuration program.
2. Click **Yes** to allows this program to make changes to the computer.
3. In the lower left of the Status tab, right-click the update icon and select **Update**.
The connector updates and then displays a message indicating that the software is up to date.
List of device configuration policies

The following tables list the Samsung service device configuration policies. The bulk of the policies are available whether you use the Windows Group Policy Management Editor (GPME) or the Samsung SDS IAM & EMM policy service. However, a few policies may be available in one but not the other.

See the Explain tab in the Windows Group Policy Management Editor or tool tips in Admin Portal for the details on implementing the policy.

- “Understanding licensing” on page 377
- “Common Mobile Settings” on page 378
- “iOS Settings” on page 380
- “Additional iOS Settings” on page 383
- “Samsung KNOX Device Settings” on page 385
- “Samsung KNOX Workspace Settings” on page 395
- “Touchdown Settings” on page 404
Understanding licensing

The device configuration policies that are available for you to enable and configure are determined by the licenses that your organization has purchased. If you enable a policy in either the Samsung SDS IAM & EMM policy service or Active Directory Group Policy Management Editor and you don’t have the required license, the policy is not installed in the device.

The following table summarizes the policies that are available with each license:

<table>
<thead>
<tr>
<th>Policy Category</th>
<th>Knox Express for IT</th>
<th>Knox Premium</th>
<th>Knox Workspace</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Mobile Settings</td>
<td>Full</td>
<td>Full</td>
<td>None</td>
</tr>
<tr>
<td>iOS Settings</td>
<td>Just Exchange</td>
<td>Full</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>ActiveSync</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung Knox Device settings</td>
<td>Full</td>
<td>Full</td>
<td>None</td>
</tr>
<tr>
<td>Samsung Knox Workspace Settings</td>
<td>Partial</td>
<td>Partial</td>
<td>Full</td>
</tr>
</tbody>
</table>
Common Mobile Settings

**Passcode Settings**

The Passcode Settings policies are available to Knox Express for IT and Knox Premium licenses. Note, however, that to set policies using the Active Directory Group Policy Management Editor, you must have a Knox Premium license. Otherwise, you can set policies through the Samsung SDS IAM & EMM policy service only.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Lock (minutes)</td>
<td>Require mobile devices to enforce passcode access.</td>
</tr>
<tr>
<td>Grace period for device lock</td>
<td>Require iOS devices to allow a grace period.</td>
</tr>
<tr>
<td></td>
<td>For iOS devices, the grace period is the amount of time that a locked device may be unlocked without entering the passcode.</td>
</tr>
<tr>
<td>Maximum number of failed attempts</td>
<td>Specify the maximum number of failed attempts that are allowed before the device is wiped.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you set Samsung Knox Workspace Settings/Enable Common Criteria mode, this policy is enabled for Samsung Workspace devices, however this setting is not shown in Admin Portal or Group Policy Management Editor. This allows you to make a separate setting for other devices.</td>
</tr>
<tr>
<td>Maximum passcode age (days)</td>
<td>Specify the number of days a passcode can exist before it must be reset.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specify the minimum number of complex characters required for the passcode.</td>
</tr>
<tr>
<td>Minimum passcode length</td>
<td>Specify the minimum number of characters required for the passcode.</td>
</tr>
<tr>
<td>Passcode history</td>
<td>Specify the number of passcodes to store and compare against new passcodes.</td>
</tr>
<tr>
<td></td>
<td>New passcodes are not allowed to repeat a stored passcode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you set Samsung Knox Workspace Settings/Enable Common Criteria mode, this policy is disabled for Samsung Workspace devices, however this setting is not shown in Admin Portal or Group Policy Management Editor. This allows you to make a separate setting for other devices.</td>
</tr>
<tr>
<td>Permit simple value</td>
<td>Allow a passcode with simple values (that is, values that use repeating, ascending, or descending character sequences).</td>
</tr>
<tr>
<td>Require alphanumeric value</td>
<td>Require alphanumeric values (that is, values with at least one letter and one integer).</td>
</tr>
<tr>
<td>Require passcode on device</td>
<td>Require mobile devices to enforce passcode access.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must set this policy for the other passcode policies to be enforced.</td>
</tr>
</tbody>
</table>
Restrictions Settings

The Restriction Settings policies are available to Knox Express for IT and Knox Premium licenses. Note, however, that to set policies using the Active Directory Group Policy Management Editor, you must have a Knox Premium license. Otherwise, you can set policies through the Samsung SDS IAM & EMM policy service only.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit camera use</td>
<td>Control whether user can use the camera and the FaceTime app on their devices.</td>
</tr>
<tr>
<td>Permit user to unenroll device</td>
<td>Control whether user can unenroll a device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This policy is only available in the Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td>Permit user to wipe device</td>
<td>Control whether user can wipe device.</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong></td>
</tr>
<tr>
<td></td>
<td>• This policy is only available in the Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td></td>
<td>• For iOS devices, this policy applies only to devices with iOS 8 or later that are configured as “supervised” in Apple Configurator.</td>
</tr>
<tr>
<td></td>
<td>• For Android devices, this policy applies only to devices that support the Samsung Knox Device SDK version 3.0 (ENTERPRISE_SDK_VERSION_3_0) or later. (The Samsung Knox Device SDK version is listed under the Operating System Settings when you open the device details in Admin Portal.)</td>
</tr>
<tr>
<td>Report mobile device location</td>
<td>Display device location in the user portal. If enabled, you have the option to enforce mandatory sharing of device location with systems administrators or allow users to control sharing of their device locations. See Location tracking. By default, this policy is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The user must also have device tracking turned on in the device and in the user portal the default setting).</td>
</tr>
</tbody>
</table>
iOS Settings

The iOS Settings policies except for the Exchange ActiveSync Settings require a Knox Premium license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange ActiveSync Settings</td>
<td>Configure Exchange ActiveSync profile for iOS devices.</td>
</tr>
<tr>
<td></td>
<td>Note: You can also use this policy if you have a Samsung SDS IAM &amp; EMM license.</td>
</tr>
<tr>
<td>Per app VPN Settings</td>
<td>Map native applications to a specific VPN connection.</td>
</tr>
<tr>
<td></td>
<td>Note: This feature is only available for VPN profiles that use the F5 VPN with certificate based authentication.</td>
</tr>
</tbody>
</table>

Kiosk Mode

The iOS Kiosk Mode policies require a Knox Premium license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow user to control assistive touch setting</td>
<td>Displays a control to let user adjust assistive touch.</td>
</tr>
<tr>
<td></td>
<td>Note: This policy only goes into effect if the “Enable assistive touch” policy is set.</td>
</tr>
<tr>
<td>Allow user to control invert-color setting</td>
<td>Displays a control to let user modify invert color settings.</td>
</tr>
<tr>
<td></td>
<td>Note: This policy only goes into effect if the “Enable invert colors” policy is set.</td>
</tr>
<tr>
<td>Allow user to control voice-over setting</td>
<td>Displays a control to let user adjust voice-over settings.</td>
</tr>
<tr>
<td></td>
<td>Note: This policy only goes into effect if the “Enable voice-over” policy is set.</td>
</tr>
<tr>
<td>Allow user to control zoom Setting</td>
<td>Displays a control to let user adjust the zoom.</td>
</tr>
<tr>
<td></td>
<td>Note: This policy only goes into effect if the “Enable zoom” policy is set.</td>
</tr>
<tr>
<td>Enable kiosk mode (Supervised Only)</td>
<td>Puts the device in kiosk (single application only) mode and lets you select the MDM client or a specific application to run as the application.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All of the other kiosk mode policies go into effect only when the policy is enabled.</td>
</tr>
<tr>
<td>Use MDM client as kiosk mode application</td>
<td>Allows users to use the Samsung SDS IAM &amp; EMM application in kiosk mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Application statuses, such as Install and Update, are not displayed when a device is in kiosk mode.</td>
</tr>
</tbody>
</table>
iOS Settings

Appendix 2

• List of device configuration policies

Restrictions Settings

The iOS Restriction Settings policies require a Knox Premium license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use built-in application as kiosk mode application</td>
<td>Allows users to use the selected built-in application (such as Contacts, Calendar, etc.) in kiosk mode. You must provide the application bundle identifier when defining this policy.</td>
</tr>
<tr>
<td>Use custom application as kiosk mode application</td>
<td>Allows users to use the defined custom application in kiosk mode.</td>
</tr>
<tr>
<td>Device control policies</td>
<td>Disable auto-lock&lt;br&gt;Disable device rotation&lt;br&gt;Disable ringer switch&lt;br&gt;Disable sleep-wake button&lt;br&gt;Disable touch&lt;br&gt;Disable volume buttons&lt;br&gt;Enable Assistive touch&lt;br&gt;Enable invert colors&lt;br&gt;Enable mono-audio&lt;br&gt;Enable speak selection&lt;br&gt;Enable Voiceover&lt;br&gt;Enable zoom</td>
</tr>
<tr>
<td>Force encrypted backups</td>
<td>Allow devices to back up to iTunes without encryption.</td>
</tr>
<tr>
<td>Force iTunes Store password</td>
<td>Require device owners to enter a password for all iTunes transactions.</td>
</tr>
<tr>
<td>Force limit Ad tracking</td>
<td>Limit device Ad tracking.</td>
</tr>
<tr>
<td>Force Siri Profanity Filter (Supervised Only)</td>
<td>Allow device to use Siri Profanity Filter.</td>
</tr>
<tr>
<td>GPME: Permit access to Airdrop (Supervised only)</td>
<td>Allow users to use AirDrop.</td>
</tr>
<tr>
<td>Samsung SDS IAM &amp; EMM policy service: Permit Airdrop (Supervised only)</td>
<td>Allow device to access erotic media in iBookstore. This setting applies only to devices that are configured as ‘supervised’ with Apple Configurator.</td>
</tr>
<tr>
<td>Permit access to erotic media of iBookstore (Supervised Only)</td>
<td>Allow device owners to access Game Center This setting applies only to devices that are configured as ‘supervised’ with Apple Configurator.</td>
</tr>
<tr>
<td>Policy</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permit access to iBookstore (Supervised Only)</td>
<td>Allow device owners to access iBookstore. This setting applies only to devices that are configured as ‘supervised’ with Apple Configurator.</td>
</tr>
<tr>
<td>Permit access to Shared Photo Stream</td>
<td>Allow device owners to access Shared Photo Stream.</td>
</tr>
<tr>
<td>Permit account modification (Supervised Only)</td>
<td>Allow device owners to modify the account.</td>
</tr>
<tr>
<td>Permit adding Game Center friends (Supervised Only)</td>
<td>Allow device owners to add Game Center friends on their devices.</td>
</tr>
<tr>
<td>Permit app cellular data usage changes (Supervised Only)</td>
<td>Allow applications to change from wi-fi to cellular data on device.</td>
</tr>
<tr>
<td>Permit automatic diagnostic reports submission</td>
<td>Allow devices to submit diagnostic reports to Apple automatically.</td>
</tr>
<tr>
<td>Permit automatic sync while roaming</td>
<td>Allow devices to automatically sync while roaming.</td>
</tr>
<tr>
<td>Permit device to show Passbook notifications on lock screen</td>
<td>Allow devices to display Passbook notifications when the device is locked.</td>
</tr>
<tr>
<td>Permit explicit music &amp; podcasts</td>
<td>Allow device owners to access explicit music and podcasts on their devices.</td>
</tr>
<tr>
<td>Permit Find My Friends settings modification (Supervised only)</td>
<td>Allow device owners to enable Find My Friends on their devices.</td>
</tr>
<tr>
<td>Permit iCloud backup</td>
<td>Allow device owners to back up their devices to iCloud.</td>
</tr>
<tr>
<td>Permit iCloud document sync</td>
<td>Allow device owners to synchronize documents and key values to iCloud.</td>
</tr>
<tr>
<td>Permit iCloud keychain sync</td>
<td>Allow device owners to synchronize keychain to iCloud.</td>
</tr>
<tr>
<td>Permit iMessage (Supervised Only)</td>
<td>Allow device owners to access iMessage.</td>
</tr>
<tr>
<td>Permit in-app purchase</td>
<td>Allow device owners to make in-app purchases.</td>
</tr>
<tr>
<td>Permit installing apps</td>
<td>Allow device owners to install apps on their devices.</td>
</tr>
<tr>
<td>Permit iTunes Music Store use</td>
<td>Allow device owners to use the iTunes Music Store on their devices.</td>
</tr>
<tr>
<td>Permit screen control center</td>
<td>Allow device to show control center during lock screen.</td>
</tr>
<tr>
<td>Permit lock screen notification view</td>
<td>Allow the device to show Notifications View during lock screen.</td>
</tr>
<tr>
<td>Permit lock screen today view</td>
<td>Allow device to show Today View during lock screen.</td>
</tr>
</tbody>
</table>
## Additional iOS Settings

These iOS Settings policies require a Knox Premium license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit manual configuration file installation</td>
<td>Allow the device to install configuration profiles and certificates interactively. This setting applies only to devices that are configured as ‘supervised’ with Apple Configurator.</td>
</tr>
<tr>
<td>(Supervised Only)</td>
<td></td>
</tr>
<tr>
<td>Permit multiplayer gaming (Supervised Only)</td>
<td>Allow device owners to play multi-player games on their devices.</td>
</tr>
<tr>
<td>Permit opening managed app documents in unmanaged apps</td>
<td>Allow device owners to open managed application documents in an unmanaged application.</td>
</tr>
<tr>
<td>Permit opening unmanaged apps documents in managed apps</td>
<td>Allow device owners to open unmanaged application documents in managed applications.</td>
</tr>
<tr>
<td>Permit Photo Stream</td>
<td>Allow device owners to use Photo Stream on their devices.</td>
</tr>
<tr>
<td>Permit removing apps (Supervised Only)</td>
<td>Allow device owners to remove apps on their devices.</td>
</tr>
<tr>
<td>Permit Safari use</td>
<td>Allow device owners to use the Safari web browser and set specific options for Safari.</td>
</tr>
<tr>
<td>Permit screen capture</td>
<td>Allow device owners to capture screens on their devices.</td>
</tr>
<tr>
<td>Permit Siri use</td>
<td>Allow device owners to use Siri on their devices.</td>
</tr>
<tr>
<td>Permit Siri use while device is locked</td>
<td>Allow device owners to use Siri on their devices while device is locked.</td>
</tr>
<tr>
<td>GPME: Permit Touch ID to unlock device</td>
<td>Allow Touch ID to unlock a device.</td>
</tr>
<tr>
<td>Samsung SDS IAM &amp; EMM policy service: Permit fingerprint unlock</td>
<td></td>
</tr>
<tr>
<td>Permit untrusted TLS prompt</td>
<td>Prompt device owners when their device receives an untrusted HTTPS certificate.</td>
</tr>
<tr>
<td>Permit user-generated content in Siri</td>
<td>Allow device to have user-generated content in Siri.</td>
</tr>
<tr>
<td>Permit voice dialing</td>
<td>Allow device owners to voice dial on their devices.</td>
</tr>
<tr>
<td>Ratings</td>
<td>Enforce a rating policy, limiting movie, TV show, and app viewing to the specified rating level.</td>
</tr>
</tbody>
</table>

### Calendar settings
Configure CalDAV server connection.

### Contacts settings
Configure CardDAV server connection.
### Additional iOS Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP settings</td>
<td>Configure LDAP server for searching contacts.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Not available in Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td>Mail settings</td>
<td>Configure POP or IMAP email account profile.</td>
</tr>
<tr>
<td>Security and privacy settings</td>
<td>Send application and system crash reports to Apple automatically.</td>
</tr>
<tr>
<td>VPN Settings</td>
<td>Set up virtual private network (VPN) connection profiles for iOS devices.</td>
</tr>
</tbody>
</table>
Samsung Knox Device Settings

You must have Samsung Knox Workspace license to use the Samsung Knox Device Settings policies. If you do not, policies you enable are not pushed to the device.

All of the policies in Samsung Knox Device Settings are available with Knox Express for IT and Knox Premium licenses. Note, however, that to set policies using the Active Directory Group Policy Management Editor, you must have a Samsung SDS IAM & EMM license. Otherwise, you can set policies through the Samsung SDS IAM & EMM policy service only.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange ActiveSync Settings</td>
<td>Configure Exchange ActiveSync profiles for Samsung Knox devices.</td>
<td>2.0</td>
<td>This policy applies to personal mode only. You configure Exchange ActiveSync profiles for Samsung Knox containers separately in the Samsung Knox Workspace Settings.</td>
</tr>
<tr>
<td>VPN Settings</td>
<td>Configure VPN for Samsung Knox Standard devices.</td>
<td>3.0</td>
<td>Do not use this policy for Samsung Knox Workspace devices. Instead, you configure VPN profiles for Samsung Knox workspace devices separately in the Samsung Knox Workspace Settings. If you enable the &quot;Allow only IPsec or SSL/TLS VPN connections&quot; policy, MDM version 4.0 is required.</td>
</tr>
<tr>
<td>APN Settings</td>
<td>Create Access Point Name profiles</td>
<td>5.0</td>
<td>Use this policy to provision a device with APNs for enterprise billing before tying the billing to a specific APN. Use the Enterprise Billing policy to specify the APN.</td>
</tr>
<tr>
<td>Wi-Fi Settings</td>
<td>Configure Wi-Fi connections on Samsung Knox devices.</td>
<td>3.0</td>
<td>You create profiles for all Knox devices, including Knox Workspace devices, in this policy.</td>
</tr>
</tbody>
</table>
# Application Management

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kiosk Mode</td>
<td>Put device is kiosk mode. When the device is in this mode, users are limited to a specific application</td>
<td>3.0</td>
<td>You can set additional policies that control multiple windows, display of the navigation and status bars, and access to the task manager when the device is in kiosk mode. See “Using the Samsung KNOX Device Settings” on page 231 for more information.</td>
</tr>
<tr>
<td>IMAP/POP Settings</td>
<td>Enable and configure IMAP or POP email account on Samsung Knox device.</td>
<td>2.0</td>
<td>This policy applies to personal mode only. You configure IMAP/POP profiles for Samsung Knox containers separately in the Samsung Knox Workspace Settings.</td>
</tr>
</tbody>
</table>

## Applications blocked based on permission restriction
- Set permission restrictions to block applications.

## Applications that can/cannot show status bar notifications
- Prevent status bar notifications.

## Applications that user can/cannot install
- Prevent installation of applications.

## Applications that user can/cannot launch
- Create blacklist of applications user cannot launch.

## Applications that user can/cannot stop
- Prevent user from stopping applications.

## Applications that user can/cannot uninstall
- Prevent uninstallation of applications.

## Applications to be added to home screen
- Select home screen applications.

## Applications to be removed from home screen
- Remove home screen applications.

## Change application’s icon
- Change the icon for a package.
### Bluetooth Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth devices that user can/cannot connect</td>
<td>Allow Bluetooth connection for specific devices.</td>
<td>2.2</td>
</tr>
<tr>
<td>Bluetooth features that user can/cannot use</td>
<td>Select which Bluetooth features users can use.</td>
<td>2.2</td>
</tr>
<tr>
<td>Bluetooth profiles that user can/cannot use</td>
<td>Enable Bluetooth profiles.</td>
<td>2.0</td>
</tr>
<tr>
<td>Enable Bluetooth discoverable mode</td>
<td>Set Bluetooth discoverability mode.</td>
<td>2.0</td>
</tr>
<tr>
<td>Enable limited discoverable mode</td>
<td>Limit Bluetooth discovery period.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit data transfer via Bluetooth</td>
<td>Permit data transfer using Bluetooth.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit desktop or laptop connection via Bluetooth</td>
<td>Allow Bluetooth connection to computer.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit outgoing calls via Bluetooth headset</td>
<td>Permit outgoing calls from Bluetooth headset.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit pairing with other Bluetooth devices</td>
<td>Allow pairing with other Bluetooth devices.</td>
<td>2.0</td>
</tr>
</tbody>
</table>

### Device Inventory Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable logging of call information</td>
<td>Enable logging call information on the device.</td>
<td>2.0</td>
</tr>
<tr>
<td>Enable logging of cellular data network statistics</td>
<td>Enable logging cellular data network usage.</td>
<td>2.0</td>
</tr>
</tbody>
</table>
### Firewall Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable logging of Wi-Fi network</td>
<td>Enable logging the number of Wi-Fi data bytes received and sent.</td>
<td>2.0</td>
</tr>
<tr>
<td>Time between updates of data logging</td>
<td>Enable interval period between updates of data log.</td>
<td>2.0</td>
</tr>
</tbody>
</table>

### Passcode Settings

There are several passcode policies labelled “Advanced Settings:” in this table. In the Group Policy Management Editor they are listed in a separate category and in the Samsung SDS IAM & EMM policy service descriptions they are in a collapsed list. Changing the settings in these policies will require all users affected by this policy to change their password regardless of whether their current password meets the new criteria.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password visibility</td>
<td>Enable password visibility.</td>
<td>4.0</td>
</tr>
<tr>
<td>Enable screen lock pattern visibility</td>
<td>Enable screen lock pattern visibility.</td>
<td>3.0</td>
</tr>
<tr>
<td>Exclude external storage for failed passwords wipe</td>
<td>Exclude external storage when the device is wiped after the user exceeded the maximum number of failed password attempts.</td>
<td>4.0</td>
</tr>
<tr>
<td>Maximum failed password attempts for disabled device</td>
<td>Specify the maximum number of failed password attempts.</td>
<td>2.0</td>
</tr>
</tbody>
</table>
### Samsung Knox Device Settings

#### Appendix 2

### List of device configuration policies

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of changed characters in password</td>
<td>Specify the minimum number of changed characters required for a new password.</td>
<td>4.0</td>
</tr>
<tr>
<td>Timeout for password change enforcement</td>
<td>Specify the maximum time allowed to change a password.</td>
<td>2.0</td>
</tr>
<tr>
<td>Advanced Settings: Forbidden strings in password</td>
<td>Set strings that are forbidden in the device password.</td>
<td>2.2</td>
</tr>
<tr>
<td>Advanced Settings: Maximum character sequence length in password</td>
<td>Specify the maximum alphabetic sequence length.</td>
<td>4.0</td>
</tr>
<tr>
<td>Advanced Settings: Maximum numeric sequence length in password</td>
<td>Specify the maximum numeric sequence length allowed in the password.</td>
<td>2.2</td>
</tr>
<tr>
<td>Advanced Settings: Maximum occurrences of a character in password</td>
<td>Specify the maximum number of occurrences of a character in the device password.</td>
<td>2.2</td>
</tr>
<tr>
<td>Advanced Settings: Password pattern enforcement</td>
<td>Force the user to enter a password based on a regular expression.</td>
<td>2.0</td>
</tr>
</tbody>
</table>

### Restrictions Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit access to manage background data usage</td>
<td>Allow the user to synchronize with a server when the application is in the background.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit access to the clipboard</td>
<td>Allow editing functions to use the clipboard.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit Android Beam use</td>
<td>Block the use of Android Beam on device.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit audio recording</td>
<td>Disable audio recording.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit Bluetooth access</td>
<td>Permit user access to Bluetooth.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit cellular data use</td>
<td>Allow mobile data connections.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit changing wallpaper</td>
<td>Allow the user to change the device wallpaper.</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit device as a media player via USB</td>
<td>Allow using the device as a USB media player.</td>
<td>2.0</td>
</tr>
<tr>
<td>Policy</td>
<td>Description</td>
<td>Minimum Device SDK version</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Permit expansion of status bar</td>
<td>Allow expansion of the status bar.</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit firmware recovery</td>
<td>Allow users to initiate a firmware recovery operation on the device.</td>
<td>5.0</td>
</tr>
<tr>
<td>Permit Google backup</td>
<td>Allow backing up to Google servers.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit home key functionality</td>
<td>Enable home key functionality.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit installation of non-Google-Play apps</td>
<td>Allow installation of non-Google-Play applications.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit killing an activity when the user leaves it</td>
<td>Allow killing an activity when the user leaves it without user interaction.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit microphone use</td>
<td>Allow the user and third-party applications to use the microphone.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit mock GPS locations</td>
<td>Allow the device to change it's actual longitude and latitude readings.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit NFC use</td>
<td>Allow the user to change the near field communication setting in the Settings application.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit power off</td>
<td>Allow the user to power off the devices using the power button.</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit S Beam use</td>
<td>Enable the user to send and receive files using S Beam.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit S Voice application use</td>
<td>Allow S Voice application use (Samsung personal assistant).</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit safe mode launch</td>
<td>Enable the user to reboot the device in safe mode.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit screen capture</td>
<td>Allow device owners to capture screens.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit SD card access</td>
<td>Enable data access to the SD card.</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit sending crash report to Google</td>
<td>Enable sending a crash report to Google.</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit setting a background process limit</td>
<td>Allow setting a background process limit by the user.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit setting mobile data limit</td>
<td>Allow the user to set the mobile data limit without user interaction.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit settings changes</td>
<td>Allow changes to Settings applications.</td>
<td>2.0</td>
</tr>
<tr>
<td>Permit sharing the clipboard between applications</td>
<td>Allow sharing a global clipboard between applications.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit stopping system app</td>
<td>Enable the use of force stop button.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit Tethering</td>
<td>Enable the device to share carrier data with another device.</td>
<td>2.0</td>
</tr>
<tr>
<td>Policy</td>
<td>Description</td>
<td>Minimum Device SDK version</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Permit upgrading the operating system (OS) over-the-air (OTA)</td>
<td>Allow user to upgrade the OS via a firmware-over-the-air (FOTA) client (for example, Samsung DM or WebSync DM).</td>
<td>3.0</td>
</tr>
<tr>
<td>Permit USB debugging</td>
<td>Allow device debugging through Dalvik Debug Monitor Server (DDMS) or adb.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>On Samsung Knox Workspace devices, the following rules are enforced:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When a container is created, USB debugging is automatically disabled and the user cannot change this setting on the device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When the container is removed and this policy is not configured, the user can change this setting on the device.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the policy is set to allow debugging before the container is created, debugging is not disabled after the container is created.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: The last rule is enforced differently on T devices (for example, the Note 4). On these devices, debugging is always disabled after the container is created. An admin can override this setting, however, by re-applying the policy after the container is created.</td>
<td></td>
</tr>
<tr>
<td>Permit USB host storage</td>
<td>Connect any portable USB storage, external HD, or Secure Digital (SD) card reader when it is mounted as a storage drive on the device.</td>
<td>4.0</td>
</tr>
<tr>
<td>Permit USB mass storage</td>
<td>Allow the user to access USB mass storage.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>This policy blocks any kind of browsing the device directory through Dalvik Debug Monitor Server (DDMS).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This policy is deprecated for devices using Android 4.0 or later. Instead, use the Media Transfer Protocol to enable and disable USB mass storage on the device.</td>
<td></td>
</tr>
<tr>
<td>Permit video recording</td>
<td>Allow using the camera to record videos.</td>
<td>4.0</td>
</tr>
<tr>
<td></td>
<td>If video recording is disabled, the device camera is still available so that user can take pictures and use video streaming.</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Description</td>
<td>Minimum Device SDK version</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Permit VPN use</td>
<td>Allow the user to establish a VPN session.</td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>When this policy is set to False (GPME) or No (Samsung SDS IAM &amp; EMM policy service), the UI for using VPN through the Settings application is inaccessible.</td>
<td></td>
</tr>
<tr>
<td>Permit Wi-Fi use</td>
<td>Enable the Wi-Fi UI setting.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>When set to False, (GPME) or No (Samsung SDS IAM &amp; EMM policy service) user or third-party applications cannot enable Wi-Fi access.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When set to True (GPME) or Yes (Samsung SDS IAM &amp; EMM policy service), the Wi-Fi UI setting is enabled but WiFi functionality is not automatically enabled.</td>
<td></td>
</tr>
</tbody>
</table>

### Roaming Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable roaming cellular data</td>
<td>Enable connection to internet when roaming.</td>
<td>1.0</td>
</tr>
<tr>
<td>Enable roaming voice calls</td>
<td>Enable voice calls when roaming.</td>
<td></td>
</tr>
<tr>
<td>Enable roaming WAP push</td>
<td>Enable processing WAP PUSH messages.</td>
<td>1.0</td>
</tr>
<tr>
<td>Enable sync automatically while roaming</td>
<td>Enable automatic application &quot;sync'ing&quot; when roaming</td>
<td>3.0</td>
</tr>
</tbody>
</table>

### Security Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable enrollment with MDM server</td>
<td>Enable enrollment with MDM server.</td>
<td>3.1</td>
</tr>
</tbody>
</table>
### VPN Restrictions

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow only IPsec or SSL/TLS VPN connections</td>
<td>Require IPsec or SSL/TLS VPN connections.</td>
<td>4.0</td>
</tr>
</tbody>
</table>

### Wi-Fi Restrictions

**Note**: If you have an environment with Wi-Fi profiles defined in Samsung Knox Device Settings and Common Mobile Settings, many of the Samsung Knox Device Wi-Fi Restrictions policies affect the Wi-Fi profiles from both settings on Samsung Knox devices.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Minimum Device SDK version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum certificate security level for EAP-TLS networks</td>
<td>Specify the minimum certificate security level for EAP-TLS networks.</td>
<td>2.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Minimum security level of connected Wi-Fi</td>
<td>Specify the minimum security level.</td>
<td>2.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Permit user to add Wi-Fi networks</td>
<td>Allows users to add Wi-Fi networks.</td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td>Description</td>
<td>Minimum Device SDK version</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Permit user to change the Wi-Fi state</td>
<td>Allows users to modify the Wi-Fi state.</td>
<td>3.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Permit user to connect automatically to known Wi-Fi network</td>
<td>Allows users to connect automatically to known Wi-Fi networks.</td>
<td>4.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Permit user to edit Wi-Fi AP settings</td>
<td>Allows users to modify Wi-Fi network access point settings.</td>
<td>2.2</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Permit user to modify Wi-Fi setting</td>
<td>Allows users to modify Wi-Fi network settings.</td>
<td>2.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Permit user to start an open (non-secured) Wi-Fi hotspot</td>
<td>Allows users to open a non-secured hotspot.</td>
<td>4.0</td>
<td></td>
</tr>
<tr>
<td>Prompt user to re-enter credentials if WPA/WPA2-PSK authentication fails</td>
<td>Prompts the user to re-enter credentials (WPA/ WPA2 networks only).</td>
<td>2.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Show password in the Wi-Fi network edit dialog</td>
<td>Shows the password characters in the Wi-Fi network edit dialog.</td>
<td>2.0</td>
<td>For Samsung Knox devices, this policy applies to Wi-Fi profiles defined in Common Mobile Settings and Samsung Knox</td>
</tr>
<tr>
<td>Wi-Fi access point setting</td>
<td>Configure Wi-Fi access point parameters.</td>
<td>2.2</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi network blacklist</td>
<td>Specify a blacklist of Wi-Fi networks.</td>
<td>2.2</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi network whitelist</td>
<td>Specify a whitelist of Wi-Fi networks.</td>
<td>2.2</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi networks to block</td>
<td>Specify Wi-Fi networks to block.</td>
<td>2.0</td>
<td></td>
</tr>
</tbody>
</table>
Samsung Knox Workspace Settings

You must have Samsung Knox Workspace license to use the Samsung Knox Workspace Settings policies. If you do not, any policies that you enable are not pushed to the device.

Some Knox Workspace Settings policies are available with Knox Express for IT and Knox Premium licenses. All of the policies are available when you have a Knox Workspace license. The tables that follow indicate whether the policy is supported by the Knox Express for IT and Knox Premium licenses.

Some of the following policies in Workspace Settings can be applied to both Knox version 1 and Knox version 2 containers. In most cases, setting a Knox version 2 policy has no affect on devices with a Knox version 1 container. Exceptions are mentioned in the Notes column.
<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure applications that can sync with container</td>
<td>Configure applications that can sync with container.</td>
<td>You can configure data synchronization between personal mode and Knox mode for the Contacts and S Planner applications. You can also control which synchronization paths are available to the user to change. See the “Permit changing applications that can sync with the container” policy in Knox Workspace &gt; Container &gt; Restrictions.</td>
</tr>
</tbody>
</table>
| Enable Common Criteria mode | Enable the following policies:  
  • Common Mobile Settings/Encrypt internal onboard storage  
  • Common Mobile Settings/Passcode Settings/Maximum number of failed attempts  
  The number of failed attempts is set to the value you set in the Enable Common Criteria mode policy for the Samsung devices only.  
  • Samsung Knox Device Settings/Security Settings/Encrypt removable storage  
  Disable the Common Mobile Settings/Passcode Settings/Passcode History policy. | The policy settings are implemented on the device only—they are not indicated in the Admin Portal policy set or the Active Directory group policy object. This allows you to have separate settings for these policies for other types of devices. Common Criteria mode puts the target device in an operational mode that enforces the following security features and policies:  
  • Bootloader blocks KIES download mode, enforces an integrity check of the kernel, and self-tests the crypto modules.  
  • The device verifies additional signature on firmware-over-the-air (FOTA) updates using RSA-PSS signature and uses FIPS 140-2 validated crypto module for EAP-TLS wi-fi connections.  
  This policy is only available on the following Knox 2 devices: Galaxy S4, Galaxy S5, Galaxy Note 3, Galaxy NotePro, Galaxy Note 10.1 and Galaxy Note 10.1 2014 Edition. |
| Enable Enterprise Billing | Enable separate bill generation for personal and enterprise data usage. | To enable enterprise billing, two different Access Point Names (APNs) are configured on the Knox device. Personal data is routed via the default APN and enterprise data is routed via the dedicated enterprise APN specified in the policy.  
  Note: This policy is only available for Knox 2.2 devices. |
<p>| Enable Knox container | Enable device to allow user to create a Knox container. | This policy is available when you have a Knox Workspace, Knox Premium, or Knox Express for IT license key. |</p>
<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable ODE Trusted Boot verification</td>
<td>Consider attestation state before decrypting the data partition.</td>
<td>When you enable this policy, applications cannot decrypt data in the data partition if attestation fails. Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current status is shown in the device details in Admin Portal. This policy is also available with a Knox Premium license.</td>
</tr>
<tr>
<td>Enable TIMA Key Store</td>
<td>Consider attestation state before writing or accessing keys and certificates.</td>
<td>The TIMA key store is implemented as a key store provider for the Java Keystore class. When enabled, it provides TrustZone-based secure storage for symmetric keys, RSA key pairs, and certificates. When you enable this policy, applications cannot retrieve or write symmetric keys, RSA key pairs, and certificates if attestation fails. Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current status is shown in the device details in Admin Portal. This policy is also available with a Knox Premium license.</td>
</tr>
<tr>
<td>Require attestation verification</td>
<td>Consider attestation state before creating the Knox container.</td>
<td>When you enable this policy, users cannot create a Knox container if attestation fails. Attestation confirms that the boot loader, kernel, and system software have not been tampered with. Attestation is performed when the user boots the device and periodically thereafter. The current status is shown in the device details in Admin Portal. <strong>Note:</strong> In devices that do not support attestation, if you set this policy, the user is not allowed to create a container. This policy is also available with a Knox Premium license.</td>
</tr>
</tbody>
</table>
**Samsung Knox Workspace Settings**

### Container settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VPN mode of operation</strong></td>
<td>Enable FIPS or non-FIPS compliance for Knox VPNs.</td>
<td>Not available in Samsung SDS IAM &amp; EMM policy service.</td>
</tr>
<tr>
<td><strong>VPN Settings</strong></td>
<td>Configure VPN profiles for Samsung Knox Workspace devices.</td>
<td>Use this policy to create VPN connection profiles to be used in the Knox Workspace container and device settings. This policy is only available with the Knox Workspace license.</td>
</tr>
</tbody>
</table>

**Application Management**

The Application Management Settings policies are available only with a Knox Workspace license.
## Browser Settings

The Browser Settings are available only with a Knox Workspace license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow applications to be moved into container</td>
<td>Adds an option to the Knox Settings application inside the container that displays the mobile applications installed in Personal mode and lets the user install them in the Knox container. <em>Note:</em> This policy is only supported on Knox 2 containers.</td>
</tr>
<tr>
<td>Application SSO whitelist</td>
<td>Specify which mobile applications are allowed to use the Samsung Knox SSO (single sign-on) service.</td>
</tr>
<tr>
<td></td>
<td>Notes:</td>
</tr>
<tr>
<td></td>
<td>• You do not need to add web applications to this list. This is just for mobile applications you install in the container that use the Samsung Knox SSO Service.</td>
</tr>
<tr>
<td></td>
<td>• You do not need to add Samsung SDS IAM &amp; EMM WebApps to this list if you are using the Samsung service for mobile device management.</td>
</tr>
<tr>
<td>Applications that can be installed</td>
<td>Creates a whitelist and blacklist of package names to restrict which mobile applications are allowed and disallowed for installation in the Knox container.</td>
</tr>
<tr>
<td></td>
<td>Notes:</td>
</tr>
<tr>
<td></td>
<td>• This policy is only supported on Knox 2 containers.</td>
</tr>
<tr>
<td></td>
<td>• This policy does not apply to applications that are part of the system image.</td>
</tr>
<tr>
<td></td>
<td>• This policy has no effect on applications that are on the blacklist but were already installed before the policy was installed.</td>
</tr>
<tr>
<td>Applications that can install other applications</td>
<td>Allow specified applications to install other applications.</td>
</tr>
<tr>
<td>Applications that user can/ cannot clear cache</td>
<td>Create list of applications that allow/disallow the user to clear the cache.</td>
</tr>
<tr>
<td>Applications that user can/ cannot clear data</td>
<td>Create list of applications that allow/disallow the user to clear the data.</td>
</tr>
<tr>
<td>Applications to be added to home screen</td>
<td>Select the applications to be displayed on the home screen.</td>
</tr>
<tr>
<td>Applications to be disabled</td>
<td>Silently deny use of specific applications.</td>
</tr>
</tbody>
</table>
## Container Account Policy

The Container Account Settings policies are available with Knox Workspace, Knox Express for IT, and Knox Premium licenses.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts addition blacklist</td>
<td>Specify which accounts are in device account blacklist.</td>
</tr>
<tr>
<td>Accounts addition whitelist</td>
<td>Specify which accounts are in device account whitelist.</td>
</tr>
</tbody>
</table>

## Email Settings

The Email Settings policies are available with Knox Workspace, Knox Express for IT, and Knox Premium licenses.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit account addition</td>
<td>Allow user to more email accounts.</td>
</tr>
</tbody>
</table>
Samsung Knox Workspace Settings

Appendix 2

List of device configuration policies

Firewall Settings

The Firewall Settings policies are only available with a Knox Workspace license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prohibit displaying email using HTML format</td>
<td>Prevent HTML email messages.</td>
</tr>
<tr>
<td>Prohibit forwarding email from specific account</td>
<td>Prevent email forwarding from specific accounts.</td>
</tr>
</tbody>
</table>

Passcode Settings

There are several passcode policies labelled “Advanced Settings:” in this table. In the Group Policy Management Editor they are listed in a separate category and in the Samsung SDS IAM & EMM policy service descriptions they are in a collapsed list. Changing the settings in these policies will require all users affected by this policy to change their password regardless of whether their current password meets the new criteria.

The Passcode Settings policies are available with Knox Workspace, Knox Express for IT, and Knox Premium licenses.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set allow rules</td>
<td>Set allow rules for iptables.</td>
</tr>
<tr>
<td>Set deny rules</td>
<td>Set deny rules for iptables.</td>
</tr>
<tr>
<td>Set redirect exception rules</td>
<td>Set redirect exception rules on iptables.</td>
</tr>
<tr>
<td>Set reroute rules</td>
<td>Set reroute rules on iptables.</td>
</tr>
<tr>
<td>Enable password visibility</td>
<td>Enable device password visibility.</td>
</tr>
<tr>
<td>Maximum failed password attempt for disabled container</td>
<td>Specify the maximum number of failed password attempts.</td>
</tr>
<tr>
<td>Maximum password age (days)</td>
<td>Specify the number of days a passcode can exist before it must be reset.</td>
</tr>
<tr>
<td>Maximum password lock delay (seconds)</td>
<td>Specify in seconds the maximum lock delay that the user can set for the security timeout in the Knox Settings.</td>
</tr>
<tr>
<td>Minimum number of changed characters in password</td>
<td>Specify the minimum number of changed characters required for a new device password.</td>
</tr>
<tr>
<td>Minimum number of complex characters</td>
<td>Specify the minimum number of complex characters required for the device password.</td>
</tr>
<tr>
<td>Minimum passcode quality</td>
<td>Specify the required quality properties for the passcode.</td>
</tr>
</tbody>
</table>
### Samsung Knox Workspace Settings

#### Restriction Settings

The Restriction Settings policies are available only with a Knox Workspace license.

The following policies are enforced only when the user is in the container. For example, if you disable the "Permit camera use" policy, users are prevented from using the camera only when they are in the container. They can still use the camera when they are outside the container.

To turn off features when users are outside the container use the Samsung Knox Device Settings.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force secure keypad</td>
<td>Force device owners to use secure keypad.</td>
</tr>
<tr>
<td>Permit camera use</td>
<td>Control whether users can use the camera on their device when they are in the container.</td>
</tr>
<tr>
<td>Permit user to delete Knox container</td>
<td>Control whether users can delete the Knox mode container.</td>
</tr>
</tbody>
</table>

---

### Policy Description

- **Minimum password length**: On Knox version 2 containers: Set the minimum length for the password and PIN used to open the Knox container. On Knox version 1 containers: Set the minimum length for the password used to open the Knox container.
- **Passcode history**: Specify the number of passcodes to store and compare against new passcodes. New passwords are not allowed to repeat a stored password.
- **Advanced Settings: Forbidden strings in password**: Specify strings that are forbidden in the device passcode.
- **Advanced Settings: Maximum character sequence length in password**: Specify the maximum alphabetic characters sequence length in a device password.
- **Advanced Settings: Maximum numeric sequence length in password**: Specify the maximum numeric character sequence length in a device password.
- **Advanced Settings: Maximum occurrences of a character in password**: Specify the maximum number of occurrences of a character in the device password.
- **Advanced Settings: Require two factor authentication**: Require the user to provide two methods of authentication—fingerprint plus either PIN, password, or pattern—to open the container. Two-factor authentication is not required to create the container. After the container is created, the user is prompted to select the second authentication factor.
  
  **Note**: This policy is available for Knox version 2.1 and later devices with a fingerprint reader only.
### Policy Settings

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent user from changing app data sync setting</td>
<td>Control whether users can change the data import and export between personal and Knox mode for the Contacts and S Planner applications. You can set the default configuration using the Applications that can sync with container policy in Samsung Knox Workspace Settings.</td>
</tr>
<tr>
<td>Permit display of share via list</td>
<td>Control whether the share via list of applications is displayed.</td>
</tr>
<tr>
<td>Permit moving files into the container</td>
<td>Control whether users can move files from device into the container. Users open the My Files application on the device to select and then move the files. The files are moved to the same folder in the container.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This policy is available for Knox version 2 containers only.</td>
</tr>
<tr>
<td>Permit moving files out of the container</td>
<td>Control whether users can move files from container into the device. Users open the My Files application in the container to select and then move the files. The files are moved to the same folder on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This policy is available for Knox version 2 containers only.</td>
</tr>
<tr>
<td>Permit screen capture in Knox container</td>
<td>Control whether users can capture the container screen.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This policy is available for Knox version 2 containers only.</td>
</tr>
</tbody>
</table>

## Device Settings

The Device Settings policies require a Knox Workspace license or a Knox Premium license.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable audit log</td>
<td>Enable an audit log on the device.</td>
</tr>
<tr>
<td>Enable certificate validation before installation</td>
<td>Enable certificate validation during installation.</td>
</tr>
<tr>
<td>Enable revocation check for application SSL connections</td>
<td>Check for certificate revocation for the specified applications.</td>
</tr>
<tr>
<td>Per app VPN settings</td>
<td>Assign a VPN profile to all applications or assign different VPN profiles to different applications. The VPN connection is opened automatically when the application is opened.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Use this policy to map applications installed in personal mode (outside the container) to the VPN profiles. For applications installed in the container, use the policy with the same name in the Container Settings category.</td>
</tr>
<tr>
<td>Trusted certificate authorities</td>
<td>Add a list of trusted CA certificates.</td>
</tr>
</tbody>
</table>
Touchdown Settings

This policy is available with a Knox Express for IT or Knox Premium license. Note, however, that to set policies using the Active Directory Group Policy Management Editor, you must have a Knox Premium license. Otherwise, you can set policies through the Samsung SDS IAM & EMM policy service only.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange ActiveSync Settings</td>
<td>Configure Exchange ActiveSync profile for Android devices other than Samsung Knox devices.</td>
</tr>
</tbody>
</table>
Re-enrolling a device in domains with a different customer ID

If your organization has multiple customer IDs in the same forest, you might encounter a situation in which users cannot unenroll a device from one domain and then enroll it in another. When they try to enroll it in the new domain, they get the message, ‘A transaction with the server at <server name> has failed with the status “403”.’

This situation can occur when you have multiple connectors, each with a different customer ID, and each connector uses a different Active Directory container to store the device object. There are a couple of common situations in which this can occur:

- When you have a test and production deployments each in a separate domain and each domain has a separate Samsung service customer ID.
- When your organization has different divisions—for example, a North America and APAC division—with separate domains and Samsung service customer IDs.

The administrative problem is this: the same device cannot have separate objects in two different organizational units within the same forest. This is a problem because unenrolling a device does not delete it from the organizational unit. When the user unenrolls a device, the Samsung service just changes the state from “enrolled” to “unenrolled.”

To allow the user to enroll the same device in another domain with a separate customer ID an administrator needs to do one of the following:

- Grant the destination connector permission to move or remove objects (in this case, the device object) in the original connector’s organizational unit.
- Manually delete the device object from the original connector organizational unit when the user unenrolls the device. You can do this in Active Directory or using Admin Portal. When the user enrolls the device the next time, the Samsung service creates a new object in the destination organizational unit when the user enrolls the device.
- Manually move the device object from the original connector organizational unit to the destination after the user unenrolls it. When the user enrolls the device the next time, the Samsung service updates the state to enrolled device in the destination organizational unit.