PUBLIC
2019-01-16

Device Management

THE BEST RUN SAP

Content

1 Groups

A group is a collection of devices.

You can link a policy to a group to apply the policy to all of the devices in the group.

1.1 Group Types

Type	Description
Static	Static groups include devices that you add manually.
Dynamic	Dynamic groups include devices that you select using a device view. The membership of dynamic groups changes when the results of the device views change.
User	User groups include devices that are associated with users in a directory group. The membership of user groups changes when the membership of groups in your organization's directory changes.
Composite	Composite groups include groups, and the devices in those groups, that you add manually. The membership of composite groups changes when the membership of the individual groups in the composite group changes.

1.2 Creating Composite Groups

Create one or more composite groups, which let you manage various types of groups as a single entity.

Procedure

1. On the *Group* page, click *New* > *Composite*.
2. Enter a group name and note.
3. Select groups from the available groups list and click *Add selected group*.
   The groups you selected are added to the linked groups list.
4. Click *Save*.

1.3 Creating a User Group

Create a group that includes devices that are associated with users that are included in a user group, as defined by the Afaria server's Windows users groups, Active Directory groups, LDAP groups, or NT domain groups.

Prerequisites

Authentication must be enabled on the Enrollment server and/or Package server in order to create user group assignments for Android and iOS. Refer to the *Installing Afaria* document for details about how to install and configure enrollment server and the Package server.

Self-Service Portal authentication can be used for user group assignments for iOS devices.

Context

Device members may change as user group membership changes. Membership changes automatically based on changes to the selected groups.

> ⚠ Caution
>
> Changes in the directory settings for LDAP or Active Directory may result in the user group definitions not working as expected.

Procedure

1. On the Group page, on the top toolbar, click *New* > *User*.
2. Enter a group name and note.
3. Select groups from the available groups list and click *Add selected group*.

   LDAP-based user group allows both Organizational Unit (OU) level and groups to be assigned but Active Directory user group only allows groups to be assigned. OU level assignments are disallowed.

   > ℹ Note
   >
   > If "Support OU membership" radio button is selected in the *Server* > *Configuration* > *Security* page and an OU is expanded that only include users and groups, an error message "Unknown error returned from LDAP request" is displayed. Reset the option to "Support OU and group membership" in the *Server* > *Configuration* > *Security* page.

   To filter LDAP groups, use the filter syntax `(&(objectCategory=group)(cn=`*groupname*`))`. Where *groupname* is the name of the group or text and wildcard characters that you use as a filter to search the directory.

For example:

- `(&(objectCategory=group)(cn=Admin))` returns the group with the name Admin
- `(&(objectCategory=group)(cn=Support*))` returns groups with names that begin with Support

To reset the filter, click the *Reset Tree* icon.

4. Click *Save*.

1.4 Creating a Dynamic Group

Create a dynamic group whose membership updates automatically based on changes to the results of the device view.

Context

You define the device view in the Device page when you click *Select View* on the left toolbar.

Procedure

1. On the Group page, on the top toolbar, click *New* > *Dynamic* .
2. Enter a group name and note.
   A list of device views from the Device page appears.
3. In the selected view list, select the view to define the group, and then click *OK*.
   The dynamic group includes the devices from the view you selected.
4. Click *Save*.

Refreshing a Dynamic Group [page 12]
Manually refresh a dynamic group.

1.4.1 Refreshing a Dynamic Group

Manually refresh a dynamic group.

Context

The list of devices in a dynamic group refreshes automatically, based on the server schedules enabled in the system. You can also refresh a dynamic group manually, if required.

Procedure

1. On the Group page, select one or more dynamic groups to refresh.
2. On the top toolbar, click *Refresh* to refresh the dynamic group.

1.5 Creating a Static Group

Create an empty static group. To populate the group afterward, use the Link panel to add devices to a group. Membership changes only when you make modifications or delete a device.

Procedure

1. On the Group page, on the top toolbar, click *New* > *Static*.
2. Enter a group name and note, and then click *Save*.
   An empty group is created.
3. To populate the group, use the Link panel to link devices to the static group.

   Adding Devices to a Static Group [page 13]
   You can add devices to a static group in the Afaria Administration console.

   Removing Devices from a Static Group [page 14]
   You can remove devices from a static group in the Afaria Administration console.

1.5.1 Adding Devices to a Static Group

You can add devices to a static group in the Afaria Administration console.

Context

As group size changes, the sort order may change which group has focus. When you link and unlink devices and policies, make sure you have the correct group selected.

While the Link panel list may span multiple pages, toolbar actions, such as link or unlink, can affect only the items selected on the current page. Navigating from one page to another clears prior selections.

Procedure

1. On the *Group* page, select the static group to which to add devices.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.
3. In the Device panel in the Link column filter, change the filter to *Unlinked* to display the list of devices not linked to this group. To narrow the list, use the filter columns or click the column title to sort.
4. Select the devices you want to add to the group and click *Link* on the device panel toolbar.
5. In the Link column, change the filter to *Linked* to show the devices linked to this group.

1.5.2 Removing Devices from a Static Group

You can remove devices from a static group in the Afaria Administration console.

Procedure

1. On the *Group* page, select the static group from which to remove devices.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.
3. In the Device panel in the Link column filter, click *Link* to display the list of devices linked to this group.
4. Select the devices to remove from the group and click *Unlink* on the device panel toolbar.
   The page refreshes without the devices in the list.

1.6 Inspecting a Group

Inspect the contents of a group, such as the groups that make up a composite group. The information you see varies by group type.

Context

To view the device membership for a static group, click *Show/Hide Link* to display the Link panel.

Procedure

1. On the Group page, select a group.
2. On the left toolbar, click *Show/Hide Inspector* to display information about the group.

1.7 Viewing Group Policies

You can view the policies that are linked to a group in the Afaria Administration console.

Context

You can filter the policies in the Policies panel. The filters for the policy panel behave differently depending upon how many groups you select.

If you select one group:

- All – displays all policies
- Linked – displays policies linked to the group
- Unlinked – displays the policies that are not linked to the group
- Both – is not applicable when only one group is selected

If you select multiple groups:

- All – displays all policies
- Linked – displays policies that are linked to all of the selected groups
- Unlinked – displays policies that are not linked to the selected groups
- Both – displays policies that are linked to any of the selected groups

Procedure

1. On the *Group* page, select a group.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

1.8 Viewing Devices in Groups

You can view the devices that are in a group in the Afaria Administration console.

Context

You can filter the devices in the Devices panel. The filters for the Devices panel behave differently depending upon how many groups you select.

If you select one group:

- All – displays all devices
- Linked – displays devices in the group
- Unlinked – displays devices that are not in the group

If you select multiple groups:

- All – displays all devices
- Linked – displays devices that are linked to all selected groups.
- Unlinked – displays policies that are not linked to any of the selected groups.

Procedure

1. On the *Group* page, select a group.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

1.9 Exporting a Group View

Export the group list in its current state with any filters or sort applied. You can export to Excel, Word, and CSV.

Procedure

1. From the Group list, click *Export View*.
2. Select *All* to export all pages of the view, or select *Current Page Only*.
3. Select the export format, and then click *OK*.

1.10 Editing a Group

Edit the group information, such as name, note, and definition.

Procedure

1. On the Group page, select the group to edit.
2. On the top toolbar, click *Edit*.
3. Edit the group name, note, and group setup as required.

   To change the device membership for a static group, link and unlink devices from the Link panel.

1.11 Linking a Policy to a Group

Link a policy to a group. All devices in the group receive the policy when they connect.

Context

Enrollment policy link relationships to groups or devices always appear as blank and cannot link to groups. Enrollment policies are applied to a device only once, when the device enrolls in management.

As group size changes, the sort order may change which group has focus. When you link and unlink devices and policies, make sure you have the correct group selected.

While the Link panel list may span multiple pages, toolbar actions, such as link or unlink, can affect only the items selected on the current page. Navigating from one page to another clears prior selections.

Procedure

1. On the Group page, select the groups for which you want to link policies.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.
3. In the Policy panel in the Link column filter, change the filter to *Unlinked* to display the list of policies not linked to this group. To narrow the list, use the filter columns.
4. Select the policies to add to the group, and click *Link* on the policy panel toolbar.
5. In the Link column, change the filter to *Linked* to show the policies linked to groups.

1.12 Unlinking a Policy from a Group

Remove a policy from a group to discontinue managing the group's devices with the policy.

Procedure

1. On the Group page, select the groups from which to remove policies.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.
3. In the Policy panel in the Link column filter, click *Link* to display the list of policies linked to the groups.
4. Select the policies you want to remove from the group and click *Unlink* on the policy panel toolbar.
   The page refreshes with the policies removed from the list.

1.13 Deleting a Group

Delete a group from the group list.

Procedure

1. On the *Group* page, select a group.
2. On the top toolbar, click *Delete*.

2 Policies

Use policies to enroll and manage devices. In the Afaria Administration console, the Policy page is the landing page for policy-focused tasks.

Policies let you:

- Provision and enroll devices in management
- Define device settings
- Secure devices and data
- Collect inventory
- Distribute software
- Collect device activity data

2.1 Policy Types

Several types of policies are available that allow you to enroll and manage different applications, devices, and channels.

Policy	Description
Application	Application policies define which applications users can view and install on devices.
Configuration	Configuration policies define device settings and collect device data. Configuration policy settings and data collection vary by device type. For many settings, the configuration policies determine the items that are visible to users on devices. For some devices, configuration policies can set items that are available only through manufacturer APIs and are not visible in the user interface.
Enrollment	Enrollment policies define the initial settings on devices and associate devices with groups during device enrollment. Enroll and provision devices that are assigned configuration policies so you can enforce security parameters and deploy and manage enterprise applications.

Policy	Description
Session	Session policies define the channels that devices run. Channels include scripted events and logic to perform tasks on the devices, such as file transfers and registry updates. Some device types let users select a schedule for running session channels. Create and manage session channels in the SAP Afaria Channel Administrator on the SAP Afaria server.

2.2 Default Enrollment Policies

SAP Afaria applies default enrollment policies to devices when you do not specify an enrollment policy during enrollment.

You configure default enrollment policies when you install SAP Afaria. You can edit default enrollment policies in the Afaria Administration console.

Editing Default Enrollment Policies [page 21]
You can edit the default enrollment policies in the Afaria Administration console.

Disabling Default Enrollment Policies [page 22]
You can disable default enrollment policies in the Afaria Administration console.

2.2.1 Editing Default Enrollment Policies

You can edit the default enrollment policies in the Afaria Administration console.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Enrollment* > *Default Enrollment Settings*.
3. Click the appropriate device tab.
4. Make changes to the default enrollment policy.

   > **i Note**
   >
   > For iOS devices, you can also edit the consent text field. For more information on this, see *Creating an Enrollment Policy for iOS*.

5. Click *Save*.

2.2.2 Disabling Default Enrollment Policies

You can disable default enrollment policies in the Afaria Administration console.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Enrollment* > *Default Enrollment Settings*.
3. Click the appropriate device tab.
4. Clear the *Enabled* check box.
5. Click *Save*.

2.3 Creating a Session Policy

Create a policy for running session channels on Android, Windows Mobile, or Windows devices.

Context

The policy includes multiple pages. Clicking the Save button at the top of any page saves all pages.

> **i** Note
>
> Session policies are not supported on Android for Work devices.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Session*.
2. On the Summary page, enter the policy name, note, and remaining properties, except the default channel.
   - State – click to indicate published or unpublished. Connecting devices receive only published policies.
   - OS – click to select the target device type.
   - Priority – set a user-defined value that Afaria uses to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority. A high priority prevails over a lower priority.
   - Authentication – select to require the server to verify the connecting user's identity against your authentication authority before allowing the policy to run. This option is available only if you have authentication enabled on the server, as defined on the *Server* > *Configuration* > *Security* page.

3. On the Channels page, click *Select Channel* to add channels to the list of channels that a device is allowed to request.
4. (Optional) Return to the general page and select a default channel from the list of allowed channels.
   The connecting device requests the default channel during every connection.
5. At the top of the page, click *Save*.

2.4 Viewing the Policy List

View policy summary information, such as operating system and type.

Context

The default sorting on the policy page is by name.

Procedure

1. On the Home page banner, click *Policy*, or click one of the links on the Policy tile.
2. Review the policy list.
   The default view is unfiltered; it includes all policies and may span multiple pages.
3. (Optional) Click the title of any column to sort by that column.

2.5 Viewing the Policy Dashboard

View a graphical representation of policies, such as type, published state, and distribution across device types.

Procedure

1. On the Policy page, click *Policy Dashboard*.
2. On the left toolbar, click *Policy List* to return a more detailed view.

2.6 Editing a Policy

Edit the policy information, such as name, note, and published state.

Procedure

1. On the Policy page, select the policy to edit.
2. On the top toolbar, click *Edit*.
3. Edit the policy information, such as note, published state, and supporting settings.

2.7 Deleting a Policy

Delete a policy from the policy list.

Procedure

1. On the *Policy* page, select a policy.
2. On the top toolbar, click *Delete*.

2.8 Inspecting a Policy

Inspect the contents of a policy, such as enrollment codes and supporting settings.

Procedure

1. On the *Policy* page, select a policy.
2. On the left toolbar, click *Show/Hide Inspector* to display information about the policy.

Viewing Package Tracking Logs [page 25]
You can view package tracking logs to see all of the applications available to devices and the status of application packages in the Afaria Administration console.

2.8.1 Viewing Package Tracking Logs

You can view package tracking logs to see all of the applications available to devices and the status of application packages in the Afaria Administration console.

Procedure

1. On the *Policy* page, select an application policy.
2. On the left toolbar, click the *Show/Hide Inspector* icon to display device inspector options.
   A right pane displays allowing you to select toolbar option and view details about a policy.
3. Click the *Package Tracking* icon in the Inspect toolbar.
   The Package Tracking page shows the list of policy package status details. You can sort on packages related to policies using the following criteria:
   - Afaria Device ID – the device ID attributed to the device when it was enrolled in SAP Afaria
   - Client – the Afaria client name
   - OS – All, iOS, Android, or Windows Phone
   - Status by Afaria – status when you push an application policy via package server (for example, Failed, Installed, or Installed by User).
   - Status by MDM – status when you push an application policy via MDM (for example, Managed or User Rejected). This is relevant only for iOS.
   - Last Update – date the device was updated last

2.9 Publishing and Unpublishing Policies

Publish policies to put them in effect. Unpublish policies to take them out of effect.

Context

Enrollment policies are always in a published state. As an alternative to unpublishing an enrollment policy, edit the policy and disable or delete its enrollment codes.

Procedure

1. On the *Policy* page, select a policy.
2. On the top toolbar:
   - Click *Publish* to publish the selected policy.

- Click *Unpublish* to unpublish the selected policy.

2.10 Viewing the Group Links for a Policy

View the groups linked to a policy.

Procedure

1. On the *Policy* page, select a policy.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.

   The filters for the Groups panel behave differently depending on how many policies you select.
   - If you select one policy:
     - All – displays all available groups, regardless of link state.
     - Linked – displays groups linked to the policy.
     - Unlinked – displays groups that are not linked to the policy.
     - Mixed linked – is not applicable when only one group is selected.
   - If you select multiple policies:
     - All – displays all available groups, regardless of link state.
     - Linked – displays groups that are linked to all selected policies.
     - Unlinked – displays groups that are not linked to any of the selected policies.
     - Mixed linked – displays groups that are linked to some of the selected policies, but not all.

2.11 Viewing the Device Links for a Policy

View the devices linked to a policy. Devices are indirectly linked to policies through their membership in a group. You can link a device to a group, and you can link a group to a policy.

Procedure

1. On the *Policy* page, select a policy.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.

   The filters for the Device panel behave differently depending upon how many policies you select.

- If you select one policy:
  - All – displays all available devices, regardless of link state.
  - Linked – displays devices linked to the policy.
  - Unlinked – displays devices that are not linked to the policy.
  - Mixed linked – is not applicable when only one policy is selected.
- If you select multiple policies:
  - All – displays all available devices, regardless of link state.
  - Linked – displays devices that are linked to all selected policies.
  - Unlinked – displays devices that are not linked to any of the selected policies.
  - Mixed linked – displays devices that are linked to some of the selected policies, but not all.

2.12 Linking a Group to a Policy

Link a group to a policy to manage the group's devices with the policy.

Context

Enrollment policy link relationships to groups or devices always appear as blank and cannot link to groups. Enrollment policies are applied to a device only once, when the device enrolls in management.

As group size changes, the sort order may change which group has focus. When you link and unlink devices and policies, make sure you have the correct group selected.

The Link panel list might span multiple pages, but the toolbar actions, such as link or unlink, can affect only the items selected on the current page. Navigating from one page to another clears prior selections.

Procedure

1. On the *Policy* page, select a policy.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.
3. In the Group panel in the Link column filter, change the filter to *Unlinked* to display the groups not linked to this policy. To narrow the list, use the filter columns or click the title to sort.
4. Select the groups to add to the policies, and click *Link* on the group panel toolbar.
5. In the Link column, change the filter to *Linked* to show the groups linked to the policies.

2.13 Unlinking a Group from a Policy

Remove a group from a policy to discontinue managing the group's devices with the policy.

Procedure

1. On the Policy page, select the policies from which to remove groups.
2. On the left toolbar, click *Show/Hide Link* to display the Link panel.

   By default, the Link panel is filtered to show linked items.
3. In the Group panel in the Link column filter, change the filter to *Linked* to display the list of groups linked to the policies.
4. Select the groups you want to remove from the policy and click *Unlink* on the group panel toolbar.

2.14 Connecting a Group's Devices to Apply Policies

Apply policies to devices immediately, rather than waiting for a manual or scheduled connection.

Procedure

1. On the Group page, select groups.
2. On the top toolbar, click *Apply Policy*.

2.15 Connecting a Group's Devices to Run a Channel

Run session policies for devices in a group that has a linked session policy.

Procedure

1. On the Group page, select groups.
2. On the top toolbar, click *Run Channel*.

2.16 Exporting a Policy View

Export the policy list in its current state with any filters or sort applied. You can export to Excel, Word, and CSV.

Procedure

1. From the Policy list, click *Export View*.
2. Select *All* to export all pages of the view, or select *Current Page Only*.
3. Select the export format, and then click *OK*.

> **i** Note
>
> The Telerik controls in Afaria utilizes Excel 2003 format to export data. If you open or export a file on a machine with Excel 2007 installed a message is displayed:

```
"The file you are trying to open, [Filename].xls, is in a different format than
specified by the file extension. Verify that the file is not corrupted and is
from a trusted source before opening the file. Do you want to open the file
now?"
```

4. Click Yes to view the exported data.

2.17 Substitution Variables

Substitution variables represent specific data for devices and users in SAP Afaria.

SAP Afaria uses substitution variables to retrieve data from devices, users, applications, or directories. SAP Afaria uses the data to customize settings and policies to specific devices and users.

Some substitution variables are associated with specific tenants. If devices move from one tenant to another, the substitution variables that apply to devices might change.

Types of Substitution Variables [page 30]
SAP Afaria represents four types of data with substitution variables: client, directory, system, and user.

Creating User Variables in the Device List [page 32]
You can create a user variable using the device list in the Afaria Administration console.

Creating User Variables in Configuration Policies [page 33]
You can create a user variable using configuration policies in Afaria Administration console.

Creating Directory Variables in the Device List [page 33]
You can create a directory variable using the device list in the Afaria Administration console.

Creating Directory Variables in Configuration Policies [page 33]
You can create a directory variable using configuration policies in Afaria Administration console.

Adding Substitution Variables to Application Policies [page 34]
You can add substitution variables to application policies for iOS and Android devices.

Related Information

Editing a Device [page 308]
Creating a Configuration Policy for Android [page 48]
Creating a Configuration Policy for iOS [page 130]
Creating a Configuration Policy for Windows Phone [page 225]
Creating an Enrollment Policy for Android [page 37]
Creating an Enrollment Policy for iOS [page 172]
Creating an Enrollment Policy for Windows Phone [page 238]

2.17.1 Types of Substitution Variables

SAP Afaria represents four types of data with substitution variables: client, directory, system, and user.

Type	Description
Client	Client substitution variables represent data from secure user prompts on Android devices. Devices can substitute client substitution variables into policies when the policies are applied on the devices. Devices encrypt and store client substitution variables, but do not send the data from client substitution variables to the SAP Afaria server.
Directory	Directory substitution variables represent data collected by SAP Afaria from AD or LDAP directories. Directory substitution variables are case-sensitive and must match the attribute name in the directory. Directory variables support directory schema extensions but do not support binary or octal formats. Directory substitution variables for the system tenant are available to all tenants, otherwise the variable is available only to the tenants in which the administrators create it.

Type	Description
System	System substitution variables represent data from devices. SAP Afaria collects this data automatically from devices. System substitution variables are predefined in SAP Afaria and available to all tenants.
User	User substitution variables represent data from users. SAP Afaria collects this data from values that users enter into device prompts. User substitution variables that you create for the system tenant are available to all tenants, otherwise the variable is available only to the tenants in which you create it. If you create a user substitution variable for the system tenant, the same variable cannot be created in another tenant. If you create a user substitution variable for the system tenant that is already defined in another tenant, the system tenant claims ownership of the variable and makes the variable available to all tenants. If you delete the variable from the system tenant, it reverts back to the original tenant ownership and is no longer available to all tenants.

System Variables [page 31]

2.17.1.1 System Variables

Variable Name	Variable Structure	Description
AfariaDeviceID	%S.AfariaDeviceID%	• The ID of the device
EUSSPDomain	%S.EUSSPDomain%	• The domain of the Self-Service Portal
EUSSPUser	%S.EUSSPUser%	• The Self-Service Portal user name for the user
ExchangeDomain	%S.ExchangeDomain%	• The domain of the Exchange server
ExchangeID	%S.ExchangeID%	• The ID for the managed Exchange account
ExchangePassword	%S.ExchangePassword%	• The password for the managed Exchange account
ExchangeUser	%S.ExchangeUser%	• The user name for the managed Exchange account
ICCID	%S.ICCID%	• The unique serial number of the SIM card in the device
IMEI	%S.IMEI%	• The International Mobile Station Equipment Identity of the device

Variable Name	Variable Structure	Description
NotificationAddress	%S.NotificationAddress%	• The email address or phone number that the user enters as a notification address
Product	%S.Product%	• The device type
SerialNumber	%S.SerialNumber%	• The serial number of the device
UDID	%S.UDID%	• The Unique Device Identifier of the device • Applies only to iOS devices
UserName	%S.UserName%	• The user name associated with the device
Version	%S.Version%	• The version of the OS on the device
WiFiMAC	%S.WiFiMAC%	• The Wi-Fi MAC address of the device

2.17.2 Creating User Variables in the Device List

You can create a user variable using the device list in the Afaria Administration console.

Procedure

1. On the *Device* page, select a device.
2. Click the *Edit* button.
3. In the *Substitution* table, click *Add*.
4. In the *Type* field, select *USR: User Defined*.
5. In the *Variable* field, enter the name of the user variable.
6. In the *Value* field, enter the value for the user variable.
7. Click the check mark.

2.17.3 Creating User Variables in Configuration Policies

You can create a user variable using configuration policies in Afaria Administration console.

Procedure

1. In the Afaria Administration console, create or edit a configuration policy.
2. Navigate to a page that includes variables (for example, *Exchange ActiveSync*).
3. Click the *Substitution* link.
4. In the *Substitution* window, click *Add*.
5. In the *Type* list, select *USR*.
6. In the *Variable* field, enter the name of the user variable.
7. Click the check mark.

2.17.4 Creating Directory Variables in the Device List

You can create a directory variable using the device list in the Afaria Administration console.

Procedure

1. On the *Device* page, select a device.
2. Click the *Edit* button.
3. In the *Substitution* table, click *Add*.
4. In the *Type* field, select *DIR: Directory*.
5. In the *Variable* field, enter the name of directory variable.
6. Click the check mark.

2.17.5 Creating Directory Variables in Configuration Policies

You can create a directory variable using configuration policies in Afaria Administration console.

Procedure

1. In the Afaria Administration console, create or edit a configuration policy.

2. Navigate to a page that includes variables (for example, *Exchange ActiveSync*).
3. Click the *Substitution* link.
4. In the *Substitution* window, click *Add*.
5. In the *Type* list, select *DIR*.
6. In the *Variable* field, enter the name of the directory variable.
7. Click the check mark.

2.17.6 Adding Substitution Variables to Application Policies

You can add substitution variables to application policies for iOS and Android devices.

Procedure

1. In the Afaria Administration console, create or edit an application policy.
2. Click *Configuration*.
3. (Optional) To import a text file that contains substitution variables, perform the following tasks:
   a. Select *Text (file)*.
   b. Click *Browse*.
   c. Navigate to the text file and click *Open*.
4. (Optional) To add a substitution variable, perform the following tasks:
   a. Select *Text*.
   b. Click *Edit*.
   c. Either type the substitution variable using the `%U.SampleHere%` syntax or click *Substitution* to select a substitution variable
   d. Click *Save*.
5. Click *Save*.

2.17.7 Adding Substitution Variables to Configuration Policies

You can add substitution variables to configuration policies for Android, iOS, Windows Phone, and Windows DM (Windows 8.1 or higher) devices.

Procedure

1. In the Afaria Administration console, create or edit a configuration policy.
2. Click the *Substitution* link beside an applicable field.

3. In the *Type* list, select the type of substitution variable to filter the list.
4. In the variable list, select the substitution variable and click *Select*.
5. Save the policy.

2.17.8 Adding Substitution Variables to Enrollment Policies

You can add substitution variables to enrollment policies.

Procedure

1. In the Afaria Administration console, create or edit an enrollment policy.
2. Click *Variable*.
3. Click *Add*.
4. In the *Variable* list, select the variable.
5. In the *Device Prompt* field, type the message that devices display to prompt users to enter a value for the variable.
6. In the *Entry Mask*, list select whether devices hides the values that users add for the variable.
7. Click the check mark.
8. Click *Save*.

2.17.9 Rules for Substitution Variables

SAP Afaria enforces rules for creating, naming, and deleting substitution variables.

Rules for creating substitution variables:

- If you add substitution variables for iOS or Android devices on the Policy or Devices page, the substitution variables are added even if you do not save the policy or device changes.
- You need editing permission to add user or directory substitution variables on the Policy and Devices pages.
- For a non-system tenant, names for user and directory substitution variables must be unique for the tenant.

Rules for naming substitution variables:

- The length must be 1 to 80 characters.
- You cannot have a period as the second character.
- You cannot use XML characters or spaces.

Rules for deleting directory variables:

- If you delete substitution variables on the Policy or Devices page, the substitution variables are deleted even if you do not save the policy or device changes.

- You need editing permission to delete user or directory substitution variables on the Policy and Devices pages.
- If the substitution variable is deleted but a policy still references it, the substitution variable returns the literal string that is in the policy.

2.17.10 Substitution Variables Examples

Functionality	Substitution Variables
Microsoft Exchange email account	• User = %S.UserName% or %S.ExchangeID% • Email address = %S.ExchangeID%@<Exchange Server domain>
Exchange 365 email account	• User = %S.UserName%@<Exchange 365 domain> • Email address = %S.ExchangeID%

2.18 Android Policies

Creating an Enrollment Policy for Android [page 37]
Create a policy for enrolling Android devices in Afaria management.

Android Enterprise Application Policies [page 39]
Android enterprise application policies define which enterprise applications are available for devices to browse and install from the SAP Afaria client app list.

Android Market Application Policies [page 44]
Android Market application policies define which Google Play applications are available for devices to browse and install from the Afaria application app list.

Creating a Configuration Policy for Android [page 48]
Create a policy for scheduling device connections, collecting inventory, and configuring device settings for Android devices.

2.18.1 Creating an Enrollment Policy for Android

Create a policy for enrolling Android devices in Afaria management.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Android*.
2. On the Summary page, enter the policy name and a description for the policy.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in the Afaria application to support duplicate policy names are compatible with Afaria 6.6 and Afaria 7 servers.
3. In the Code field, click *Add* and define the code properties:
   - State – indicate whether devices are prevented from enrolling if the code is disabled at enrollment time. If you do not want to use the code yet, set the state to disabled and enable it later.
   - Portal Only – indicate whether the code is valid only when used with Afaria Self-Service Portal enrollment.
   - URL Service – select your preferred URL shortening service, as enabled on the *Server* > *Configuration* > *Enrollment Code* page.
     The Google service produces case-sensitive codes.
   - (Optional) Expiration Date – by default, expiration occurs at the end of the selected day. If you do not specify a date, the code does not expire. Devices are prevented from enrolling if the code is expired at enrollment time.
4. In the Code field, at the end of the line you are editing, click the *Save* icon to generate an enrollment code and a creating date.
5. On the General page, define the policy for enrolling the devices.
   - Server Address – Afaria server address or relay server address. The value, which you can change here, is initially populated by the Address for Client Communication value, as defined on the *Server* > *Configuration* > *Device Communication* page.
   - (Optional) FCM Sender ID/GCM Project ID – configure the Afaria client for Afaria-based Firebase Cloud Messaging (FCM) push notifications. FCM replaces Google Cloud Messaging (GCM). FCM Sender ID is the new name for the GCM Project ID parameter.
   - (Optional) Channel – default channel or channel set for the devices to request when they connect to the SAP Afaria server. For Android devices to appear on the list, the channels must exist and be published.
   - (Optional) Connection – select *automatic connection after install* to have the device initiate its first connection to the server without requiring user interaction.

- (Optional) Certificate – select to generate an identity certificate after the initial connection to Afaria server, and use this certificate for future authentications against the server and as the SSL client certificate for all future https connections. Identity certificates are supported with the Afaria managed authentication option for the enrollment and package servers.
  Identity certificates use only the Certificate Authority server assigned to the enrollment server, and require the enrollment server to be configured as the CA proxy. This option is not available in the Afaria Administration console, and is available in `<EnrollmentServer>\program files\AIPS\bin \ServerSCEPtest.exe`. It is set to On, by default, on new Afaria installations and upgrades.

  > **i Note**
  >
  > Identity certificates are supported only on 2008 CA servers, for Android versions 4.x and above. To support identity certificates, the Afaria application on the device must be version SP3 or above.

- If automatically creating a name for enrolling devices, select naming options:
  - Optional Prefix – enter a prefix to use for the name. For example "Sales_".

    > **i Note**
    >
    > The optional prefix is temporary for Android devices. This prefix is removed from the device ID during the next device connection.

  - Data Column – select a data item to concatenate with the prefix. The list includes predefined columns, the user name variable, and any additional user-defined substitution variables you defined. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
    If you select a data item that is based on a user's response to a user prompt that you add to the enrollment policy, the user's response forms the name, even if it is inaccurate. For example, if you prompt for an e-mail address and the user incorrectly types the address, the name contains the incorrect address, even if the correct address is later stored in inventory.

  Selecting an item that requires user prompts automatically adds the variable to the policy's Variable page.

6. On the Group page, select any groups to populate when devices enroll.

   A device receives the group's linked policies.

   Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of that group's definition criteria. Upon execution of the Dynamic Group Refresh schedule, if the device does not meet the group criteria, it is removed from the group.

7. On the Variable page, click *Add* to select any variables to populate during enrollment. Users are prompted on the device during enrollment.

   Define the variable prompts:

   - Variable – from the database, the variable to populate with the user's response.
   - Device Prompt – the text for the user-facing prompt.
   - Entry Mask – indicate whether the entry at the device is masked with asterisk (*) characters as the user types.

   Automatic Naming Data for Android Enrollment Policies [page 39]
   Automatic naming data columns include predefined columns, the user name variable, and any additional user-defined substitution variables you defined.

2.18.1.1 Automatic Naming Data for Android Enrollment Policies

Automatic naming data columns include predefined columns, the user name variable, and any additional user-defined substitution variables you defined.

Columns include:

- Device Serial Number
- Device Sync Name
- Device type – concatenation of device OS and platform version.
- IMEI/MEID/ESN – for GSM devices, IMEI; for CDMA devices, MEID; for non-telephony devices, serial number.
- International Mobile Subscriber Identity (IMSI) Number.
- Telephone Number – blank for non-telephony devices.
- UserName – variable. User is prompted for a value during enrollment. Review the device prompt text and mask on the enrollment policy's Variable page.

2.18.2 Android Enterprise Application Policies

Android enterprise application policies define which enterprise applications are available for devices to browse and install from the SAP Afaria client app list.

Enterprise applications are produced by third-party entities and are delivered from the SAP Afaria package server. Application packages include:

- Identifying information for the application
- (Application onboarding) File or data for application onboarding data provisioning

Preparing Android Devices for Application Management [page 40]
Enable applications from unknown sources and enroll Android devices in Afaria management.

Preparing for Android Enterprise Application Management [page 40]
For each enterprise-developed application, use Android development procedures to make compiled applications available for SAP Afaria use.

Creating an Application Policy for Android Enterprise Applications [page 40]
Create policies for managing enterprise-developed applications on Android devices. For Samsung Advanced Enterprise Security (AES) devices that use the Samsung-signed Afaria application, you can create a required enterprise application for silent installation that the user cannot remove unless you change the application's attribute to optional and redeliver the policy.

Deploying Android Enterprise Applications [page 42]
Deploy Android enterprise applications by deploying the application policy. Use the application list in Afaria and launch a Package-Server-based installation.

Removing an Android Required Enterprise Application from a Device [page 43]
For required enterprise applications installed on Samsung AES devices that have the Samsung-signed Afaria application, remove a required enterprise application to prevent its use on the device. The user cannot remove it unless you change the application's attribute to optional and redeliver the policy.

2.18.2.1 Preparing Android Devices for Application Management

Enable applications from unknown sources and enroll Android devices in Afaria management.

Procedure

1. To allow enterprise application deployment, ensure that devices allow installing applications from unknown sources. On the 2.x and 3.x devices, click *Settings* > *Applications* and enable unknown sources. On 4.x devices, click *Settings* > *Security* and enable unknown sources.
2. Ensure that devices have installed the Afaria application.
3. Ensure that devices have a configuration policy that has inventory enabled.
4. Ensure that devices have either a configuration policy that configures C2DM messaging or have an SMS address on their device record.

2.18.2.2 Preparing for Android Enterprise Application Management

For each enterprise-developed application, use Android development procedures to make compiled applications available for SAP Afaria use.

Procedure

1. Make a copy of the compiled application (`.apk`) available to the administrator responsible for creating application policies.
2. On the Policy page, create an application policy for the application.

2.18.2.3 Creating an Application Policy for Android Enterprise Applications

Create policies for managing enterprise-developed applications on Android devices. For Samsung Advanced Enterprise Security (AES) devices that use the Samsung-signed Afaria application, you can create a required enterprise application for silent installation that the user cannot remove unless you change the application's attribute to optional and redeliver the policy.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

The Configuration page is reserved for application onboarding data provisioning and is not part of this procedure. See topic *Provisioning Data for iOS and Android Applications* for more details.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Application* > *Android Enterprise*.
2. On the Summary page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in the Afaria application to support duplicate policy names and multiple categories are compatible with Afaria 6.6 and Afaria 7 servers.
3. Enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished.
   - Featured – tag the application as featured, which means it appears in a ticker on the home page of the device.
4. On the General page, define an application's information, and wait for it to populate the information box before continuing.
   - Install – choose optional or required. The required attribute affects only Samsung-signed Afaria devices. It installs the application silently at the device, without user interaction, and the user cannot remove it. To remove an Android required enterprise application, use a configuration policy.
   - KNOX Container App – Select if the application is only to be available for installation in a device's KNOX container.
   - Start Required App After Install – Select if you want the application to start automatically following installation. This option is only available if you choose *Required* as the *Install* option on this page.
   - APK – click *Browse* to locate and upload the application (`.apk`). If an application image is detected inside the APK file, it appears as the Application Icon.
     The APK file path is relative to the administrator user's workstation. The package server does not serve an application policy without the APK file details, to the connecting devices.
   - Artwork (512x512px) – click *Browse* to locate and upload the image, which appears as the Featured Application Artwork.
     Artwork supports PNG and JPEG formats with a resolution of 512x512 pixels.
5. (Optional) On the Categories page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.
6. (Optional) Select *Yes* or *No* to indicate whether the selected category is a featured category.
7. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note, if required.

> **Note**
>
> The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. It is recommended that you use smaller image files of size up to 100KB, to enable easy download and to minimize data traffic.
>
> The recommended resolution for the category image on an Android device is up to 1920 x 1080 pixels. The category image is scaled to the required resolution, without changing the aspect ratio, and is then center-cropped.

8. (Optional) In the Available Categories list, make changes by selecting a category and clicking *Edit*, *Delete*, *Inspect Image* or *Clear Image*.

   If you delete a category that is attached to another policy, the category is also deleted from the referring policy.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking *Clear Image* removes the image associated with the Available Category.
9. (Optional) In the Pre-defined Categories list, make changes by selecting a category and clicking *Edit*, *Inspect Image* or *Clear Image*.

   Enterprise, Play Store and All are the Pre-defined System Categories listed.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking the Clear Image removes the image associated with the Pre-defined Category.
10. (Optional) On the Description Detail page, enter a description for the application and modify the display name.

    The display name and the version of the application are automatically updated when you upload the application package on General page.
11. Click *New* to browse to and select the application screen shot that appears on the device.

    You can upload as many as eight screen shots from which you can select the application image to appear on the device.

> **Note**
>
> The appearance of the uploaded image may change, depending on the size of the image and the browser settings. The maximum image size allowed is 1MB.

2.18.2.4 Deploying Android Enterprise Applications

Deploy Android enterprise applications by deploying the application policy. Use the application list in Afaria and launch a Package-Server-based installation.

Context

After installing an application, only the user can remove it, unless the device is a Samsung AES device and you use a configuration policy with Samsung application properties to remove it.

Procedure

1. On the Policy page, link the application policy to a group.
2. On the Group page, connect the group's devices to apply policies.
   The device connects and reports its current software inventory.
3. On the device, the user opens Afaria and can browse the list of applications by going to the Apps page. When the user opens the Apps page, the device connects to the package server. The server refreshes the device's list of applications.
4. The user browses the application list and installs the application.

   If you use the optional category attribute, applications are grouped by category.
5. On the device, the user clicks *Install* to launch an installation.

   Afaria connects to the Package Server, downloads the application, and initiates the installation.

2.18.2.5 Removing an Android Required Enterprise Application from a Device

For required enterprise applications installed on Samsung AES devices that have the Samsung-signed Afaria application, remove a required enterprise application to prevent its use on the device. The user cannot remove it unless you change the application's attribute to optional and redeliver the policy.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *Android*.
2. Define the policy with these *Samsung* > *Application policy* page properties:
   - Samsung Application Enable/Disable Policy – add the application to the list and set the Uninstallation Enable/Disable attribute to enabled.
   - Samsung Application Install/Remove/Update Policy – add the application package name to the list and set the Policy attribute to remove.
3. On the Policy page, link the configuration policy to a group.
4. On the Group page, send a command to the group to connect the group's devices to apply policies.
   The device connects and reports inventory. The server delivers instructions to remove the application from the device.

Results

After a subsequent connection, the *Device Inspector > Managed Software* inventory will show the application is removed.

2.18.3 Android Market Application Policies

Android Market application policies define which Google Play applications are available for devices to browse and install from the Afaria application app list.

Commercial applications are delivered from the Google Play commercial market. Application packages include:

- Identifying information for the application
- (Application onboarding) File or data for application onboarding data provisioning

Preparing Android Devices for Application Management [page 40]
: Enable applications from unknown sources and enroll Android devices in Afaria management.

Preparing for Android Google Play Application Management [page 45]
: For each Google Play application of interest, collect required application information.

Creating an Application Policy for Android Google Play Apps [page 45]
: Create policies for managing applications from Google Play.

Deploying Android Google Play Apps [page 47]
: Deploy Android Google Play applications by deploying the application policy. On the device's SAP Afaria client, users can use the application list to browse the list of applications and launch a Google Play installation.

2.18.3.1 Preparing Android Devices for Application Management

Enable applications from unknown sources and enroll Android devices in Afaria management.

Procedure

1. To allow enterprise application deployment, ensure that devices allow installing applications from unknown sources. On the 2.x and 3.x devices, click *Settings* > *Applications* and enable unknown sources. On 4.x devices, click *Settings* > *Security* and enable unknown sources.
2. Ensure that devices have installed the Afaria application.
3. Ensure that devices have a configuration policy that has inventory enabled.
4. Ensure that devices have either a configuration policy that configures C2DM messaging or have an SMS address on their device record.

2.18.3.2 Preparing for Android Google Play Application Management

For each Google Play application of interest, collect required application information.

Procedure

Use a Web search or other means to locate and record an application name, as defined by the developing entity.

You can use the Google Play site from your desktop to discover the package name by selecting an application and extracting the package name from the URL. For example, the application package name for the Kindle for Android application is com.amazon.kindle.

You can use SAP Afaria to discover the package name by collecting software inventory from a device that has the application of interest installed. The application package name is reported as the software name.

2.18.3.3 Creating an Application Policy for Android Google Play Apps

Create policies for managing applications from Google Play.

Prerequisites

Complete the procedure to prepare for a Google Play application, which includes recording the application name.

The device user must have an account with Google Play. Google Play user agreements and costs are independent of SAP Afaria operations.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

The Configuration page is reserved for application onboarding data provisioning and is not part of this procedure. See topic *Provisioning Data for iOS and Android Applications* for more details.

Procedure

1. On the top toolbar, click *New* > *Application* > *Android Market*.

   Google Android Market is renamed to Google Play.
2. On the Summary page, enter the policy name and note and indicate whether the policy is published or unpublished.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Connecting devices receive only published policies.
3. (Optional) Select *Featured* to tag the application as featured, which means it appears in a ticker on the home page of the device.
4. On the General page, define an application's information, and then click *Update* to populate the Information box.
   - Package – application name, such as com.amazon.kindle.
   - Deploy for Android for Work devices – For Android for Work applications. Select to set the application to be an Android for Work application. By default, Android for Work apps are deployed to all managed users.
     If you select this option, the *Required* checkbox becomes available.
   - Required – For Android for Work applications. Select to install the application in the managed profile when the app policy is applied to the device.
     If you clear this checkbox, the app is treated as an optional app. When the app policy is applied to the device, the app is displayed as an available app in the managed profile and can be installed by the device user if desired.
   - Accept all changes – Select to accept the permissions on behalf of end-users. This supports the silent installation of Android for Work applications and means users do not have to accept permissions for managed applications.

     > **i Note**
     >
     > After you accept the initial set of permissions for the first time, only new permissions are displayed. If there are no new permissions, the `All permissions for this application have been accepted or there are no permissions available for this application.` message is displayed.

   Data retrieval is subject to data availability from the Google Play.
5. (Optional) On the Categories page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.
6. (Optional) Select *Yes* or *No* to indicate whether the selected category is a featured category.
7. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note, if required.

   > **i Note**
   >
   > The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. It is recommended that you use smaller image files of size up to 100KB, to enable easy download and to minimize data traffic.

> The recommended resolution for the category image on an Android device is up to 1920 x 1080 pixels. The category image is scaled to the required resolution, without changing the aspect ratio, and is then center-cropped.

8. (Optional) In the Available Categories list, make changes by selecting a category and clicking *Edit*, *Delete*, *Inspect Image* or *Clear Image*.

   If you delete a category that is attached to another policy, the category is deleted from the referring policy also.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking *Clear Image* removes the image associated with the Available Category.

9. (Optional) In the Pre-defined Categories list, make changes by selecting a category and clicking *Edit*, *Inspect Image* or *Clear Image*.

   Enterprise, Play Store and All are the Pre-defined System Categories listed.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking *Clear Image* removes the image associated with the Pre-defined Category.

10. (Optional) On the Description Detail page, enter a description for the application and modify the display name.

    The display name of the application is automatically updated when you upload the application package on General page.

2.18.3.4 Deploying Android Google Play Apps

Deploy Android Google Play applications by deploying the application policy. On the device's SAP Afaria client, users can use the application list to browse the list of applications and launch a Google Play installation.

Prerequisites

The device user must have an account with Google Play. Google Play user agreements and costs are independent of SAP Afaria operations.

Context

After installing an application, only the user can remove it, unless the device is a Samsung AES device and you use a configuration policy with Samsung application properties to remove it.

Procedure

1. On the Policy page, link the application policy to a group.
2. On the Group page, connect the group's devices to apply policies.
   The device connects to SAP Afaria and reports its current software inventory.
3. On the device, the user opens the SAP Afaria client and can browse the list of applications by going to the Apps page.

   If you use the optional category attribute, applications are grouped by category.
4. On the device, the user clicks *Install* to launch an installation.
   The SAP Afaria client closes and the device connects to Google Play, where the user can initiate the installation.

   For Android for Work:

   After a device is enrolled for Android for Work, an Android for Work application is installed when the Afaria administrator pushes the application to the device or when the Android for Work scheduler runs on the device.

   When an application contains restrictions set by the administrator, if the application is installed but the restrictions are not sent from the Afaria Server to the device, the application remains hidden on the device and the `Trying to connect to server to check restrictions for this app <app name>` message is displayed. In such cases, the user must wait until the restrictions are sent to the device. Or the user can open the SAP Afaria client and click *Connect*.

2.18.4 Creating a Configuration Policy for Android

Create a policy for scheduling device connections, collecting inventory, and configuring device settings for Android devices.

Context

The policy includes multiple pages, such as *Summary* and *Schedule* and device-specific policy settings. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the *Policy* page, on the top toolbar, click *New* > *Configuration* > *Android*.
2. On the *Summary* page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.

3. Enter or select the remaining properties.
    - *Note* – add a description for the policy.
    - *State* – set to published or unpublished. Connecting devices receive only published policies.
    - *Priority* – set a user-defined value to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
    - *Authentication* – validate the user identity against your authentication authority before allowing the policy to run. This option is available only if you have authentication enabled on the server, as defined on the *Server* > *Configuration* > *Security* page.
    - *Inventory* – select the inventory type to collect. You can view inventory information on the Device page's Device Inspector.
        - *Do not collect inventory* – no inventory collection.
        - *Hardware only* – scan collects data relating to the device's physical components, such as processors and memory cards.
        - *Software and Hardware* – scan collects hardware data and data for installed software.
4. (Optional) To configure a daily connection, define *Schedule* page properties.
5. (Optional) Configure policy pages according to your requirements.

Schedule Page [page 50]
: For Android configuration policies, sets a schedule the SAP Afaria client uses to connect to SAP Afaria and apply the configuration policy. On the Schedule page, you can create, select, edit, and delete schedules. You can also define the number of times the server should retry the scheduled task, if the task fails.

Android Pages [page 51]
: The policies in the Android page group apply to all supported Android devices. This page group includes pages for configuring security, Bluetooth, Wireless WAN, and device communications.

Android for Work Pages [page 55]
: The policies in the Android for Work page group apply to all Android devices that support Android for Work. This page group includes pages for configuring Google Chrome, setting up Exchange Account policies, application restrictions, security and wi-fi.

NitroDesk Pages [page 67]
: Configure NitroDesk TouchDown clients to connect to an enterprise Microsoft Exchange environment.

LG Pages [page 73]
: Configuration policy LG features let you use Afaria Advanced Enterprise Security (AES) on LG Android devices that support enterprise device management, and have installed the LG-signed Afaria application. The application is available from either the LG Apps store or Google Play.

Samsung KNOX Standard Pages [page 80]
: Samsung KNOX Standard policies allow you to use Samsung for Enterprise on Samsung devices that support enterprise device management, and have the Samsung-signed Afaria application installed. The application is available from either the Samsung Apps store or Google Play.

Samsung KNOX Pages [page 96]
: Use the policy pages in the Samsung KNOX page group to configure policies on KNOX-capable Samsung devices.

Post-Session Processing for Policies [page 110]
: For configuration policies, some configuration items require processing after the Afaria session ends.

Related Information

Substitution Variables [page 29]

2.18.4.1 Schedule Page

For Android configuration policies, sets a schedule the SAP Afaria client uses to connect to SAP Afaria and apply the configuration policy. On the Schedule page, you can create, select, edit, and delete schedules. You can also define the number of times the server should retry the scheduled task, if the task fails.

To create a new schedule, click *New* to open the Schedule Editor. To edit a schedule, highlight a schedule and click *Edit*. To set the number and frequency or retries, click *Retries* and configure the settings in the Configuration Policy > Retries dialog box.

General Settings

Setting	Description
Selected Schedule	The active schedule for the policy. To set a schedule as the selected schedule, highlight the schedule in the schedule list and click *Select*. To clear the field, click *Clear*.

Retry Settings

Setting	Description
On error retry	The number of times the SAP Afaria client tries to connect with the server after an error. Available from the *Retries* link.
Every	The frequency of retries from 0 to 720 minutes. Available from the *Retries* link.

Schedule Editor Settings

Setting	Description
Schedule	A name for the schedule

Setting	Description
Note	A description for the schedule. Optional.
Type	The schedule type
Rate: Start Time	The hour the schedule is scheduled to start. Use the Time Picker to select a start time.
Rate: Every	The frequency of the schedule. Set the frequency from 1 to 365 days or select the days of the week
Rate: If missed	Select *Run at Startup* to apply the configuration policy at start-up if the client was not running at the defined start time.
Range: Limit Dates	Select to apply the configuration policy only between two dates
Range: Starting	The start date for the range. Use the Date Picker to select a date.
Range: Ending	The end date for the range. Use the Date Picker to select a date.
Repeat: Enable	Select to repeat the application of the configuration policy for until a specified hour or for a specified duration
Repeat: Every	The interval between repetitions of the schedule
Repeat: Until/For	Allows you to repeat the schedule either until a specified hour or until the end of a specified duration
Randomize: Randomize By	Allows you to set the interval for randomizing the start time for the scheduled task.

2.18.4.2 Android Pages

The policies in the Android page group apply to all supported Android devices. This page group includes pages for configuring security, Bluetooth, Wireless WAN, and device communications.

Security Page [page 52]
: For Android devices, sets properties for passwords. For remote device unlock authority, Afaria requires exclusive device administrator privileges for password management. The properties are set only if the device has a password enabled.

Bluetooth Page [page 54]
: For Android devices, sets properties for using Bluetooth capabilities.

Wireless LAN Page [page 54]
: For Android devices, sets properties for a single wireless LAN (WLAN) connection per session. To set properties for multiple connections, connect the device for multiple sessions, and define one Wireless LAN connection in each separate session.

Device Communications Page [page 55]

For Android devices, sets configuration properties to connect to the Afaria server, either directly or through its relay server proxy.

2.18.4.2.1 Security Page

For Android devices, sets properties for passwords. For remote device unlock authority, Afaria requires exclusive device administrator privileges for password management. The properties are set only if the device has a password enabled.

All Devices

Setting	Description
Password required	Yes or No. Select *Yes* to enable password protection. Enable this field to configure the remaining password-related fields.
Restrict policies until password is set	Yes or No. Select *Yes* to apply policies only after the user has set a password on their device.
Password format	The password format required: Alphabetic, Numeric, Alphanumeric, or Complex (for Android 3.x devices)
Minimum password length	The minimum length for the password. Range is 4 – 16 characters.
Invalid password attempts before the device hard resets	The number of times a user can enter a wrong password before the device hard resets. To remove this setting from a device after it has been applied, change the number of password attempts to "0" and then reapply the policy. This ensures the device will never hard reset due to a failed password entry.
Maximum idle time until lock	The maximum time that the user can configure the device to remain idle before the device screen locks. The options are: 15 sec, 30 sec, 1 min, 2 min, 5 min, 10 min, and 30min.

Android 3.x and Above Devices

> **i** Note
>
> For properties set to 0, the property does not restrict the policy. If you previously deployed a policy using a nonzero value for this property, and now want to deploy a policy that ignores the property, set the value to 0.

Setting	Description
Minimum password letters	Minimum number of letters in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Minimum password lowercase	Minimum number of lowercase letters in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Minimum password uppercase	Minimum number of uppercase letters in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Minimum password non-letter	Minimum number of non letter characters in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Minimum password numeric	Minimum number of numbers in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Minimum password complex characters	Minimum number of symbols in the password. Range is 0 – 16. This option is only available if the "Complex" password format is selected.
Password history	The number of passwords stored on the history list. Range is 1 – 100. Default is 10.
Password expiration timeout in days	Number of days a password remains valid. Range is 0 – 365. 0 means there is no restriction (the password does not expire). Default is 90 days.
Encrypt storage	Yes or No. Select *Yes* to encrypt device memory. Select *No* to leave device memory unencrypted.

Android 4.x and Above Devices

Setting	Description
Camera disabled	Yes or No. Select *Yes* to disable the camera on ICS devices. Default is "Yes". When device users try to use the camera on their device, the device displays the following message: `Camera is disabled by server policy`.
Allow Afaria client screen shots	Yes or No. Select *Yes* to allow screen shots of the Afaria client. Default is "No". Selecting *No* prevents users or the Android operating system from capturing an image of the Afaria client. Allowing screen shots is a security risk because a screen shot could include sensitive corporate information.

Android 5.x and Above Devices

Setting	Description
Smart Lock disabled	Yes or No. Select *Yes* (the default) to disable Smart Lock on Android 5.x and higher devices. Smart Lock is an Android feature that allows users to unlock their devices automatically.

2.18.4.2.2 Bluetooth Page

For Android devices, sets properties for using Bluetooth capabilities.

Setting	Description
Enable Bluetooth	Yes or No. Select *Yes* to enable the device's Bluetooth radio.
Scan Devices	Yes or No. Select *Yes* to enable scanning for nearby discoverable devices.

2.18.4.2.3 Wireless LAN Page

For Android devices, sets properties for a single wireless LAN (WLAN) connection per session. To set properties for multiple connections, connect the device for multiple sessions, and define one Wireless LAN connection in each separate session.

Some values are established by your network administrator.

Setting	Description
Enable Wifi	Yes or No. Select *Yes* to enable wireless access to a LAN. If you enable this setting, the SSID setting becomes available.
SSID	The Service Set Identifier (SSID) for the WLAN. If you enable this field, the other settings on this page become available.
Hidden SSID	Yes or No. Select *No* to broadcast the SSID. Select *Yes* to hide the SSID.
Security	The network mode used by the network. Options are: None, WEP, WPA/WPA2 PSK, and 802.1x Enterprise.
Pre-shared Key	The passphrase used to access the network.
WEP Key 1	The WEP key value

2.18.4.2.4 Device Communications Page

For Android devices, sets configuration properties to connect to the Afaria server, either directly or through its relay server proxy.

Setting	Description
Enable seed data	Select this check box to make seed data settings on this page available.
Seed data: Server	The fully-qualified host name or IP address of the Afaria server
Seed data: Relay server farm ID	If using a relay server proxy, the farm ID as defined on the *Server* > *Configuration* > *Relay Server* page.
Seed data: Relay server prefix	If using a relay server proxy, the relay server prefix as defined on the *Server* > *Configuration* > *Relay Server* page.
Seed data: Channel name	The published channel or channel set for the device to request when connecting to the Afaria server
Seed data: GCM Project ID	The GCM Project ID, now known as the FCM Sender ID, as configured in the *Server* > *Configuration* > *GCM Server* page.

2.18.4.3 Android for Work Pages

The policies in the Android for Work page group apply to all Android devices that support Android for Work. This page group includes pages for configuring Google Chrome, setting up Exchange Account policies, application restrictions, security and wi-fi.

Google Chrome Page [page 56]
: Configure settings for Google Chrome installed as part of Android for Work.

Exchange Account Policy Page [page 62]
: For a user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client.

Restrictions Page [page 63]
: For Android for Work devices, defines restrictions for user access to certain features.

Security Page [page 64]
: Configure password settings and provide certificates for the Android for Work profile on Android devices.

WiFi Page [page 65]
: Configure WiFi connections on Android for Work devices to allow users to connect wirelessly to your network. You can also choose to block users from connecting to a configured network connection.

2.18.4.3.1 Google Chrome Page

Configure settings for Google Chrome installed as part of Android for Work.

Setting	Description
Enable Google Chrome	Allows you to set Google Chrome settings for the configuration policy. Select *Enable Google Chrome* to make the settings on this page available.
Incognito Mode Availability	Available, Disabled, Forced. Incognito mode allows users to open incognito tabs in their browser session. In incognito tabs, cookies are disabled and no browser history is maintained. You can choose to enable incognito mode (*Available*), disable it (*Disabled*), or force all tabs to be opened in incognito mode (*Forced*).
Save browser history	Disable, Enable. Controls whether the browser saves the user's browsing history.
Password Manager	Not Enforced, Enabled, Disabled If you enable Password Manager, Google Chrome memorizes user passwords for future website logins. If you disable Password Manager, users cannot save passwords, nor use previously saved passwords. You can allow the user to configure the option, or you can specify that it is always on or always off.
Autofill	Not Enforced, Disabled Specifies whether the user can use the autofill feature to complete online forms. The first time a user fills out a form, Google Chrome automatically saves the entered information, such as the name, address, phone number, or email address, as an autofill entry. You can allow the user to configure the option, or you can specify that it is disabled.
Edit bookmarks allowed	Yes, No Bookmark editing allows users to add, edit, or remove items from their Google Chrome bookmarks bar.
Alternate error page	Not Enforced, Enabled, Disabled Controls whether Google Chrome suggests alternate pages to the user when the page they are trying to reach is unavailable. The user sees suggestions to navigate to other parts of the website or to search for the page with Google. This setting corresponds to the *Use a web service to help resolve navigation errors* Google Chrome setting. You can allow the user to configure the option, or you can specify that it is always on or always off.
Prerender Webpages	Not Enforced, Enabled, Disabled Pre-rendering web pages can speed up the user's browsing experience by allowing Google Chrome to pre-load and render linked pages. This setting

Setting	Description
	corresponds to the user setting *Network action predictions* on the *Privacy* section of the **Advanced** settings tab. You can allow the user to configure the option, or you can specify that it is always on or always off.
Default search provider	Not Enforced, Disabled This setting specifies whether the user can set a default search provider for the omnibox (Google Chrome's address bar) or not.
Force safe search	Yes, No Selecting *Yes* forces your users' Google searches in Google Chrome to be done with SafeSearch turned on.
Search Suggest	Not Enforced, Enabled, Disabled When users enter information into the address bar, Google Chrome can use a prediction service to help complete the web addresses or search terms. You can allow the user to configure the option, or you can specify that it is always enabled or disabled. This setting corresponds to the *Use a prediction service to help complete searches and URLs typed in the address bar* setting in Google Chrome's *Settings* page.
Safe Browsing	Not Enforced, Enabled, Disabled Specifies whether or not Safe Browsing is turned on for users. Safe Browsing helps protect users from websites that may contain malware or phishing content. You can allow users to decide whether to use Safe Browsing, or specify that it is always on or always off.
Google Translate	Not Enforced, Enabled, Disabled Lets you specify whether Google Chrome uses Google Translate, which offers content translation for web pages in languages not specified in the *Language* settings on a user's Google Chrome device. You can set Google Chrome to let users set this option in their local Google Chrome *Settings*, always offer translation, or never offer translation.
Data compression proxy	Not Enforced, Enabled, Disabled Enabling this setting can reduce cellular data usage and speed up mobile web browsing by using proxy servers hosted at Google to optimize and compress website content. You can set Google Chrome to allow the user to decide whether to use the data compression proxy, enable the data compression proxy, or disable the data compression proxy.

Proxy Settings

Setting	Description
Proxy Mode	Not Enforced, None, Auto-Detect, System, PAC Script, Manual Specifies how Google Chrome connects to the Internet. If you leave the setting as *Not Enforced*, the user can change the proxy configuration in their Chrome *Settings*. If you choose any of the other Proxy Mode options, the user can't change the configuration. The remaining options are: **None** Google Chrome always establishes a direct connection to the Internet without passing through a proxy server. A direct connection is also the default configuration for Chrome devices if you do not set a policy and the user doesn't change the configuration. **Auto-Detect** Google Chrome determines which proxy server to connect to using the Web Proxy Autodiscovery Protocol (WPAD). **System** TBD. **PAC** Proxy Auto-detect. Always use the proxy auto-config (`.pac`) file specified in the *Proxy PAC URL* field. **Manual** Sets the server specified in the *Proxy Server* field as the proxy server to handle requests from Google Chrome. If you select this option, you need to enter the URL of the proxy server in the Proxy Server URL field below. Format the Proxy Server URL as 'IP address:port', such as '192.168.1.1:3128'. Leave it empty for any other Proxy Mode setting.
Proxy PAC URL	Available if *PAC Script* is selected. Specify the URL of the `.pac` file to use for network connections.
Proxy Server	Available if Manual is selected.

If there are any URLs that should bypass the proxy server that handles other user requests, enter them in the *Proxy Bypass URLs* list. You can set up multiple URLs.

To define a Proxy bypass URL, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the proxy bypass URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the proxy bypass server.

URL Blacklist and Whitelist Settings

A blacklist prevents Chrome devices from accessing specific URLs. A whitelist explicitly allows Chrome devices to access specific URLs. You can enter up to 1000 URLs for each list. URLs take the following form:

- Each URL must consist of a valid host name (such as google.com), an IP address, or an asterisk (*) in place of the host. The asterisk functions as a wildcard, representing all host names and IP addresses.

- URLs can also include:
  - The URL scheme, which is http, https, or ftp, followed by ://.
  - A valid port value from 1 to 65535.
  - The path to the resource.
  - Query parameters.

> **Note**
>
> - To optionally disable subdomain matching, put an extra period before the host.
> - You cannot use user:pass fields, such as http://user:pass@ftp.example.com/public/file.xyz. Instead, enter http://ftp.example.com/public/file.xyz.
> - When both blacklist and blacklist exception filters apply (with the same path length), the exception filter takes precedence.
> - If an extra period precedes the host, the policy filters exact host matches only.
> - The policy searches wildcards (*) last.
> - Optional query parameters consist of a set of key-value and key-only tokens delimited by '&'. The key-value tokens are separated by '='. A query token can optionally end with a '*' to indicate prefix match. Token order is ignored during matching.
>
> For examples of valid whitelist and blacklist specifications, search for "Set Chrome policies for users" at support.google.com.

To add a URL to the blacklist or whitelist, click *Add* from the appropriate toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the proxy bypass URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site you want to allow or deny.

Managed Bookmark Settings

To add a bookmark, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to add the bookmark to users' available bookmarks when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
Name	Enter a name for the bookmarked site.
URL	The URL of the site to bookmark.

Geolocation Settings

Sets whether websites are allowed to track users' physical locations. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Location*. Tracking physical locations can be set by the user (*Not Enforced*), allowed by default (*Allow*), the user can be asked each time a website requests the physical location (*Ask*), or denied by default (*Block All*).

Cookie Settings

The *Default cookies setting* option determines whether websites are allowed to store browsing information, such as user site preferences or profile information. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Cookies*. Whether to allow cookies can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Cookie session only URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie session-only URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow or deny cookies.

Cookie blocked URLs. Allows you to specify a list of URL patterns of sites that are not allowed to set cookies. If this policy is not set, what you specify under *Default cookie settings* will be the global default, or the user can set their own configuration.

Cookie blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block cookies.

Cookie allowed URLs. Allows you to specify a list of URL patterns of sites that are allowed to set cookies. If this policy is not set, what you specify under *Default cookie settings* will be the global default, or the user can set their own configuration.

Cookie allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the cookie-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow cookies.

Image Settings

The *Default images setting* option determines whether websites are allowed to display images. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Images*. Whether to display images can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Image blocked URLs. Allows you to specify a list of URL patterns of sites that are not allowed to set display images. If this policy is not set, the user can set their own configuration.

Image blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the image-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block images.

Image allowed URLs. Allows you to specify a list of URL patterns of sites that are allowed to display images. If this policy is not set, the user can set their own configuration.

Image allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the image-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow images.

JavaScript Settings

The *Default javascript setting* option determines whether websites are allowed to run JavaScript. If you disable JavaScript, some sites may not work properly.

Sets whether websites are allowed to run JavaScript. This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *JavaScript*. Whether to allow JavaScript can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Javascript blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the JavaScript-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block JavaScript.

Javascript allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the JavaScript-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow JavaScript.

Popup Settings

The *Default popup setting* option determines whether websites are allowed to display pop-ups.

This setting corresponds to the Chrome settings under *Privacy* > *Content settings* > *Pop-ups*. Whether to allow pop-ups can be set by the user (*Not Enforced*), allowed by default (*Allow All*), or denied by default (*Block All*).

Popup blocked URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the pop-up-blocked URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to block pop-ups.

Popup allowed URLs options:

Setting	Description
Include/Exclude	Select *Include* to include the pop-up-allowed URL when the policy is run. If you select *Exclude*, the URL remains on the list but is not deployed to the device.
URL	The URL of the site for which you want to allow pop-ups.

2.18.4.3.2 Exchange Account Policy Page

For a user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client.

You can use substitution variables for most of the values defined on this page. See *Substitution Variables* for more information.

Setting	Description
Enable Exchange Account	Allows you to set Exchange Account settings for the configuration policy. Enable to make the settings on this page available.

Setting	Description
Username	User's Exchange user name
Password	User's Exchange password
Domain	User's e-mail domain for the Exchange account **i Note** This is not a required field. The domain must be specified in either the *Username* field ("user@domain" or "domain\user") or the *Domain* field. If specified in the *Domain* field, Afaria appends it to the username. If it is specified in both places and the domain is different, Afaria use the one in the username field.
Email Address	User's Exchange e-mail address
Exchange host	Fully qualified domain name for the Microsoft Exchange server
Require SSL	Select *Yes* to require the use of SSL for Exchange sessions.
Trust All Certificates	Select *Yes* to allow the device to accept certificates without user intervention.
User Certificate	To add the client certificate, click *Add Certificate*, browse to select a certificate, and then specify a password for the certificate. To add a SCEP request, click *Add request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. You may also specify an alt name for the certificate.
Signature	Signature for user-initiated messages. If left blank, the user can enter a signature.
Maximum attachment size (MB)	The maximum size of attachments in megabytes.
Enable tasks application	Select *Yes* to enable the Exchange Tasks application on the device.

2.18.4.3.3 Restrictions Page

For Android for Work devices, defines restrictions for user access to certain features.

Setting	Description
Enable Restrictions	Allows you to set restrictions for the configuration policy. Enable to make the settings on this page available.
Screen Capture	Allows you to enable or disable screen captures on the device.
Enable Camera	Allows you to enable or disable the camera on the device.

2.18.4.3.4 Security Page

Configure password settings and provide certificates for the Android for Work profile on Android devices.

Setting	Description
Enable Password	Allows you to set password settings for the configuration policy. Enable to make the password settings on this page available.
Password Quality	The password format required, either Something, Numeric, Alphabetic, Alphanumeric, or Complex.
Minimum password length	The minimum length for the password. The range is 4 – 16 characters.
Invalid password attempts before Android for Work data wipe	The number of times a user can enter a wrong password before data wipe occurs.
Maximum idle time until lock	The maximum time that the user can configure the device to remain idle before the device screen locks. The options are: 15 sec, 30 sec, 1 min, 2 min, 5 min, 10 min, and 30 min.
Password History	The number of passwords stored in the history list. The range is 1 – 100. The default is 10.
Maximum number of days until password expires	The number of days a password remains valid. The range is 0 – 365. 0 means there is no restriction (the password does not expire). The default is 90 days. **i Note** This setting is currently not enforced by Google.
Minimum password letters Complex password format only	The minimum number of letters in the password. The range is 1 – 16.
Minimum password lowercase Complex password format only	The minimum number of lowercase letters in the password. The range is 0 – 16.
Minimum password uppercase Complex password format only	The minimum number of uppercase letters in the password. The range is 0 – 16.
Minimum password non-letter Complex password format only	The minimum number of non-letter characters in the password. The range is 0 – 16.
Minimum password numeric Complex password format only	The minimum number of numbers in the password. The range is 1 – 16.
Minimum password complex characters Complex password format only	The minimum number of symbols in the password. The range is 1 – 16.

Setting	Description
Smart Lock disabled	Yes or No. Select *Yes* to disable Smart Lock. Smart Lock is an Android feature that allows users to unlock their devices automatically. Default is "No".

Certificates

Configure settings for CA certificates used to authenticate connections between the Android for Work profile and your network.

To add a certificate, click *Add* from the toolbar and set the following:

Setting	Description
Include/Exclude	Select *Include* to include the certificate when the policy is run. If you select *Exclude*, the certificate remains on the list but is not deployed to the device.
Certificate	To add the client certificate, click *Add Certificate*, browse to select a certificate, and then specify a password for the certificate. To add a SCEP request, click *Add request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. You may also specify an alt name for the certificate. **i Note** In order to install a SCEP certificate on a device, the device must have a password. If you include a SCEP request in this policy, ensure you configure password settings on this page.

2.18.4.3.5 WiFi Page

Configure WiFi connections on Android for Work devices to allow users to connect wirelessly to your network. You can also choose to block users from connecting to a configured network connection.

To remove a network configuration from the Android Client, include the item you wish to delete and delete the Network SSID. The item with that Identifier will then be deleted when the Client runs this policy.

Setting	Description
Enable Wifi	Allows you to set WiFi settings for the configuration policy. Enable to make the settings on this page available.
Include/Exclude	Allows you to include or exclude the connection profile from the configuration policy.

Setting	Description
Identifier	A system-generated ID for the network connection. This field is not editable.
Network SSID	Network Service Set Identifier (SSID). This is a name for the Wi-Fi connection as configured on the wireless router. This name is used to identify the connection in the device's Wi-Fi list. Required.
Hidden SSID	Indicates whether the SSID is hidden. If the SSID is hidden, the WiFi router does not broadcast its identity. The WiFi network is not listed on the device.
Network link security	The security protocol used to authenticate network link connections. Depending on the security protocol used, you may need one of the following: • A network WEP key 1 for WEP • A network pre-shared key for WPA/WWPA2-PSK • A CA certificate and either a client certificate or SCEP request for all version of EAP
CA Certificate	The certificate used by the router to authenticate the connection. Available if EAP is used. To add a CA certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. **i Note** A device password must be enabled.
Client certificate	The certificate used by the device to authenticate the connection. Available if EAP is used. To add a client certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. To add a SCEP request, click *Add SCEP request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. **i Note** A device password must be enabled.
Network identity value	The network identity value. Available if EAP is used.
Network password	The network password for authenticating the network connection. Available if EAP is used.
Network pre-shared key	A pre-shared key. Required when WAP/WAP2-PSK is used.
Network WEP key 1	A WEP key 1. Required when WEP is used.

2.18.4.4 NitroDesk Pages

Configure NitroDesk TouchDown clients to connect to an enterprise Microsoft Exchange environment.

TouchDown provides access to Exchange e-mail, contacts, and calendars using ActiveSync technology. Product documentation for configuring and using the TouchDown client is available on the NitroDesk Web site.

2.18.4.4.1 Configuring NitroDesk TouchDown on Android Devices

For planned NitroDesk TouchDown client users, define a configuration policy that launches the TouchDown client configuration wizard with optional license key and optional configuration data.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *Android*.

2. On the Summary page, enter the policy name, note, and remaining properties.
3. On the *NitroDesk* > *Account Configuration* page, select *Enable Account Configuration* to launch the configuration wizard.
4. (Optional) To apply a license key as purchased from NitroDesk, enter the license key.
5. Define account configuration data.

   Some data elements are optional.
6. (Optional) To override Exchange ActiveSync settings with more restrictive settings, define *NitroDesk* > *EAS Overrides* page properties.
7. (Optional) To define additional security settings for using the TouchDown client, define *NitroDesk* > *Security Settings* page properties.
8. (Optional) To define additional settings for using the TouchDown client, define *NitroDesk* > *User Setting*, *NitroDesk* > *Email Options*, or *NitroDesk* > *Calendar Options* page properties.
9. Save and publish the policy, link it to a group profile, and then connect the devices.
10. On the device, at the conclusion of the Afaria session, the TouchDown client configuration wizard launches and the user completes the configuration steps.

    For configuration data not defined in the policy, the wizard prompts the user.

    When the wizard is complete, the device connects to the e-mail server.

> **i Note**
>
> When a user is disabled in Active Directory, Afaria does not send a wipe command to the Android device to wipe NitroDesk unless an inventory scan is generated on the device and processed on the Afaria server prior to initiating the Stop management command.

2.18.4.4.2 Converting NitroDesk TouchDown Trial Clients to Licensed Clients

For current NitroDesk TouchDown trial client users, apply a license key to convert a trial TouchDown instance to a licensed instance, without reinstalling the client.

Prerequisites

A TouchDown license from NitroDesk is required for this task.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *Android*.

2. On the Summary page, enter the policy name, note, and remaining properties.
3. On the *NitroDesk* > *Account Configuration* page, select *Enable Account Configuration* to launch the configuration wizard.
4. Enter the license key.
5. Save and publish the policy, link it to a group profile, and then connect the devices.

2.18.4.4.3 Account Configuration Page

For planned NitroDesk TouchDown client users, account configuration sets properties for a new TouchDown client when launching the TouchDown client configuration wizard. For current NitroDesk TouchDown trial client users, account configuration applies an account license key to an installed trial version.

Setting	Description
Enable account configuration	Enable this check box to enable other settings on this page. Applying a policy with NitroDesk account configuration launches the TouchDown client configuration wizard on the device.
Account License Key	The license key for the TouchDown client as purchased from NitroDesk. For TouchDown trial users, applying the license key converts the trial instance to a licensed instance.
Account Configuration: User ID	The user id for the user's Exchange account
Account Configuration: Password	The password for the user's Exchange account
Account Configuration: Email Address	The e-mail address for the user's Exchange account. Optional. If not provided, the user is prompted to enter a value.
Account Configuration: Domain	The name of the network domain on which the Exchange server resides
Account Configuration: Exchange server	The fully qualified domain name for the server that hosts the ActiveSync service
Account Configuration: Allow any server certificate	Yes or No. Select *Yes* to allow.
Account Configuration: Certificate	Enable and add a certificate or a SCEP request. To add a certificate, click *Add Certificate*, select a certificate, and enter a password for the certificate. To add a SCEP request, click *Add SCEP request*, select a CA profile from the drop-down list and enter the common name and password for the CA.
Account Configuration: Auto-start	Yes or No. Select *Yes* to launch the TouchDown client configuration wizard automatically.

2.18.4.4.4 EAS Overrides Page

For NitroDesk TouchDown client users, you can set configuration properties to override Exchange ActiveSync settings. These settings override the Exchange settings only if they are more restrictive than the Exchange settings.

Setting	Description
Reset policies	Yes or No. Select *Yes* to clear all existing policies before assigning override policies.
TouchDown password	Yes or No. Select *Yes* to require a password. Selecting *Yes* enables the settings in the TouchDown Password area.
TouchDown Password: Alphanumeric password required	Yes or No. Select *Yes* to require an alphanumeric password.
TouchDown Password: Minimum password length	The minimum length for the password. Range is 1 – 16 characters.
TouchDown Password: Minimum number of complex characters	Minimum number of symbols in the password. Range is 1 – 4. This option is only available if *Alphanumeric password required* is selected.
TouchDown Password: Password history count	The number of passwords stored on the history list. Range is 0 – 65535. Default is 0.
TouchDown Password: Password expiration days	Number of days a password remains valid. Range is 0 – 65535. 0 means there is no restriction (the password does not expire). Default is 0.
TouchDown Password: Maximum password failed attempts	The number of times a user can enter a wrong password
Maximum inactivity time TouchDown lock (seconds)	The time in seconds before an inactive device locks. Range is 0 – 65535.
Require TouchDown encryption	Yes or No. Select *Yes* to encrypt TouchDown. Select *No* to leave TouchDown unencrypted.
Require storage card encryption	Yes or No. Select *Yes* to encrypt the storage card. Select *No* to leave the storage card unencrypted.
Allow attachments on storage card	Yes or No. Select *Yes* to allow attachments on the storage card.
Attachments	Enable or Disable. Select *Enable* to allow users to send attachments in an e-mail.
Maximum attachment size (bytes)	Maximum attachment size in bytes. Range is 0 – 2147482624.
Maximum calendar age filter	Maximum number of days to synchronize past events. Options are: No Filter, 2 weeks, 1 month, 3 months, and 6 months.

Setting	Description
Maximum email age filter	Maximum number of days to synchronize past e-mail messages. Options are: No Filter, 1 day, 3 days, 1 week, 2 weeks, and 1 month.
Maximum email body size	Maximum size allowed for the e-mail message body. Options are: No Body, 4 KB, 5 KB, 7 KB, 10 KB, 20 KB, 50 KB, 100 KB, and Full Emails.
Allow HTML email	Yes or No. Select *Yes* to allow e-mail messages to be sent in HTML format.
Require manual synchronization when roaming	Yes or No. Select *Yes* to require users to synchronize their device manually when roaming.

2.18.4.4.5 Security Settings Page

For NitroDesk TouchDown client users, you can set configuration properties for additional security settings for using the TouchDown client.

Consider these items:

Setting	Description
Phone book copy fields	A comma-delimited list of data elements that are eligible for copy to phone book: • org • photo • note • title • location • dept • wphone • wphone2 • hphone • hphone2 • mphone • ofax • hfax • assistantphone • radiophone • carphone • pager • compphone • email1 • email2 • email3 • homeaddress • workaddress

Setting	Description
	• otheraddress
Set signature	If left blank, users can enter their own signature
Set suppressions	A comma-delimited list of codes for suppressing user-facing items after TouchDown has been configured. Examples of suppression codes and associated items: • 101 – Quick Configuration Button • 102 – Connection Mode • 103 – User ID, Domain, and Email Address • 104 – Language • 150 – Server Information • 151 – ISA Flags Settings • 200 – Push and Polling Settings • 201 – Email History • 203 – Signature **i Note** A complete list of suppression codes is available in the NitroDesk client users guide.

2.18.4.4.6 User Settings Page

For NitroDesk TouchDown client users, sets properties for general user settings.

Setting	Description
Email body style	Specify fonts, sizes, colors, and styles used to create new HTML messages. The email body style syntax is: `font-family:<FONT_NAME>;font-size:<FONT_SIZE>`

2.18.4.4.7 Email Options Page

For NitroDesk TouchDown client users, sets properties for additional email options.

2.18.4.4.8 Calendar Options Page

For NitroDesk TouchDown client users, sets properties for calendar options.

2.18.4.5 LG Pages

Configuration policy LG features let you use Afaria Advanced Enterprise Security (AES) on LG Android devices that support enterprise device management, and have installed the LG-signed Afaria application. The application is available from either the LG Apps store or Google Play.

Use configuration policy LG property pages for:

- Security management
- Application management
- Configuration management
- Microsoft Exchange client configuration

LG product documentation for devices is available from the LG support site.

Application Policy [page 74]
For LG Android devices, sets properties for accessing Google Play (renamed from Android Market), managing consumer and enterprise applications, and managing application data.

Bluetooth Policy [page 76]
The Bluetooth setting under *Configuration Policy > Android* disables Bluetooth, but allows the user to enable it again. This setting disables Bluetooth and disables the user from changing the setting. Audio only disables Bluetooth radio for connecting to computers and other devices.

Email Account Policy Page [page 76]
For LG Android devices, sets properties for connecting to and from remote email server.

Exchange Account Policy Page [page 77]
For an LG Android user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client. Once the client is defined on a device, allows you remove it from the device.

Location Policy Page [page 78]
For LG Samsung devices, enables GPS location provider

Password Policy Page [page 79]
For LG Android devices, sets properties for additional security for the password. This password is enabled on the policy editor's Security page.

Restriction Policy Page [page 79]
For Android LG devices, defines restrictions for user access to certain features.

Roaming Policy Page [page 80]

For LG Android devices, sets properties for data synchronization while roaming. The properties set values on your device's *Settings* > *Wireless and Network* > *Mobile Networks*.

Security Policy Page [page 80]

For Android LG devices, sets properties for device encryption and credential storage.

2.18.4.5.1 Application Policy

For LG Android devices, sets properties for accessing Google Play (renamed from Android Market), managing consumer and enterprise applications, and managing application data.

User interaction is required to install applications from a consumer market, such as Google Play. User interaction is not required to install applications from your Afaria Package Server.

> ⚠ Caution
>
> Disabling Afaria causes subsequent sessions to fail. Removing the disabled application may fail, and reinstalling the application may not restore normal operations.

The Application Policy page includes these properties:

LG Application Installation Mode Settings

Setting	Description
Enable application installation mode	Check this box to define white list or blacklist applications
Application installation mode	Define which applications can be installed on a device. You can deploy applications to devices by creating a white list (allowed applications) and a blacklist (disallowed applications). Options are: • Block all except white list below – The blacklist is ignored and no applications, other than the ones you define in this list, can be installed by a user. • Allow all except black list below – The white list is ignored and all applications available on the market, except the ones in this list, can be installed by a user. **i Note** Wildcard characters are not supported for package names in black/white lists.

Black and White List Management Settings

Add rules to add or delete applications.

Setting	Description
Include/Exclude	Select "Include" to deploy the policy during the next session. If you select "Exclude", the policy remains on the list but is not deployed to the device.
Policy	Select to install or remove an application
Package name	Use a complete package name, as defined by the developing entity, such as com.apps.app1

Enable/Disable Policy Settings

Define a policy to enable or disable an application.

Setting	Description
Include/Exclude	Select "Include" to deploy the policy during the next session. If you select "Exclude", the policy remains on the list but is not deployed to the device.
Package name	Use a complete package name, as defined by the developing entity, such as com.apps.app1
App Enable/Disable	Select to enable or disable the application. Disabled applications remain installed, but do not function.
Uninstallation Enable/Disable	Select to enable or disable the user's ability to remove the named application

Install/Remove/Wipe Policy

Define a policy to install, remove, or wipe application data or cache.

Setting	Description
Include/Exclude	Select "Include" to deploy the policy during the next session. If you select "Exclude", the policy remains on the list but is not deployed to the device.
Policy	Select to install, remove, or wipe app data or cache
Package Path	Required for installing and updating an application. Define the path and file name, such as `/data/new/app1.apk or mnt/sdcard/app1.apk`, to the compiled application file. **i Note** For devices running Jelly Bean ROM, the path is /storage/sdcard0.

Setting	Description
Package Name	Required for removing an application. Package name, as defined by the developing entity, such as com.apps.app1.

2.18.4.5.2 Bluetooth Policy

The Bluetooth setting under *Configuration Policy > Android* disables Bluetooth, but allows the user to enable it again. This setting disables Bluetooth and disables the user from changing the setting. Audio only disables Bluetooth radio for connecting to computers and other devices.

2.18.4.5.3 Email Account Policy Page

For LG Android devices, sets properties for connecting to and from remote email server.

To add a configuration item to the list in the policy editor, click *Add*. To remove an email account from the Android Client, include the item you wish to delete and delete the Email Address. The item with that Identifier will then be deleted when the client runs this policy.

Setting	Description
Include/Exclude	Select "Include" to deploy the policy during the next session. If you select "Exclude", the policy remains on the list but is not deployed to the device.
Identifier	Uniquely identifies the e-mail account in Afaria and on the device. You can configure the account for a user on multiple devices. You can configure multiple accounts for a user on a device.
Email address	The email address of the account
Incoming protocol	Post Office Protocol (POP) or Internet message access protocol (IMAP)
Incoming login	Login name associated with the user e-mail account
Incoming password	Password associated with the user e-mail account
Incoming address	The e-mail protocol incoming address, for example, imap.gmail.com
Incoming port	Server associated with the user e-mail account
Enable SSL	Indicates whether to use secure protocol for e-mail connections
Outgoing login	Login name associated with the outgoing e-mail server account
Outgoing password enabled	Require an outgoing password when the user sends an e-mail

Setting	Description
Outgoing password	Password associated with the outgoing e-mail account
Outgoing address	The outgoing server address, for example, smtp.gmail.com
Outgoing port	Server associated with the outgoing e-mail server
Enable Outgoing SSL	Set this policy to require SSL on outgoing e-mail server connections
Sync Interval	Interval or method for ongoing synchronization from the device to the e-mail server
Attachments	Allow or disallow attachments in e-mails sent to and from this device
Max Attachment Size	Define a maximum size for sent and received attachments
Max mails to show	set the default number of e-mails to show in the e-mail account inbox

2.18.4.5.4 Exchange Account Policy Page

For an LG Android user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client. Once the client is defined on a device, allows you remove it from the device.

> ⚠ Caution
>
> Do not remove an item from the list in the policy editor until after you remove the configuration from a device. You cannot remove the configuration from a device if it is not on the editor's list with the same identifier originally delivered to the device.

Setting	Description
Include/Exclude	Select "Include" to deploy the policy during the next session. If you select "Exclude", the policy remains on the list but is not deployed to the device.
Identifier	Uniquely identifies the Exchange account in Afaria and on the device. You can configure the account for a user on multiple devices. You can configure multiple accounts for a user on a device.
Email address	The user's Microsoft Exchange e-mail address
Domain	The user's e-mail domain for the Microsoft Exchange account
User	The user's Microsoft Exchange user name
Password	The user's Microsoft Exchange password

Setting	Description
Account name	The name of the account on the device. Name appears on the device's *Settings* > *Accounts and Sync* page as a managed account.
Accept all certificates	Device accepts certificates without user intervention
Calendar sync	Interval or method for ongoing synchronization of Microsoft Outlook calendar
Active Sync Host	IP address of the ActiveSync Host
Contacts sync	Interval or method for ongoing synchronization of email contacts
Email sync	Allows the device to synch with the Microsoft Exchange server upon connection
Max Email Age	Only keeps emails to a specific date on a device
Tasks sync	Syncs all tasks from the calendar on the Exchange server to the device
Attachments	Allow or disallow attachments in emails sent to and from this device
Max Attachment Size	Define a maximum size for sent and received attachments
Max email body truncation size	Allows emails of a specific length only
Use SSL	Indicates whether to use secure protocol for Microsoft Exchange sessions
Set client authentication certificate	Path on device to the certificate, such as /mnt/sdcard/certname.p12
Certificate password	Password for client authentication certificate
Amount to synchronize	Time range or amount of history to synchronize for each synchronization request
Sync interval	Interval or method for ongoing synchronization
Vibrate on email notification	Notification mode
Signature	Signature for user-initiated messages. If blank, user can enter a signature.

2.18.4.5.5 Location Policy Page

For LG Samsung devices, enables GPS location provider

Setting	Description
Enable GPS location provider	Click this box to enable GPS location services
Enable network location provider	Click this box to enable network location services

2.18.4.5.6 Password Policy Page

For LG Android devices, sets properties for additional security for the password. This password is enabled on the policy editor's Security page.

Setting	Description
Allow simple password	Enables/disables passwords with regular patterns, for example: “abcd”, “aaaa”, “1234”, or “2222”.

2.18.4.5.7 Restriction Policy Page

For Android LG devices, defines restrictions for user access to certain features.

Setting	Description
Enable SD Card	Enable the memory card on the device
Allow camera	Allow the Camera application
Allow USB	Enabled a USB connection on the device
Allow USB Tethering	Allows for USB tethering from device to device or whenever the device is connected to a computer or laptop via a USB cable
Allow sending SMS	Allow SMS text messaging
Allow WiFi	Allow Wi-Fi. The user cannot change this value. This setting overrides the Wi-Fi setting on the policy editor Wireless LAN page.
Allow browser	Allow Internet browser to be installed on the device
Allow mobile network	Allows the device to access a mobile network
Allow screen capture	Allow user to take a screen shot of an image on the device
Allow factory reset	Allows user to reset changes to the device default settings
Allow admin-device deactivation	Allow administrators to deactivate the device from the Afaria Administration console
Allow POP/IMAP e-mail	Allow device to send/receive email through a defined POP/IMAP server.

2.18.4.5.8 Roaming Policy Page

For LG Android devices, sets properties for data synchronization while roaming. The properties set values on your device's *Settings* > *Wireless and Network* > *Mobile Networks*.

Setting	Description
Allow roaming data	Allows the user data roaming privileges when they change networks
Allow automatic sync while roaming	Automatically synchronizes email, calendars and contacts when the device roams onto a different network

2.18.4.5.9 Security Policy Page

For Android LG devices, sets properties for device encryption and credential storage.

The following are data wipe options for LG devices:

- Factory reset (erase all PIM data)
- SD Card + Factory Reset
- UICC delete + SD Card + Factory Reset (Verizon only)

2.18.4.6 Samsung KNOX Standard Pages

Samsung KNOX Standard policies allow you to use Samsung for Enterprise on Samsung devices that support enterprise device management, and have the Samsung-signed Afaria application installed. The application is available from either the Samsung Apps store or Google Play.

Use Samsung KNOX Standard policy pages for:

- APN configuration
- Application management
- Bluetooth configuration
- Email account configuration
- Microsoft Exchange client configuration
- Firewall configuration
- Location configuration
- Password management
- Enterprise device management
- Restriction configuration
- Roaming configuration
- Security management
- WiFi configuration

> **i Note**
>
> For devices with OS version greater than 4.2 (API level > 17), after you upgrade to the September version of the SAP HANA Cloud Platform, mobile service for app and device management client, you are prompted to accept the Samsung Enterprise License Model (ELM) to access Samsung KNOX Standard pages. This is also applicable for re-enrollment of the SAP HANA Cloud Platform, mobile service for app and device management client.

Samsung product documentation for devices is available from the Samsung support site.

Important Information for Upgrading Samsung Clients

Only the policies assigned to devices during upgrade are reapplied when the device connects from an upgraded Samsung client. Ensure that all policies previously applied on devices are correctly assigned to the device during the upgrade.

APN Policy Page [page 82]
: Configure one or more Access Point Name (APN) profiles for a Samsung KNOX Standard device. An APN identifies a gateway between the user's mobile network and a data network and is required for users to access the Internet or send and receive MMS messages. You can create default or MMS APN profiles.

Application Policy Page [page 83]
: For Samsung KNOX Standard devices, define properties for accessing Google Play, managing consumer and enterprise applications, and managing application data.

Bluetooth Policy Page [page 86]
: For Samsung KNOX Standard devices, sets properties for select Bluetooth capabilities.

Email Account Policy Page [page 86]
: For Samsung KNOX Standard devices, sets properties for connecting to the remote email server.

Exchange Account Policy Page [page 87]
: For a Samsung KNOX Standard user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client. Once the client is defined on a device, lets you remove it from the device.

Firewall Policy Page [page 89]
: For Samsung KNOX Standard devices, sets properties for Firewall options.

Location Policy Page [page 90]
: For Samsung KNOX Standard devices, enables GPS location provider.

Password Policy Page [page 90]
: For Samsung KNOX Standard devices, sets properties for additional security for the password you enable on the policy editor Security page, and lets you execute a remote restart on the device.

Device Manager Policy Page [page 90]
: The Device Manager Policy controls whether users of Samsung KNOX Standard devices can deactivate the SAP Afaria Samsung MMEP application or Afaria application as a device administrator. The SAP Afaria Samsung MMEP application is an SAP Afaria client extension for managing Samsung devices.

Restriction Policy Page [page 91]
: For Samsung KNOX Standard devices, defines restrictions for user access to certain features.

Roaming Policy Page [page 92]

For Samsung KNOX Standard devices, sets properties for data synchronization while roaming. The properties set values on your device's *Settings* > *Wireless and Network* > *Mobile Networks*.

Security Policy Page [page 92]
For Samsung KNOX Standard devices, sets properties for device encryption and credential storage.

WiFi Policy Page [page 93]
Configure Wi-Fi connections on Samsung KNOX Standard devices to allow users to connect wirelessly to your network. You can also choose to block users from connecting to a configured network connection.

2.18.4.6.1 APN Policy Page

Configure one or more Access Point Name (APN) profiles for a Samsung KNOX Standard device. An APN identifies a gateway between the user's mobile network and a data network and is required for users to access the Internet or send and receive MMS messages. You can create default or MMS APN profiles.

You can configure an APN profile to allow corporate devices direct access to your internal network from a mobile network. By defining a profile for your corporate environment, you can provide better control over who has access to your network. You can also configure additional profiles so that users who are traveling for business can connect through an APN server in their region.

To create an APN profile, click *Add* and configure settings as required.

Setting	Description
Include/Exclude	Select *Include* to add this APN to a device when the configuration policy is applied; Select *Exclude* if you do not want to add this APN to the device or you want to remove it from a device after it has been applied.
Identifier	A system-generated ID for the APN. This field is not editable.
Name	A user-friendly name for the APN such as "North-East Region". This name is used to identify the APN in the device's APN list. Required.
APN	The hostname of the APN server. Required.
Proxy Address	The IP address of a proxy server if one is used. Optional.
Port Number	The port number for the proxy server if one is used. Optional.
Username	The username of an account on the APN server if authentication is required. Optional.
Password	The password of an account on the APN server if authentication is required. Optional.
Server Address	The IP address of the APN server. Usually, only the APN is required. Optional.
MMS Server Address	The IP address or hostname of the MMS server. Define to provide MMS service through this profile. Optional.

Setting	Description
MMS Proxy Address	The IP address or hostname of the MMS proxy server if one is used. Optional.
MMS Port Number	The port number of the MMS proxy server if one is used. Optional.
Mobile Country Code	The Mobile Country Code (MCC) for the APN. The MCC is a 3-digit code for the country where the APN is located. For example, MCCs for the U.S. are 310, 311, and 316. The MCC and Mobile Network Code (MNC) uniquely identify a mobile carrier's network. Required.
Mobile Network Code	The Mobile Network Code (MNC) for the APN. The MNC is a 2- or 3-digit code for the network where the APN is located. The MCC and Mobile Network Code (MNC) uniquely identify a mobile carrier's network. Required.
Authentication Type	The protocol used to authenticate the connection to the network. Options are: • None • PAP – Password Authentication Protocol • CHAP – Challenge-Handshake Authentication Protocol • PAP or CHAP
Access Point Type	The type of the connection through the APN, either "Default" or "MMS". A default APN profile is used for all data traffic; MMS is used for MMS service.

2.18.4.6.2 Application Policy Page

For Samsung KNOX Standard devices, define properties for accessing Google Play, managing consumer and enterprise applications, and managing application data.

User interaction is required to install applications from a consumer market, such as Google Play. User interaction is not required to install applications from your SAP Afaria Package Server.

> ⚠ Caution
>
> Do not disable the SAP Afaria client because subsequent sessions fail. Removing the disabled application might fail and reinstalling the application might not restore normal operations.

General Settings

Setting	Description
Enable Android Market	Disable (No) or enable (Yes) the Android Market application
Enable Application Installation Mode	Check this box to define whitelist or blacklist application

Setting	Description
Application Installation Mode	Define which applications are deployed to a device. You can deploy applications to devices by creating a white list (allowed applications) and a blacklist (disallowed applications): • Block all except white list below – No applications, other than the ones you define in this list, can be installed by a user. • Allow all except black list below – All applications available on the market, except the ones in this list, can be installed by a user.

Application Black and White List Management Settings

Use the blacklist to define applications you do not want users to download from Google Play. Use the white list to define applications that users can download.

Setting	Description
Include/Exclude	Select "Include" to apply the rule when the policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Policy	Select whether the item is for installation or deletion.
Package name	Use a complete package name, as defined by the developing entity, such as com.apps.app1. **i Note** Wildcards are not supported in package names.

Enable/Disable Policy Settings

Use this policy to enable or disable an application.

Setting	Description
Include/Exclude	Select "Include" to apply the rule when the policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Package name	Use a complete package name, as defined by the developing entity, such as com.apps.app1. **i Note** Wildcards are not supported in package names.

Setting	Description
App Enable/Disable	Select to enable or disable the application. Disabled applications remain installed, but do not function.
Installation Enable/Disable	Select to enable or disable the user's ability to install the named application. Attempting to install an application when the installation is set to “Disable” may result in user-facing error messages that do not describe the condition. Set expectations with your users.
Uninstallation Enable/Disable	Select to enable or disable the user's ability to remove the named application
Wipe App Data	Delete application data associated with the named application
Delete Managed App Info	After the next session that runs an inventory channel, delete the inventory data for the managed application from *Afaria Administrator* > *Data Views* > *Inventory*.

Application Install/Remove/Update Policy Settings

Use this policy to install, remove, or update an application.

Setting	Description
Include/Exclude	Select "Include" to apply the rule when the policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Policy	Select to install, remove, or update an application
Package Path	Required for installing and updating an application. Define the path and file name, such as /data/new/app1.apk or mnt/sdcard/app1.apk, to the compiled application file. The APK file must be stored on the device in a location that is read- and write-accessible to the Afaria device. Locations may vary by device. **i Note** For devices running Jelly Bean ROM, the path is /storage/sdcard0.
Package name	Required for removing an application. Use a complete package name, as defined by the developing entity, such as com.apps.app1. **i Note** Wildcards are not supported in package names.

2.18.4.6.3 Bluetooth Policy Page

For Samsung KNOX Standard devices, sets properties for select Bluetooth capabilities.

Setting	Description
Enable discoverable	Enable to allow the device to discover nearby Bluetooth devices
Enable desktop/laptop connectivity	Enable desktop/laptop connectivity

2.18.4.6.4 Email Account Policy Page

For Samsung KNOX Standard devices, sets properties for connecting to the remote email server.

Select the checkbox to deploy the policy during the next session. If you unselect the check box, the policy remains on the list but is not deployed to the device.

Consider the following:

Setting	Description
Identifier	Uniquely identifies the email account in Afaria and on the device. You can configure the account for a user on multiple devices. You can configure multiple accounts for a user on a device.
Incoming address	The email protocol incoming address, for example, `imap.gmail.com`
Incoming protocol	Post Office Protocol (POP) or Internet message access protocol (IMAP)
Incoming login	Login name associated with the user email account
Incoming port	Server associated with the user email account. 993.
Incoming password	Password associated with the user email account
Incoming path prefix	Configure the incoming server path prefix of the email
Incoming SSL	Indicates whether to use secure protocol for email connections
Outgoing port	SMTP server used only to send emails to the device
Outgoing protocol	SMTP
Outgoing path prefix	Configure the outgoing server path prefix of the email
Outgoing password	Password associated with outgoing email server
Outgoing login	Login name associated with the outgoing email server account
Outgoing port	Server associated with the outgoing email server. 465.

Setting	Description
Outgoing address	The outgoing server address, for example, `smtp.gmail.com`
Outgoing password enabled	Require an outgoing password when the user sends an email
Account name	The name of the account
Sync Interval	Interval or method for ongoing synchronization from the device to the email server
Set as default account	Sets the defined email account as the default for the device
Sender name	Name of the user.
Enable Incoming SSL	Indicates whether to use secure protocol for email connections
Enable Outgoing SSL	Set this policy to re require SSL on outgoing email server connections
Signature	Signature for user-initiated messages. If blank, user can enter a signature.
Incoming accepts all certs	Accept all certificates sent by Incoming server
Outgoing accepts all certs	Accept all certificates sent by Outgoing server

2.18.4.6.5 Exchange Account Policy Page

For a Samsung KNOX Standard user that is already defined in the Microsoft Exchange environment, sets properties for the native Microsoft Exchange ActiveSync (EAS) client. Once the client is defined on a device, lets you remove it from the device.

If the client has multiple e-mail accounts, and the accounts use shared preference settings, then all accounts use one preferred signature setting. In SAP Afaria, the last account on the policy editor list is applied last and becomes the preferred setting for all accounts.

To add a configuration item to the list in the policy editor, click *Add account*.

To remove an ActiveSync item from the client, include the item you want to delete and delete the email address. The item with that Identifier will then be deleted when the client runs this policy. To remove a defined item from the list, select it and click *Remove current account*.

> ⚠ Caution
>
> Do not remove an item from the list in the policy editor until after you remove the configuration from a device. You cannot remove the configuration from a device if it is not on the editor's list with the same identifier originally delivered to the device.

Setting	Description
Include/Exclude	Select "Include" to apply the configuration item when the policy is run. If you select "Exclude", the item remains on the list but is not deployed to the device.
Identifier	Uniquely identifies the Exchange account in SAP Afaria and on the device. You can configure the account for a user on multiple devices. You can configure multiple accounts for a user on a device.
Active Sync host	The fully-qualified domain name for the Microsoft Exchange server
Domain	The user's e-mail domain for the Exchange account
Email address	The user's Exchange e-mail address
User	The user's Exchange user name in the format configured on the Exchange server. **i Note** Verify the user format on your Exchange server before continuing. Some Exchange servers may require a fully-qualified email address in the user field in the format `<user>@<domain>`. The incorrect format may result in a failure to configure the email account on the device. When using substitution variables: • If the Exchange server requires only the unqualified user name, use only the Exchange user system variable (`%S.ExchangeUser%`) • If the Exchange server requires a fully-qualified user name, use both the Exchange user and Exchange domain system variables separated by the @ symbol (`%S.ExchangeUser%@%S.ExchangeDomain%`)
Password	The user's Exchange password
Account name	The name of the account on the device. The name appears on the device's *Settings* > *Accounts and Sync* page as a managed account.
Accept all certificates	Device accepts certificates without user intervention.
Use SSL	Indicates whether to use secure protocol for Exchange sessions
Set client authentication certificate	To add the client certificate, click *Add Certificate*, browse to select a certificate, and then specify a password for the certificate. To add a SCEP request, click *Add SCEP request*, select a CA profile from the drop-down list, and specify the common name and password for the CA.
Amount to synchronize	The time range or amount of history to synchronize for each synchronization request
Sync interval (Off-Peak)	The interval or method for ongoing synchronization during off-peak hours

Setting	Description
Vibrate on email notification	The notification mode
Signature	The signature for user-initiated messages. If blank, user can enter a signature.

2.18.4.6.6 Firewall Policy Page

For Samsung KNOX Standard devices, sets properties for Firewall options.

Setting	Description
Enable IP proxy rule	Enable the firewall policy
IP address	IP addresses in IPv4 format (including wildcards, example, 192.168.*.*)
Port	A port or a range of ports (0 – 65535)

Deny Rules

Deny rules let you specify the denied destination addresses for incoming and outgoing traffic for a specified application. For example, to define a deny rule that drops outgoing traffic from a KNOX container app to port 80 on IP 1.2.3.4, specify "1.2.3.4" for the host, "80" for the port, "remote" for the port location, and the package name of the app.

Setting	Description
Hostname	The domain name or IP address of the destination device. IP ranges such as "100.0.0.0-100.0.0.10" are allowed. Use an asterisk (*) as a wildcard to allow or deny all IP addresses. Required.
Port	The port on the destination device. Port ranges such as "8080-8085" are allowed. Use an asterisk (*) as a wildcard to allow or deny all ports. Required.
Port Location	Allows you to specify whether the port is located on the device or on a remote device. Options are "All", "Local", and "Remote".
Application Package	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle". For deny rules only.
Network Interface	Allows you to specify whether the rule applies to connections through a Wi-Fi or data network interface

2.18.4.6.7 Location Policy Page

For Samsung KNOX Standard devices, enables GPS location provider.

Setting	Description
Enable GPS location provider	Click this box to enable GPS location services

2.18.4.6.8 Password Policy Page

For Samsung KNOX Standard devices, sets properties for additional security for the password you enable on the policy editor Security page, and lets you execute a remote restart on the device.

Setting	Description
Maximum number of days until password expires	The maximum number of days for a password to remain valid. When set to 0, the property does not restrict the policy. If you previously deployed a policy using a non-zero value for this property, and now want to deploy a policy that ignores the property, set the value to 0.
Minimum number of complex characters in password	Enforce a minimum number of complex characters
Password history	The number of previous passwords stored on the system's history list. When set to 0, the property does not restrict the policy. If you previously deployed a policy using a non-zero value for this property, and now want to deploy a policy that ignores the property, set the value to 0.
Remote reset	Restarts the device ⚠ Caution It is recommended that you apply the remote reset property as the policy's only setting. The reset occurs as the first configuration action after the session ends, canceling any other actions in the session. Re-running the session repeats the action.

2.18.4.6.9 Device Manager Policy Page

The Device Manager Policy controls whether users of Samsung KNOX Standard devices can deactivate the SAP Afaria Samsung MMEP application or Afaria application as a device administrator. The SAP Afaria Samsung MMEP application is an SAP Afaria client extension for managing Samsung devices.

The behavior of these settings depends on the MDM version on the Samsung device. For devices with MDM version 4 or higher, this setting allows you to prevent a user from removing the Samsung MMEP application as a device administrator, enable the *Allow Afaria Device Admin Deactivation* checkbox, and select *No*. If you want

to prevent a user from removing the base SAP Afaria client application instead, use the Application Policy page under Samsung KNOX Standard to disable removal of this application.

> **i** Note
>
> - Samsung introduced support for this setting starting with Android 3.0. It is not supported on Samsung devices running earlier versions of the OS. Be aware that users of these older devices can remove the SAP Afaria Samsung MMEP application as a device administrator even when this setting is set to "No".
> - For devices running Android OS 4.2 and higher, the Samsung Enterprise License Model (ELM)

2.18.4.6.10 Restriction Policy Page

For Samsung KNOX Standard devices, defines restrictions for user access to certain features.

Setting	Description
Allow Unknown Source Install	Allows the installation of non-Google Play apps
Allow Settings Changes	Allows the user to change settings
Enable Background Data	Enables applications syncing, sending, and receiving data at any time
Enable Backup	Allows the user to save a copy of Contacts to a secure web site
Enable Bluetooth	Enables the Bluetooth radio. The user cannot change this value. This setting overrides the Bluetooth setting on the policy editor Bluetooth page
Enable Bluetooth Tethering	Enables Bluetooth tethering
Enable NFC	Enables Near Field Communication on the device
Enable Camera	Enables the camera application
Enable Clipboard	Enables the clipboard application
Enable Microphone	Enables the Voice Dialer application
Enable SD Card	Enables the SD card
Allow SD Card Write	Allows applications to write to the SD card
Enable USB Debugging	Enables USB debugging
Enable USB Media Player	Enables the USB Media Player
Enable Screen Capture	Enables the user to create screen captures
Enable USB Tethering	Enables USB tethering on the device

Setting	Description
Enable WiFi	Enables Wi-Fi. The user cannot change this value. This setting overrides the Wi-Fi setting on the policy editor's Wireless LAN page.
Enable WiFi Tethering	Enables WiFi tethering
Allow Multiple Users	Allows multiple users to use the device
Allow Factory Reset	Allows the user to reset the device to its factory settings
Allow OTA Upgrade	Allows the device to receive Over-the-air software upgrades
Allow Nonemergency Calls	Allows the user to place nonemergency calls

2.18.4.6.11 Roaming Policy Page

For Samsung KNOX Standard devices, sets properties for data synchronization while roaming. The properties set values on your device's *Settings* > *Wireless and Network* > *Mobile Networks*.

Setting	Description
Allow roaming data	Allows data use while roaming
Allow automatic sync while roaming	Automatically synchronizes email, calendars and contacts when the device roams onto a different network
Allow push while roaming	Allows push synchronization while roaming

2.18.4.6.12 Security Policy Page

For Samsung KNOX Standard devices, sets properties for device encryption and credential storage.

Setting	Description
Encrypt device	Select *Yes* to encrypt the device memory and internal SD card. **i Note** Once Encrypt device is applied at the device, for each subsequent connection, that includes the Encrypt device attribute, it is a known behavior of the Samsung APIs that the user may observe the message "The same policy applied." The user can disregard the message.
Encrypt SD card	Select *Yes* to encrypt the external SD card.

Setting	Description
	If Encrypt SD card is applied at the device, the following are known behaviors of the Samsung APIs: • "Unable to use SD card without data encryption," or similar. The user can dismiss the message by clicking *OK*. The device encrypts the data. • Executing a Samsung policy to encrypt the SD card presents the following prompt: "Data encryption policy-- Data encryption policy received from IT administrator. Smart phone will be rebooted to encrypt system storage and USB storage". Insert SD card into the device and re-apply the policy. • Executing a Samsung policy to decrypt the SD card does not initiate the decryption process and results in the following message: "Data decryption policy -- Data encryption policy received from IT administrator. Smart phone will be rebooted to decrypt system storage and USB storage", which should trigger another prompt to enter device's password (if the device is password-protected) and should reset the device before the decryption. The session completes with no prompts and the device remains encrypted. Manually reboot the device to start the decryption process.
Install certificate	To install a certificate, click *Add Certificate*, browse to select a certificate, and specify a password for the certificate. To add a SCEP request, click *Add SCEP request* to enhance security, select a CA profile from the drop-down list, and specify the common name and password for the CA.
Clear installed certificates	Remove installed certificates

2.18.4.6.13 WiFi Policy Page

Configure Wi-Fi connections on Samsung KNOX Standard devices to allow users to connect wirelessly to your network. You can also choose to block users from connecting to a configured network connection.

This policy also allows you to configure a device's wireless adapter. For example, you can allow or block users from configuring their own profiles or from changing the settings of network connections configured through this policy.

> **i** Note
>
> To remove a network configuration from a device, clear the Network SSID from the connection profile and set it to "Include". The connection with this ID is deleted from the device when the policy is applied.

Wireless Adapter Settings

Setting	Description
Allow user policy changes	Allows or blocks users from making changes to network connections configured through a configuration policy. If you select "No", users are blocked from removing these connections or from changing settings.
Allow user profiles	Allows or blocks users from adding Wi-Fi connection profiles on their device. Selecting *No* prevents the user or another application from adding a profile to the device. When this is set to *No*, only an MDM client such as the Afaria application on the device can add a profile. On a device managed by more than one administrator, the user is blocked from adding profiles if one of the administrators has disabled profile additions.
Hide password	Masks the password in the Wi-Fi connection settings on the device
Minimum required security	Sets the minimum security required to connect to a network. Options in the list are ordered from lowest to highest security level. Network connections with lower security levels are displayed in the list of Wi-Fi connections on the device but the user is blocked from connecting.
Prompt for credentials	Sets whether the device prompts the user to re-enter credentials if WPA/WPA2-PSK authentication fails. If you select "No", the user is not prompted to re-enter credentials if authentication fails.
TLS certificate security level	Sets the TLS certificate security level for connections using EAP-TTLS or EAP-TLS. Options are: • Low – The certificate key store is left unlocked after the private key is read and is only locked again on reboot • High – The certificate key store is locked after each use of the key store

Network Connection Settings

Setting	Description
Include/Exclude	Allows you to include or exclude the connection profile from the configuration policy.
Identifier	A system-generated ID for the network connection. This field is not editable.
Network SSID	Network Service Set Identifier (SSID). This is a name for the Wi-Fi connection as configured on the wireless router. This name is used to identify the connection in the device's Wi-Fi list. Required.
Block network	Allows you to block users from connecting to this connection

Setting	Description
IP settings	The IP addressing method used by the wireless router, either static IP or Dynamic Host Control Protocol (DHCP). If using static IP, configure the default gateway, default IP, and subnet mask.
Default gateway	The IP address of the wireless router. Required if static IP is used.
Default IP	The IP address of the device. Required if static IP is used.
Default primary DNS	The IP address of the primary Domain Name System server
Default secondary DNS	The IP address of the secondary Domain Name System server
Default subnet mask	The subnet mask for the wireless router. Required if static IP is used.
Network link security	The security protocol used to authenticate network link connections. Depending on the security protocol used, you may need one of the following: • A network WEP key 1 for WEP • A network pre-shared key for WPA/WWPA2-PSK • A CA certificate and either a client certificate or SCEP request for all version of EAP
CA Certificate	The certificate used by the router to authenticate the connection. Available if EAP is used. To add a CA certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. **i Note** The use of certificates is supported only on Samsung devices running Android 4.x and above. A device password must be enabled.
Client certificate	The certificate used by the device to authenticate the connection. Available if EAP is used. To add a client certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. To add a SCEP request, click *Add SCEP request*, select a CA profile from the drop-down list, and specify the common name and password for the CA. **i Note** The use of certificates is supported only on Samsung devices running Android 4.x and above. A device password must be enabled.
Network identity value	The network identity value. Available if EAP is used.

Setting	Description
Network password	The network password for authenticating the network connection. Available if EAP is used.
Network pre-shared key	A pre-shared key. Required when WAP/WAP2-PSK is used.
Network WEP key 1	A WEP key 1. Required when WEP is used.

2.18.4.7 Samsung KNOX Pages

Use the policy pages in the Samsung KNOX page group to configure policies on KNOX-capable Samsung devices.

Samsung KNOX is a hardware and software security solution for Samsung devices. The solution includes a secure container on the device for enterprise data. This container allows users to separate personal and business content on a device. It also includes security features such as boot tampering protection with Samsung Attestation.

When you use a KNOX policy to configure a KNOX-capable device, the KNOX container is first installed and then configured on the device.

> **i Note**
>
> You must obtain a Samsung Enterprise license from a KNOX reseller and enter the license key into Afaria before you can install the KNOX container on a device. For more information, see Entering a Samsung Enterprise License Key.

Entering a Samsung Enterprise License Key [page 97]
: Provide a Samsung Enterprise license key to install and configure KNOX on Samsung devices.

Application Policy Page [page 98]
: The Application Policy page allows you to define application data and cache clearing rules for applications installed in the KNOX container. You can also configure an application policy to uninstall or disable KNOX container applications as well as add or delete application shortcuts from the KNOX home screen. Uninstalling an application removes it from the container; disabling an application leaves it installed but prevents users from launching it.

Browser Policy Page [page 99]
: Configure settings for the browser installed in the KNOX container. You can disable cookies, JavaScript, and pop-ups on the browser. You can also specify the address of the web proxy server you want the browser to use.

Certificate Policy Page [page 100]
: Configure settings for CA certificates used to authenticate connections between the KNOX container and your network. You can specify which certificates are trusted and which are untrusted. Untrusted certificates are removed from the system. Untrusted items take precedence over trusted items. When a certificate is added as untrusted, it will be removed from the system even if it is part of a trusted certificate chain.

Email Account Policy Page [page 101]

Configure an Exchange email account in the KNOX container.

Firewall Policy Page [page 102]
: The firewall policy allows you to create firewall rules that control network traffic to and from the KNOX container on a Samsung device. You can create Allow, Deny, Reroute, and Redirect Exception rules. The KNOX firewall inspects the destination host and port on incoming and outgoing network packets and allows, redirects, or drops them based on the rules you configure here. You can also create rules to block the browser in the KNOX container from accessing a URL.

Password Policy Page [page 105]
: Configure password settings for the KNOX container. For example, you can set the timeout period, the password type, and the expiration period. You can also define character strings that are not allowed in the KNOX password.

Premium VPN Policy Page [page 106]
: The VPN policy allows you to define how a Samsung KNOX device connects to your enterprise's virtual private network (VPN). To create a VPN policy, create one or more VPN profiles and then either add them to a list of VPN profiles available from KNOX or associate them with an application on the device. VPN profiles define the VPN settings required to establish a connection to the VPN server including the VPN server hostname or IP address, the authentication method required, and Internet Key Exchange (IKE) configuration information.

Restriction Policy Page [page 109]
: Configure restrictions on the KNOX container. For example, you can configure the policy to disable the camera when inside the KNOX camera.

Security Policy Page [page 109]
: Configure the KNOX attestation security check for KNOX-capable devices.

Single Sign-On Policy Page [page 110]
: Configure single sign-on (SSO) on the KNOX container. Single sign-on allows users to sign in to SSO-enabled applications in the KNOX container with one set of credentials.

2.18.4.7.1 Entering a Samsung Enterprise License Key

Provide a Samsung Enterprise license key to install and configure KNOX on Samsung devices.

Context

You must provide a license key in order to install and configure the KNOX container on a device. When you apply a KNOX configuration policy to a device, the device connects with the Samsung Licensing server and uses the key to enable KNOX on the device. A license key can be configured for multiple tenants or per-tenant.

> **i** Note
>
> Obtain a license key from an authorized KNOX reseller.

Procedure

1. On the Server page, on the left toolbar, click *Configuration*.
2. Select *Component* > *Samsung Enterprise*.
3. Enter the license key in *Samsung Enterprise License Key* field.
4. (Optional) Type a note for the license key in the *Note* field.

2.18.4.7.2 Application Policy Page

The Application Policy page allows you to define application data and cache clearing rules for applications installed in the KNOX container. You can also configure an application policy to uninstall or disable KNOX container applications as well as add or delete application shortcuts from the KNOX home screen. Uninstalling an application removes it from the container; disabling an application leaves it installed but prevents users from launching it.

Cache and Data Clearing Rules

When you create a list of rules for app data and cache clearing, you can specify whether the list is a "white" list or a "black" list. A white list means users can only clear cache or data if the application is on the list. They are prevented from clearing anything on all other KNOX container applications. A black list means users are only restricted by the rules in the list. They are allowed to clear cache and data all other KNOX container applications.

Setting	Description
Behavior	Allows you to allow or block application clearing on the listed applications: • Allow only those listed – Allows users to clear cache and data only on applications on the list. Use this option to create a white list. • Block only those listed – Blocks users from clearing cache and data only on applications on the list. Use this option to create a blacklist.
Include/Exclude	Select "Include" to apply the rule when the policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Storage Type	Choose the type of information users are allowed to clear or restricted from clearing on the application. Options are: • Data and Cache – For white lists, users are allowed to clear an application's cache and data; For black lists, users are restricted from clearing an application's cache and data. • Cache Only – For white lists only. Users are only allowed to clear the application's cache. Clearing application data is restricted. • Data Only – For black lists only. Users are only restricted from clearing the application's data. Clearing the application's cache is permitted.

Setting	Description
Package Name	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle".

Uninstalling or Disabling Applications

To uninstall or disable an application installed in the KNOX container, click *Add* from the appropriate toolbar and set the following:

Setting	Description
Include/Exclude –	Select "Include" to uninstall or disable the application when the application policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Package Name	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle".

Adding or Deleting Application Shortcuts

Setting	Description
Include/Exclude	Select "Include" to include this rule in the application policy. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Action	Choose whether you want to add or delete a shortcut for the application
Package Name	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle".

2.18.4.7.3 Browser Policy Page

Configure settings for the browser installed in the KNOX container. You can disable cookies, JavaScript, and pop-ups on the browser. You can also specify the address of the web proxy server you want the browser to use.

Most of the settings include a User-controlled option. If you select *User-controlled*, the user is allowed to set these settings on the device.

Setting	Description
Enable KNOX Browser Policy	Allows you to set browser settings for the configuration policy. Enable to make the settings on this page available.

Setting	Description
Cookies	Allows you to prevent web pages from installing cookies on the device
Forms	Allows you to prevent the browser from auto-filling forms
JavaScript	Allows you to disable JavaScript on the browser
Pop-ups	Allows you to block Pop-ups on the browser
HTTP Proxy	The address of the proxy you want the browser to use

2.18.4.7.4 Certificate Policy Page

Configure settings for CA certificates used to authenticate connections between the KNOX container and your network. You can specify which certificates are trusted and which are untrusted. Untrusted certificates are removed from the system. Untrusted items take precedence over trusted items. When a certificate is added as untrusted, it will be removed from the system even if it is part of a trusted certificate chain.

You can also configure the system to check if a certificate used to authenticate a connection for a specific application has been revoked.

Setting	Description
Certificate Install-time Validation	Allows you to validate certificates during installation
Certificate Installation Failure Alert	Allows you to generate an alert if installation of a certificate fails
Application Signature Information	Allows you to show or hide application signature information
Trusted/Untrusted CA Certificate	Allows you to specify a certificate as trusted or untrusted in the Trusted or Untrusted CA Certificates list. To add a CA certificate, click *Add Certificate*, browse to and select the certificate file, and then click *Yes, Continue* to add the file to the list.
Include/Exclude	Select "Include" to apply the rule when the policy is run. If you select "Exclude", the rule remains on the list but is not deployed to the device.
Package Name	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle".
Type	Allows you to set the revocation method. Options are: • None – Disables revocation checking • CRL Only – Enables Certificate Revocation List (CRL) checking • OCSP and CRL – Enables Online Certificate Status Protocol (OCSP) checking. If OCSP checking fails, the application uses CRL checking instead.

2.18.4.7.5 Email Account Policy Page

Configure an Exchange email account in the KNOX container.

From the Email Account Policy page, select *Enable KNOX Email Account Policy* to configure an email account.

Setting	Description
User Created Accounts	Select *Allow* to allow users to add email accounts to the KNOX container. To prevent users from adding email accounts, disable this setting.
Include/Exclude	Select *Include* to include this account in the email account policy; Select *Exclude* if you do not want to add this account to the policy or you want to remove the account after the policy has been applied.
Exchange Server	IP address of the Exchange server
Domain	The domain for the user's email account
Email Address	The user's email address
User	The user's email user name
Password	The user's email password
Account Name	The name of the account on the device. The name appears on the device's Settings > Accounts and Sync page as a managed account.
Accept All Certificates	Allows you to configure the device to accept certificates without user intervention
Use SSL	Allows you to configure the email account to use Secure Socket Layer (SSL) security for sessions with the email server
Set client authentication certificate	Allows you to select a certificate for client authentication. You can also choose to send a certificate request to the Certificate Authority (CA) instead. To add a client certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. To add a request to the CA, click *Add Request*, select a CA profile from the drop-down list, and specify the common name, Subject Alt Name type and value, and password for the issued certificate.
Amount to Synchronize	The time range or amount of history to synchronize for each synchronization request
Sync Interval (peak)	The frequency of synchronization requests during the peak period. By default, the peak period is normal business hours, from 9:00 AM to 5:00 PM. To synchronize only when there are new items to synch, select *Push*. To require the user to synch items manually, select *Manual*.

Setting	Description
Vibrate on Email Notification	Allows you to set the device to vibrate when a new email message arrives
Signature	The signature for outgoing messages. If blank, the user can enter a signature.
Peak Start Time	The starting time of the peak period, normally the start of the business day. Start and end times are used to determine peak and off-peak periods for synchronization purposes.
Peak End Time	The ending time of the peak period, normally the end of the business day. Start and end times are used to determine peak and off-peak periods for synchronization purposes.
Sync Interval (off-peak)	The frequency of synchronization requests during off-peak hours. By default, the off-peak period is between 5:00 PM and 9:00 AM. To synchronize only when there are new items to synch, select *Push*. To require the user to synch items manually, select *Manual*.
Roaming Schedule	Allows you to override synchronization settings when the user is roaming. Select *Manual* to require the user to synch items manually when roaming.
Email Size	Allows you to set a maximum size for emails synced to the KNOX container. To download email headers only, select *Headers Only*; to download all emails, select *All*.
Calendar Synch	Allows you to configure whether or not to synch the calendar on the account
Calendar Synch Period	The time range to synchronize when synchronizing the calendar
Contacts Synch	Allows you to configure whether or not to synch contacts on the account
Set as Default Account	Allows you to set the account as the default

2.18.4.7.6 Firewall Policy Page

The firewall policy allows you to create firewall rules that control network traffic to and from the KNOX container on a Samsung device. You can create Allow, Deny, Reroute, and Redirect Exception rules. The KNOX firewall inspects the destination host and port on incoming and outgoing network packets and allows, redirects, or drops them based on the rules you configure here. You can also create rules to block the browser in the KNOX container from accessing a URL.

Allow and Deny Rules

Allow rules let you specify allowed destination addresses for incoming and outgoing traffic. For example, to define an allow rule that allows outgoing traffic to port 80 on IP 1.2.3.4, specify "1.2.3.4" for the host, "80" for the port, and "remote" for the port location.

Deny rules let you specify the denied destination addresses for incoming and outgoing traffic for a specified application. For example, to define a deny rule that drops outgoing traffic from a KNOX container app to port 80 on IP 1.2.3.4, specify "1.2.3.4" for the host, "80" for the port, "remote" for the port location, and the package name of the app.

Setting	Description
Hostname	The domain name or IP address of the destination device. IP ranges such as "100.0.0.0-100.0.0.10" are allowed. Use an asterisk (*) as a wildcard to allow or deny all IP addresses. Required.
Port	The port on the destination device. Port ranges such as "8080-8085" are allowed. Use an asterisk (*) as a wildcard to allow or deny all ports. Required.
Port Location	Allows you to specify whether the port is located on the device or on a remote device. Options are "All", "Local", and "Remote".
Application Package	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle". For deny rules only.
Network Interface	Allows you to specify whether the rule applies to connections through a Wi-Fi or data network interface

Reroute Rules

Reroute rules let you to reroute traffic from applications running within the KNOX container from one target IP address and port to another IP address and port. This allows you to redirect traffic to a proxy server.

Setting	Description
Host Target	The domain name or IP address of the target device. IP ranges such as "100.0.0.0-100.0.0.10" are allowed. Use an asterisk (*) as a wildcard to redirect traffic to all IP addresses. If you use a wildcard, ensure the proxy is configured to resolve DNS; otherwise, Web pages will be accessed only through their raw IP addresses. Required.
Port Target	The port on the target device. Port ranges such as "8080-8085" are allowed. Use an asterisk (*) as a wildcard to allow or deny all ports. Required.
Proxy IP Address	The IP address of the proxy server.

Setting	Description
Proxy Port	The port on the proxy server where you want to redirect traffic. You cannot use an asterisk (*) as a wildcard to allow or deny all ports.
Application Package	The name of the package. For example, the application package name for the Kindle for Android application is "com.amazon.kindle".
Network Interface	Allows you to specify whether the rule applies to connections through a WiFi or data network interface

Redirect Exception Rules

Redirect exception rules let you override reroute rules to exclude specific target IP destinations from being rerouted.

Setting	Description
IP Address	The domain name or IP address of the destination device. IP ranges such as "100.0.0.0-100.0.0.10" are allowed. Use an asterisk (*) as a wildcard to allow or deny all IP addresses. Required.
Port Target	The port on the destination device. Port ranges such as "8080-8085" are allowed. Use an asterisk (*) as a wildcard to allow or deny all ports. Required.

Blocked URL Rules

Blocked URL rules let you block the browser in the KNOX container from accessing a Web page, site, or domain.

Setting	Description
URL	The URL of the Web page or site you want to block. Use an asterisk (*) as a wildcard to block all Web pages on a site. For example: *.example.com or www.example.com/*. Required.

2.18.4.7.7 Password Policy Page

Configure password settings for the KNOX container. For example, you can set the timeout period, the password type, and the expiration period. You can also define character strings that are not allowed in the KNOX password.

Setting	Description
Enable KNOX Password Policy	Allows you to set a password policy for KNOX containers. Enable this check box to make the other settings available.
Maximum Security Timeout	The amount of time without activity before the KNOX container is locked. To disable timeout on the KNOX container, select *Not Enforced*.
Maximum Failed Attempts	The number of incorrect passwords entered before the KNOX container is locked. Once locked, only an Afaria admin can unlock the KNOX container.
Minimum Length	The minimum length of the password from 6 to 16
Quality	The type of password required either *Alphanumeric* (numbers and letters) or *Symbol Required* (numbers, letters, and symbols).
Minimum Numbers and Symbols	The minimum number of numbers and symbols required from 2 to 16. This field is only available if you select "Symbol Required" from the *Quality* list.
Maximum Character Occurrences	Maximum number of times from 0 to 16 a character can occur in the password. A setting of "0" means the rule is not enforced.
Maximum Character Sequence	Maximum number of character in sequence from 0 to 16 that can occur in the password. For example, a setting of "5" prevents users from using "ABCDEF" as a password. A setting of "0" means the rule is not enforced.
Maximum Numeric Sequence	Maximum number of numbers in sequence from 0 to 16 that can occur in the password. For example, a setting of "5" prevents users from using "123456" as a password. A setting of "0" means the rule is not enforced.
Expiration Days	The number of days after a password is set before it expires and must be changed. Range is 0 to 365 (1 year). A setting of "0" means the rule is not enforced and the password will never expire.
Prior Passwords Blocked	The number of prior passwords blocked. If the field is set to "7", the user is prevented from reusing any of their last 7 passwords. Default is "7".
Minimum Character Changes	Minimum number of characters from 1 to 16 that must change when setting a new password. For example, setting this field to "2" prevents users from simply incrementing their password by changing a trailing number from "3" to "4".
Show Password Option	Allows you to control if the password is shown or hidden when the user logs in to the KNOX container. If this field is set to "Hidden", the password is masked.

Setting	Description
Forbidden Strings	Allows you to define character strings that are not allowed to be used as a password. For example, defining "password" prevents users from using this as their password. To define a string, click *Add* and enter the string in the *Forbidden String* field.

2.18.4.7.8 Premium VPN Policy Page

The VPN policy allows you to define how a Samsung KNOX device connects to your enterprise's virtual private network (VPN). To create a VPN policy, create one or more VPN profiles and then either add them to a list of VPN profiles available from KNOX or associate them with an application on the device. VPN profiles define the VPN settings required to establish a connection to the VPN server including the VPN server hostname or IP address, the authentication method required, and Internet Key Exchange (IKE) configuration information.

> **i** Note
>
> The VPN policy requires that the Mocana KeyVPN app and KeyVPN service APKs are installed on the device.

VPN Profile Settings

Setting	Description
Operating Mode	Allows you to specify the operating mode, either "FIPS" or "Non-FIPS". FIPS stands for “Federal Information Processing Standards” and is a set of US Government standards for computer systems. If you select "FIPS", the VPN client on the device only allows connections to FIPS-compliant VPN servers.
Name	A name for the VPN profile. This name identifies the profile in the VPN profile list in Afaria and on the device
Server	The hostname or IP address of the VPN server
Authentication	Allows you to specify if a username and password is required to access the VPN server. If "Required" is selected, enter a username and password in the appropriate fields.
Username	The username of an account on the VPN server. This field is disabled if "Not Required" is selected from the *Authentication* list.
Password	The password of an account on the VPN server. This field is disabled if "Not Required" is selected from the *Authentication* list.

Setting	Description
Authentication Method	The authentication method required for establishing a network connection with the VPN server, either "Pre-shared Key" or "Certificate". If "Pre-shared Key" is selected, provide the key as well as the IKE Identity type and ID.
Pre-shared Key	The pre-shared key required to authenticate the network connection between the VPN server and the device. This field is disabled if "Certificate" is selected from the *Authentication Method* list.
CA Certificate	The certificate the VPN server uses to authenticate the network connection. This field is disabled if "Pre-shared Key" is selected from the *Authentication Method* list. To add a CA certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate.
User Certificate	The certificate the device uses to authenticate the network connection. This field is disabled if "Pre-shared Key" is selected from the *Authentication Method* list. To add a user certificate, click *Add Certificate*, browse to and select the certificate file, and then specify a password for the certificate. To request a certificate from your Certificate Authority, click *Add Request* , select a CA profile from the drop-down list, and specify the common name, Subject Alt Name type and value, and password for the certificate.
IKE Identity	The identity type of the local endpoint that performs VPN tunnel negotiations. Types supported are: "Automatic", "IP Address", "Domain Name", "Email Address", and "Key Identifier". IKE is Internet Key Exchange, an IPsec protocol used to establish the connection to a virtual private network.
IKE Identity Value	The identity of the local endpoint that performs VPN tunnel negotiations. The value must match the type selected from the *IKE Identity Type* list. If "Automatic" is selected, the system determines the value and this field is disabled. IKE is Internet Key Exchange, an IPsec protocol used to establish the connection to a virtual private network.
Backup Server	The hostname or IP address of the backup VPN server
IKE Version	The IKE protocol phase, either 1 or 2. If phase 1 is selected, select the mode from the *IKE Phase 1 Mode* list.
IKE Phase 1 Mode	The phase 1 mode either "Main" or "Aggressive". This list is disabled if "2" is selected from the *IKE Version* list.

Setting	Description
MOBIKE	Specifies whether the VPN server uses MOBIKE. MOBIKE is a version of IKE for mobile devices and allows mobile devices to maintain a connection to the VPN even as the IP address changes.
Dead Peer Detection	Specifies whether the VPN server uses dead peer detection. Dead peer detection is a method for detecting a dead IKE peer. It is a "keep alive" sent between client and server to help detect when the connection goes down.
Perfect Forward Secrecy	Specifies whether the VPN server uses Perfect Forward Secrecy. Perfect Forward Secrecy ensures that a session key derived from a private key is not compromised if the private key is compromised in the future. If enabled, keys are renegotiated periodically; if disabled, then the key exchange happens only once.
Suite B Algorithm	Specifies the Suite B algorithm used by the VPN server. Suite B is a set of cryptographic algorithms from the National Security Agency.
Diffie-Hellman	Specifies the Diffie-Hellman group used to establish the VPN connection. Diffie-Hellman is a method for exchanging keys.

Device-Wide VPN Settings

Use these settings to configure device-wide VPN connection profiles you want to push to the device. These VPN connection profiles appear in the VPN profile list on the device and can be used by the user to initiate a connection to your enterprise's VPN.

Setting	Description
Include/Exclude	Select "Include" to configure the VPN connection profile on the device when the policy is run. If you select "Exclude", the profile is not configured on the device.
VPN Profile	The name of a VPN profile configured in the VPN Profiles list
Split Tunnel Type	Specifies whether the VPN connection allows split tunneling. Split tunneling allows the user to access a public network directly rather than through the VPN server. If "manual' is selected, provide one or more network addresses in the *Forward Routes* field.
Forward Routes	Allows you to specify network addresses for split tunneling if "manual" is selected from the *Split Tunnel Type* list. Enter network addresses in a semicolon (;) delimited list CIDR notation.

Application VPN Settings

Use these settings to associate an application with a VPN profile. If you associate a VPN with an application, the device establishes a VPN connection for the application as soon as the profile is applied to the device. This

application remains connected to the VPN indefinitely. Only traffic for the specified app is forwarded through the tunnel. You can create per-app for both KNOX and non-KNOX applications using the appropriate list.

Setting	Description
Default VPN Profile	The default VPN profile for KNOX app VPN connections
Include/Exclude	Select "Include" to configure the VPN connection profile on the device when the policy is run. If you select "Exclude", the profile is not configured on the device.
Application Name	The name of the application such as "com.amazon.kindle"
VPN Profile	The name of a VPN profile configured in the VPN Profiles list

2.18.4.7.9 Restriction Policy Page

Configure restrictions on the KNOX container. For example, you can configure the policy to disable the camera when inside the KNOX camera.

Setting	Description
Share List	Allows you to enable or disable a share list
Camera	Allows you to enable or disable the device's camera
Keyboard	Allows you to restrict users to using the Samsung keyboard. To allow users to use a different keyboard on the device, select "User-controlled".

2.18.4.7.10 Security Policy Page

Configure the KNOX attestation security check for KNOX-capable devices.

Setting	Description
Enable KNOX Security Policy	Allows you to set a security policy for KNOX containers. Enable this check box to make the other settings available.
KNOX Attestation	Allows you to enable or disable KNOX Attestation on the device. If you enable this security check, select a failure action from the *Failure Action* list.
Failure Action	Specifies the action taken if the KNOX Attestation security check fails. Options are: • Log Only – Logs the failure but does not block the creation of the KNOX container

Setting	Description
	• Block KNOX (Mixed Mode) – Blocks the creation of the KNOX container on devices that support Attestation • Block KNOX (all devices) – Blocks the creation of the KNOX container on all devices. If the device does not support Attestation, the Attestation security check fails and the KNOX container is not created on the device.

2.18.4.7.11 Single Sign-On Policy Page

Configure single sign-on (SSO) on the KNOX container. Single sign-on allows users to sign in to SSO-enabled applications in the KNOX container with one set of credentials.

Setting	Description
Enable KNOX Single Sign-On (SSO) Policy	Allows you to Single Sign-On for KNOX containers. Enable this check box to make the other settings available.
Provider's Customer ID	The provider's customer ID
Company Name	The company name
Company Logo	The file for the company logo. To select the logo file, click *Browse* to navigate to the file location, select the file, and click *Open*.
SSO Enabled Applications	Allows you to specify which applications to include in Single Sign-On. To include an application, click *Add* and enter the package name of the application in the *Application* field.

2.18.4.8 Post-Session Processing for Policies

For configuration policies, some configuration items require processing after the Afaria session ends.

After an Afaria session ends, the user may see informational and error messages in the device log. Messages are received from the device and appear in the device log without formatting. These messages are normal. Set expectations with your users.

2.19 iOS Policies

App Store Application Policies for iOS Devices [page 111]

iOS App Store application policies define which Apple App Store applications are available for install from the Afaria application app list.

Enterprise Application Policies for iOS Devices [page 119]
: iOS enterprise application policies define which enterprise-signed applications are available for devices to install.

Creating a Configuration Policy for iOS [page 130]
: Create a policy to create MDM payloads, which define settings such as settings for items such as Wi-Fi and passcodes.

Creating an Enrollment Policy for iOS [page 172]
: Create a policy for enrolling iOS devices in Afaria management.

Volume Purchase Program Licensed Application Policies for iOS Devices [page 177]
: The Volume Purchase Program (VPP) from Apple provides a simple and efficient method to purchase iOS apps from the App Store in bulk, for distribution within your organization. iOS VPP licensed application policies define which Apple VPP store apps can be installed on the devices in your enterprise.

Per-App VPN Considerations [page 184]
: Per-app VPN profiles help you to secure application data, control access to your corporate network, and control use of your corporate VPN.

2.19.1 App Store Application Policies for iOS Devices

iOS App Store application policies define which Apple App Store applications are available for install from the Afaria application app list.

Commercial applications are delivered from the Apple App Store.

Application package content includes:

- Identifying information for the application
- (Optional) Information for Apple redemption codes
- (Application onboarding) File or data for application onboarding data provisioning

Creating an Application Policy for iOS App Store Apps [page 112]
: Create a policy for an application from the Apple App Store, including taking over management of an already-installed unmanaged application on a user's device.

Deploying iOS App Store Apps [page 115]
: Deploy iOS applications by deploying the application policy to a device automatically using the MDM protocol option or allow a user to browse the app list on their device and install the application.

iOS App Store Application Policy Settings [page 115]

2.19.1.1 Creating an Application Policy for iOS App Store Apps

Create a policy for an application from the Apple App Store, including taking over management of an already-installed unmanaged application on a user's device.

Prerequisites

Complete the procedure to prepare an App Store application, which includes recording the application's App Store number and country code.

The device user must have an iTunes account. App Store user agreements and costs are independent.

Context

- The policy includes multiple pages, which should be completed in order. To save changes on all pages, click *Save* at the top of any page.
- To take over management of an already-installed unmanaged application on a user's device, follow these instructions, specifying the unmanaged application in the *Search by App Name* field. The status of the request to take over management is found in the Package Tracking Log (in the *Device* list or *Policy* list), in the *Status by MDM* column. Refer to *Viewing the Device Package Tracking Log* for detaled information.
- The *Configuration* page is reserved for application onboarding data provisioning and is not part of this procedure. See the topic *Provisioning Data for iOS and Android Applications* for more details.

Procedure

1. On the *Policy* list page on the top toolbar, click *New* > *Application* > *iOS App Store*.
2. On the *Summary* page, enter the policy name and note, and indicate whether the policy is published or unpublished.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Connecting devices receive only published policies.
3. (Optional) Select *Featured* to tag the application as featured, which means it appears in a ticker on the home page of the device.
4. On the General page, enter the app name in the Search by App Name field.
   A dynamic list of all apps from the App Store that match the entered app name is displayed.
5. Enter a valid Country Code in order to use the Search by App Name feature or retrieve an app using the App Store number and bundle ID. The default value for Country Code is 'US'.
6. Select the desired app from the results list.
   The fields AppStore Number, Bundle ID, and Information are automatically populated with information.
7. Alternatively, if you do not want to use the Search by App Name feature, you can type in the App Store number or bundle ID, and click *Update* to retrieve the desired app and its corresponding details.

> **Note**
>
> The Country Code is required in order to retrieve app details using App Store number or bundle ID.

- AppStore Number – application number from Apple App Store. You can find the application number in the URL for the application. You must provide the App Store number or the bundle ID for the app.
- Country Code – country code for Apple App Store. The default value for Country Code is 'US'.
- (Optional) Bundle ID – bundle identifier for the application on the Apple App Store. The bundle identifier populates automatically when you click *Update* after typing a valid App Store number. To support package tracking capabilities, enter the identifier, as defined by the developing entity. For example, the identifier for application "Paper Toss" developed by Backflip Studios is com.backflipstudios.PaperToss. Afaria reports this value in a device's software inventory "Identifier" field. Enter the application package after you retrieve the identifier from the software view.

  > **Note**
  >
  > If this field is left blank and the App Store package is deployed using the MDM protocol, it is automatically populated with the application identifier during the MDM process. If you enter the ID manually, please note that it is case sensitive and must be entered exactly as the identifier appears in the application for package tracking results to display correctly. The package server does not serve an application policy without the ID, to the connecting devices.

- Deploy using MDM protocol – enable this option to push the application policy to the device when MDM commands are processed.
  - Prevent data backup – this setting blocks the backup utility (in iTunes) from backing up the data for this application from the device to the backup stored in iTunes. This option is automatically selected and is editable, if you select 'Deploy using MDM protocol'.
  - Remove with MDM relationship – if the device is removed from MDM control, the application is removed from the device. This option is automatically selected and is editable, if you select 'Deploy using MDM protocol'.
  - Not MDM managed – this indicates whether the application is managed using MDM. This option is enabled only if you select 'Deploy using MDM protocol'.

  > **Note**
  >
  > Apps deployed using the MDM protocol do not appear on the *Updates* tab of the iOS Afaria application when an update is available. Instead, updates are pushed to the device during the next connection to the Afaria server.

- Per-App VPN – select the VPN profile if the application uses one. You can create VPN profiles using configuration policies.
- Install – choose optional or required. MDM protocol is mandatory for required apps. Applications configured with the MDM protocol option are pushed to the device automatically the next time that the device connects. Optional apps are pushed to the device when the application policy is applied the next time a device connects. Users can browse to and manually install optional apps in their Afaria apps list. The Install field is enabled only if *Deploy using MDM protocol* is selected.
- B2B App – enable this option if the application is a business-to-business application.
- App Icon – click *Browse* and select the icon for the B2B application. App icon supports JPG, JPEG and PNG formats with a resolution of 57x57 pixels.
- ArtWork – click *Browse* and select the artwork image for the application. Artwork supports JPG, JPEG and PNG formats with a resolution of 512x512 pixels.

Data retrieval is subject to data availability from the App Store.

8. (Optional) On the Categories page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.

9. (Optional) Select *Yes* or *No* to indicate if the selected category is a featured category.

10. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note.

    > **i Note**
    >
    > The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. It is recommended that you use smaller image files of size up to 100KB, to enable easy download and to minimize data traffic.
    >
    > The recommended resolution for the category image on an iOS device is up to 1448 x 1422 pixels (iPad 3 with retina display). The category image is scaled to the required resolution, without changing the aspect ratio, and is then center-cropped.

11. (Optional) In the Available Categories list, make changes by selecting a category and clicking *Edit*, *Delete*, *Inspect Image* or *Clear Image*.

    If you delete a category that is attached to another policy, the category is deleted from the referring policy also.

    Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

    If the user wishes to upload an image file in the application policy under categories section, then the user must perform the following steps when the ASA database is hosted on a remote machine:

    1. From Sybase Central (ASA 12), Set 'allow_read_client_file' option value to 'On' in Database Options. (To access go to *File* > *Options* while on the database view).
    2. Click *Set Permanent Now*.
    3. Set 'allow_read_client_file' option value to 'On' for your user in User Options. (To access go to *File* > *Options* while on the users & groups view.)
    4. Restart the ASA database server.

    Clicking *Clear Image* removes the image associated with the category.

12. (Optional) In the Pre-defined Categories list, make changes by selecting a category and clicking *Edit*, *Inspect Image* or *Clear Image*.

    Enterprise, App Store and All are the Pre-defined System Categories listed.

    Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

    Clicking *Clear Image* removes the image associated with the Pre-defined Category.

13. (Optional) On the Description Detail page, enter a description for the application and modify the display name.

    The display name of the application is automatically updated when you upload the application package on General page.

14. (Optional) On the Redemption Codes page, click *Add* to add a redemption code purchase order spreadsheet, as received from Apple.

    Redemption codes are required by users for Apps with a charge being deployed via MDM.

After the user enrolls in device management and application policies are created, applications are deployed to devices in the following ways:

- The user browses the App Store list and installs the application.
- If the device was put under MDM control during the enrollment phase, when device connectivity is established, applications are installed immediately.

2.19.1.2 Deploying iOS App Store Apps

Deploy iOS applications by deploying the application policy to a device automatically using the MDM protocol option or allow a user to browse the app list on their device and install the application.

Prerequisites

The device user must have an iTunes account with Apple. App Store user agreements and costs are independent of Afaria operations.

Complete the procedures to prepare for an iOS App Store application, which includes creating the application policy and configuring it for use with the MDM protocol option, if desired.

> **i** Note
>
> The MDM protocol option is not compatible with an iOS Configuration policy with a Restriction payload that disables the Apple App Store.

Procedure

Users open Afaria, enrolling or reenrolling in device management.
The device connects to Afaria. If the policy was defined using the MDM protocol with Install Required option, the user is prompted to install each application pushed to the device. A user can postpone an installation, but not cancel it. If the policy is defined using the MDM protocol with Install Optional option or not defined with the MDM protocol option, the application appears in their app list for installation.

2.19.1.3 iOS App Store Application Policy Settings

Summary Page [page 116]

General Page [page 116]

Categories Page [page 118]

Description Detail Page [page 118]

Configuration Page [page 118]

Redemption Codes Page [page 119]

2.19.1.3.1 Summary Page

Setting	Description
Policy	The name of the application policy.
Note	The description of the application policy.
State	Whether the policy is published or unpublished.
Last Modified	The date when the policy was last modified.
Type	The type of the policy.
OS	The device operating system to which the policy applies.
Featured	Whether the application that the application policy governs is featured on devices. The SAP Afaria client displays featured applications on the client home page.

2.19.1.3.2 General Page

Setting	Description
AppStore Number	The application number from the Apple App Store. You can find the application number in the URL for the application. When you have typed the application number, click *Update* to populate the application policy with information about the application from the App Store.
Country Code	The country code for Apple App Store.
Bundle ID	The bundle identifier for the application on the Apple App Store. The bundle identifier populates automatically when you click *Update* after typing a valid App Store number.

Setting	Description
Information	The description and icon for the application. The information populates automatically when you click *Update* after typing a valid App Store number.
Deploy using MDM protocol	Whether the application is deployed using the MDM protocol.
Prevent data backup	Whether users can back up application data using iTunes. This option is automatically selected and is editable, if you select 'Deploy using MDM protocol'.
Remove with MDM relationship	Whether the application is removed when the MDM relationship is removed from the phone. This option is automatically selected and is editable, if you select 'Deploy using MDM protocol'.
Not MDM managed	Whether the application is not managed using MDM. This option is enabled only if you select 'Deploy using MDM protocol'.
Per-App VPN	The VPN profile that the application uses. You create VPN profiles using configuration policies. This field is enabled if you select 'Deploy using MDM protocol'.
Install	Whether the application is optional or required. Install option automatically changes to 'Required', if you select 'Deploy using MDM protocol'; you can manually change this option if needed.
B2B App	Whether the application is a business-to-business application. In the Redemption Codes page, the administrator uploads the redemption codes for the B2B apps purchased.
App Icon	The icon for the business-to-business application. Click *Browse* and select the icon for the application. App icon supports JPG, JPEG and PNG formats with a resolution of 57x57 pixels.
ArtWork	The artwork for the business-to-business application. Click *Browse* and select the artwork image for the application. Artwork supports JPG, JPEG and PNG formats with a resolution of 512x512 pixels.

2.19.1.3.3 Categories Page

Settings	Description
Available Categories	The categories that you can associate with the application.
Selected Categories	The categories associated with the application.
Pre-defined Categories	The pre-defined categories that you can associate with the application.

2.19.1.3.4 Description Detail Page

Setting	Description
Display Name	The display name of the application. This field updates automatically if you click *Update* after entering a valid App Store number.
Afaria Description	The application description that the SAP Afaria client displays.

2.19.1.3.5 Configuration Page

Setting	Description
Managed App Configuration	The configuration data for managed applications on iOS 8 and later devices. You can use configuration data to configure application settings remotely. When you add configuration data, you add a parameter name and a value. The managed application then uses the value whenever it requires the parameter.
Configuration Data: Format	The format of the configuration data. For binary file and text (file), you must browse to and select the file. For text, type the configuration data in the text box.

Setting	Description
Security: Enable Signing Certificate	Whether the application uses a signing certificate to secure the connection between the Afaria client and the SAP Afaria package server to receive configuration date. For this setting to apply, the application must support digital signing.
Security: Signing Certificate Name	The name of the signing certificate. By default, the certificate name is the name of the Apple push certificate that you add on the iOS Notification page of the Server configuration in the Afaria Administration console.

2.19.1.3.6 Redemption Codes Page

Setting	Description
Redemption Code table	The redemption codes for the application. You can purchase and download redemption codes from the Apple App Store. When you have a spreadsheet with redemption codes, add the redemption code file to this page.

2.19.2 Enterprise Application Policies for iOS Devices

iOS enterprise application policies define which enterprise-signed applications are available for devices to install.

Enterprise-signed applications are produced by your developing entity and are delivered from the Package Server. Application packages include:

- Identifying information for the application
- MDM protocol, if defined
- (Application onboarding) File or data for application onboarding data provisioning

The preparation and deployment process differs based on whether you define the application as required or optional in the application policy:

- Required – for deployment, users are prompted from the Afaria application to install the application automatically without browsing a list of applications. Preparing for deployment includes:
  1. Compile the application.
  2. Deploy its provisioning file in a configuration policy.
  3. Create an application policy.
- Optional – for deployment, users must use the Self-Service Portal for device management to browse and install applications. Preparing for deployment includes:

1. Compile the application.
2. Deploy its provisioning file in a configuration policy.
3. Create an application policy.
4. Create an enrollment policy to define the appropriate group for the application policy.
5. Install, reinstall, or verify an instance of the portal that is configured for the enrollment policy.
6. Update the enrollment policy with a reference to the portal for the app list that appears in the device's Afaria application.

Preparing iOS Devices for Application Management [page 120]
Enroll iOS devices in management prior to deploying applications to prepare them for application management.

Preparing for iOS Enterprise Application Management for Required Applications [page 120]
For each required enterprise-signed application of interest, make the compiled application and its provisioning file available for Self-Service Portal use, deploy the provisioning file to devices, and create the application policy. Deploying the provisioning file in advance of the application ensures that you can disable the application in the future if needed.

Preparing for iOS Enterprise Application Management for Optional Applications [page 121]
For each optional enterprise-signed application of interest, make the compiled application and its provisioning file available to Afaria to prepare for Self-Service Portal use, and deploy the provisioning file to devices. The portal self-management lets users browse and install optional enterprise applications. Deploying the provisioning file in advance of the application ensures that you can disable the application in the future.

Creating an Application Policy for iOS Enterprise Applications [page 122]
Create an application policy for enterprise applications on iOS devices.

Deploying iOS Enterprise Applications [page 125]
Deploy iOS enterprise required or optional applications.

Disabling an iOS Enterprise Application on a Device [page 126]
Disable an optional or required enterprise application to prevent the user from running it.

iOS Enterprise Application Policy Settings [page 126]

2.19.2.1 Preparing iOS Devices for Application Management

Enroll iOS devices in management prior to deploying applications to prepare them for application management.

2.19.2.2 Preparing for iOS Enterprise Application Management for Required Applications

For each required enterprise-signed application of interest, make the compiled application and its provisioning file available for Self-Service Portal use, deploy the provisioning file to devices, and create the application policy. Deploying the provisioning file in advance of the application ensures that you can disable the application in the future if needed.

Prerequisites

This procedure describes preparing for managing devices that have the Apple App Store version of the Afaria application installed, rather than an enterprise-signed version of Self-Service Portal.

Procedure

1. Compile your application according to iOS Developer Enterprise Program procedures.

   The Apple iOS Developer Enterprise Program is defined and managed by Apple.
2. Make a copy of the compiled application (`.ipa`) and the application's associated provisioning file (`.mobileprovision)`) available to the Afaria Administration console user responsible for creating application policies.

   The application must include a complete manifest file (`.plist`), as defined by Apple iOS Developer Enterprise Program.
3. On the Policy page, create an iOS configuration policy that uses the application's provisioning file to define an MDM Payload > Provisioning File item.
4. Deploy the provisioning file to the group to which you plan to deploy the application.
   a. On the Policy page, link the configuration policy to the group.
   b. On the Group page, send a command to the group to connect the group's devices to apply policies. Devices connect to Afaria and install the provisioning file without requiring user interaction. You can verify the file on the device on the Settings > General > Profiles page.
5. On the Policy page, create an application policy for the application with the required attribute.

2.19.2.3 Preparing for iOS Enterprise Application Management for Optional Applications

For each optional enterprise-signed application of interest, make the compiled application and its provisioning file available to Afaria to prepare for Self-Service Portal use, and deploy the provisioning file to devices. The portal self-management lets users browse and install optional enterprise applications. Deploying the provisioning file in advance of the application ensures that you can disable the application in the future.

Prerequisites

This procedure describes preparing for managing devices that have the Apple App Store version of Afaria installed, rather than an enterprise-signed version.

Procedure

1. Compile your application according to iOS Developer Enterprise Program procedures.

   The Apple iOS Developer Enterprise Program is defined and managed by Apple.
2. Make a copy of the compiled application (`.ipa`) and the application's associated provisioning file (`.mobileprovision`) available to the administrator responsible for creating application policies.

   The application must include a complete manifest file (`.plist`), as defined by Apple iOS Developer Enterprise Program.
3. On the Policy page, create a configuration policy for iOS devices that uses the application's provisioning file to define an MDM Payload > Provisioning File item.
4. Deploy the provisioning file to the group to which you plan to deploy the application.
   a. On the Policy page, link the configuration policy to the group.
   b. On the Group page, send a command to the group to connect the group's devices to apply policies. Devices connect to Afaria and install the provisioning file without requiring user interaction.
5. On the Policy page, create an application policy for the application with the optional attribute.
6. On the Policy page, create an enrollment policy that includes the group.
7. Install, reinstall, or verify an instance of Self-Service Portal that is configured for the enrollment policy to which the group can connect for reenrollment and management.
8. On the Policy page, update the enrollment policy on the General page to define the attributes for Self-Service Portal.
   - Title – user-facing title for identifying the portal in the Self-Service Portal application app list on the device.
   - Description – user-facing description for the portal in the Self-Service Portal application app list on the device.
   - URL – address for the portal that is configured with the enrollment policy.

2.19.2.4 Creating an Application Policy for iOS Enterprise Applications

Create an application policy for enterprise applications on iOS devices.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

The Configuration page is reserved for application onboarding data provisioning and is not part of this procedure. See topic *Provisioning Data for iOS and Android Applications* for more details.

Procedure

1. On the top toolbar, click *New* > *Application* > *iOS Enterprise*.
2. On the *Summary* page, type a name for the policy.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in the Self-Service Portal application to support duplicate policy names and multiple categories are compatible with Self-Service Portal 6.6 and Self-Service Portal 7 servers.
3. Enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished.
   - Featured – enable to tag the application as featured, which means it appears in a ticker on the home page of the device.
4. On the General page, define application details.
   - Passcode – require passcode before allowing the application to install. The passcode must be enabled on the device, as recorded in the device inventory on the server, before allowing the application to install.
   - Deploy using MDM protocol – enable this option to push the application policy to the device automatically when MDM commands are processed.
     - Prevent data backup – blocks the backup utility (in iTunes) from backing up the data for this application from the device to the backup stored in iTunes.
     - Remove with MDM relationship – if the device is removed from MDM control, the application is removed from the device. If an application is configured to be removed using MDM, the relationship is removed but the application remains on the device.
   - Install – choose optional or required. MDM protocol is mandatory for required apps. Applications configured with the MDM protocol option are pushed to the device automatically the next time the device connects. Optional apps are pushed to the device when the application policy is applied the next time a device connects. Users can browse to and manually install optional apps in their Self-Service Portal apps list.

     > **i Note**
     >
     > In the event that the user uninstalls a required application from the device, an inventory scan (device refresh) has to be initiated from the server in order to get the updated software inventory from the device to update the Package Tracking status to `Uninstalled`. When the SAP Afaria inventory shows that the application is no longer installed, the user receives a prompt to install the application only when a subsequent Apply Policies action is sent from the server. You must either manually send an Apply Policies notification to that device, or set the iOS Apply Policies schedule accordingly.
   - IPA – click *Browse* to locate and upload the application (`.ipa`). If an application image is detected inside the IPA file, it is displayed as the Application Icon. The file path is relative to the administrator user's workstation.
     The package server does not serve an application policy without the IPA file details, to the connecting devices.
   - Artwork (512x512px) – click *Browse* to locate and upload the image, which appears as the Featured Application Artwork. This is enabled only if there is no pre-existing artwork image.
     Artwork supports PNG and JPEG formats with a resolution of 512x512 pixels.

5. (Optional) On the Categories page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.

6. (Optional) Select *Yes* or *No* to indicate whether the selected category is a featured category.
7. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note.

   > **i Note**
   >
   > The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. It is recommended that you use smaller image files of size up to 100KB, to enable easy download and to minimize data traffic.
   >
   > The recommended resolution for the category image on an iOS device is up to 1448 x 1422 pixels (iPad 3 with retina display). The category image is scaled to the required resolution, without changing the aspect ratio, and is then center-cropped.

8. (Optional) In the Available Categories list, make changes by selecting a category and clicking *Edit*, *Delete*, *Inspect Image*, or *Clear Image*.

   If the user wishes to upload an image file in the application policy under categories section, then the user must perform the following steps when the ASA database is hosted on a remote machine:

   1. From Sybase Central (ASA 12), Set 'allow_read_client_file' option value to 'On' in Database Options. (To access go to *File* > *Options* while on the database view).
   2. Click *Set Permanent Now*.
   3. Set 'allow_read_client_file' option value to 'On' for your user in User Options. (To access go to *File* > *Options* while on the users & groups view.)
   4. Restart the ASA database server.

   If you delete a category that is attached to another policy, the category is deleted from the referring policy also.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking *Clear Image* removes the image associated with the Available Category.

9. (Optional) In the Pre-defined Categories list, make changes by selecting a category and clicking *Edit*, *Inspect Image* or *Clear Image*.

   Enterprise, App Store and All are the Pre-defined System Categories listed.

   Clicking *Inspect Image* opens the image in *Server* > *Category Image File* window.

   Clicking *Clear Image* removes the image associated with the Pre-defined Category.

10. (Optional) On the Description Detail page, enter a description for the application and modify the display name.

    The display name and the version of the application are automatically updated when you upload the application package on General page.

11. Click *New* to browse to and select the application screen shot that appears on the device.

    You can upload as many as eight screen shots from which you can select the application image to appear on the device.

    > **i Note**
    >
    > The appearance of the uploaded image may change, depending on the size of the image and the browser settings. The maximum image size allowed is 1MB.

After the user enrolls in device management and application policies are created, applications are deployed to devices in the following ways:

- The user browses the App Store list and installs the application.
- If the device was put under MDM control during the enrollment phase, when device connectivity is established, applications are installed immediately, or when an Administrator applies policies.

2.19.2.5 Deploying iOS Enterprise Applications

Deploy iOS enterprise required or optional applications.

Prerequisites

Create a new iOS enterprise application policy and define it to install as required or optional. If an application is configured to be removed using MDM, the application is deleted from the device when the MDM control is removed from the device.

Procedure

Users open the Afaria application on their device, and enroll or reenroll in device management.
The device connects to Afaria. Applications defined to deploy using MDM are pushed to the device automatically. If you did not define the application policy to use the MDM protocol, the application is considered optional and is pushed to the device next time it connects where it will display in the Afaria app list for users to browse to and manually install.

> **i Note**
>
> A user can postpone the installation of a required application, but not cancel it.

> **i Note**
>
> In the event that the user uninstalls a required application from the device, an inventory scan (device refresh) has to be initiated from the server in order to get the updated software inventory from the device to update the Package Tracking status to `Uninstalled`. Once the Afaria inventory is showing the application is no longer installed, the user will then receive a prompt to install the application ONLY when a subsequent Apply Policies action is sent from the server. You must either manually send an Apply Policies notification to that device, or set the iOS Apply Policies schedule accordingly.

> **i Note**
>
> Some latency exists between the time a user installs software and the time it is reported to the database. Therefore, a user may be prompted to install software that is already installed. Similarly, some latency exists between the time a user removes a required application and the time the server prompts the user to

install it again. To force an inventory update, Administrator can execute an apply policies action or run the iOS Device Refresh schedule.

For applications that are 100MB or smaller, the status bar effectively tracks progress. For applications larger than 100MB, the device may appear to freeze at the 100% progress point, but just needs additional time to complete. Set expectations with your users.

2.19.2.6 Disabling an iOS Enterprise Application on a Device

Disable an optional or required enterprise application to prevent the user from running it.

Context

Disabling does not remove the application from the device. Once installed, only the user can remove it. If the device is managed using MDM and removed from MDM management, the device is removed from service but the application remains on the device.

Procedure

1. On the configuration policy that delivered the application's provisioning file to the device, remove the provisioning file payload from the policy.
2. On the Group page, send a command to the group to connect the group devices to apply policies.
   The device connects to Afaria and reports its current inventory. The server delivers instructions to remove the provisioning file from the device.

Results

Subsequent attempts to launch the application fail. You can restore the user's ability to run the application by reinstalling the provisioning file payload.

2.19.2.7 iOS Enterprise Application Policy Settings

Summary Page [page 127]

General Page [page 127]

Categories Page [page 128]

Description Detail Page [page 129]

Configuration Page [page 129]

2.19.2.7.1 Summary Page

Setting	Description
Policy	The name of the application policy.
Note	The description of the application policy.
State	Whether the policy is published or unpublished.
Last Modified	The date when the policy was last modified.
Type	The type of the policy.
OS	The device operating system to which the policy applies.
Featured	Whether the application that the application policy governs is featured on devices. The SAP Afaria client displays featured applications on the client home page.

2.19.2.7.2 General Page

Setting	Description
IPA	The iPhone application (IPA) file for the application. Browse to and upload the file to this page.
Artwork	The graphic for the application. This setting is available if the iPhone application (IPA) file does not include an iTunesArtwork file. Browse to and upload the file to this page. If the iPhone application (IPA) file includes an iTunesArtwork file, devices display the artwork from the file for the application.
Information	The description of the application.

Setting	Description
Passcode: Require	Whether devices must have passcodes for the application to install. Passcodes must be configured on devices and recorded in device inventories before the application can install. Refresh the device inventories if the passcodes were set since the last refresh of the device inventories.
Deploy using MDM protocol	Whether the application is deployed using the MDM protocol.
Prevent data backup	Whether users can back up application data using iTunes.
Remove with MDM relationship	Whether the application is removed when the MDM relationship is removed from the phone. This setting is available when Deploy using MDM protocol is selected.
Per-App VPN	The VPN profile that the application uses. You create VPN profiles using configuration policies. This setting is available when Deploy using MDM protocol is selected.
Install	Whether the application is optional or required. Install option automatically changes to 'Required', if you select 'Deploy using MDM protocol'; you can manually change this option if needed.

2.19.2.7.3 Categories Page

Setting	Description
Available Categories	The categories that you can associate with the application.
Selected Categories	The categories associated with the application.
Pre-defined Categories	The pre-defined categories that you can associate with the application.

2.19.2.7.4 Description Detail Page

Setting	Description
Display Name	The display name of the application.
Version	The version of the application.
Afaria Description	The description of the application that the SAP Afaria client displays.
ScreenShots	The screenshots for the application that the SAP Afaria client displays.

2.19.2.7.5 Configuration Page

Setting	Description
Managed App Configuration	The configuration data for managed applications on iOS 8 and later devices. You can use configuration data to configure application settings remotely. When you add configuration data, you add a parameter name and a value. The managed application then uses the value whenever it requires the parameter.
Configuration Data: Format	The format of the configuration data. For binary file and text (file), you must browse to and select the file. For text, type the configuration data in the text box.
Security: Enable Signing Certificate	Whether the application uses a signing certificate to secure the connection between the Afaria client and the SAP Afaria package server to receive configuration date. For this setting to apply, the application must support digital signing.
Security: Signing Certificate Name	The name of the signing certificate. By default, the certificate name is the name of the Apple push certificate that you add on the iOS Notification page of the Server configuration in the Afaria Administration console.

2.19.3 Creating a Configuration Policy for iOS

Create a policy to create MDM payloads, which define settings such as settings for items such as Wi-Fi and passcodes.

Context

The policy includes multiple pages, such as Summary and MDM Payload. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *iOS*.
2. On the Summary page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types.
3. Enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished. Connecting devices receive only published policies.
   - Priority – set a user-defined value that SAP Afaria uses to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
4. (Optional) Configure additional pages according to your requirements.

   MDM Payloads [page 131]
   MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and e-mail applications.

   iOS NitroDesk TouchDown Configuration [page 165]
   NitroDesk TouchDown for iOS provides access to Microsoft Exchange e-mail messages, contacts, and calendars using ActiveSync technology. You can either install TouchDown directly on the device or use Afaria to push the TouchDown application to the device.

   Sending Multiple Configuration Policies to Devices [page 170]
   Afaria combines multiple policies into a single delivery payload before sending them to a device. Apple designed iOS management to support multiple instances of some policy types and support only a single instance of other policy types. Apple reserves the right to change requirements without notice.

   The SSL Option in Policies [page 171]
   If you plan to use the SSL option in any policy that includes SSL as an option, the device may require a certificate with appropriate credentials. For some policy types, you can select the appropriate certificate from within the policy editor to define credentials. For other policy types, define a separate Credentials policy.

   Embedded SCEP Requests as Identity Certificates [page 171]
   Wi-Fi and VPN policies include an option to define and embed a SCEP request to obtain an identify certificate when the policy is deployed.

Importing iOS Device Configuration Policies [page 171]
: Import Apple iPhone (iOS) configuration policies or exported Afaria policies to make them available as SAP Afaria configuration policies.

iOS Policies from the Apple iPhone Configuration Utility [page 172]
: As an alternative to using the Afaria Administration console to create device configuration policies, you can import policies that you export from the Apple iPhone Configuration Utility. From the utility, export and save policies as individual files (`.mobileconfig`). From the Afaria Administration console Administration Policy page, import policies.

Related Information

Substitution Variables [page 29]

2.19.3.1 MDM Payloads

MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and e-mail applications.

Policy definitions are compliant with the Apple iPhone Configuration Utility (iPCU) version 3.6 definitions. Refer to Apple resources for detailed guidance; for example iPCU help and Apple support resources for enterprise device management.

MDM policies can include these payload types:

- Advanced – changes the device Access Point Name (APN) and cell network proxy settings. These settings define how the device connects to the carrier's network. Change these settings only as directed by the carrier.
- AirPlay – adds AirPlay destinations to the AirPlay devices that are available to the iOS device. Use AirPlay to stream music, photos, and video wirelessly to Apple TV and other AirPlay-enabled devices on the same Wi-Fi network as iOS devices.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- AirPrint – adds printers to a device's AirPrint. Users use AirPrint to print wirelessly to an AirPrint-enabled printer, from apps such as Mail, Photos, and Safari. This makes it easier to support environments where printers and devices are on different subnets.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- Calendar – configures a connection to a calendar server. The account is added to the device and the user is prompted for any information that is required but not defined by the policy.
- Contacts – configures a connection to a contact list.

- Credential – adds certificates and identities to the device. Certificate files must be accessible from the machine running the Afaria Administration console. When installing credentials on a device, install all the intermediate certificates that link to a trusted certificate.
- Enterprise SSO – uses Kerberos SSO and authenticates user credentials only once for accessing corporate apps or apps from the App Store on a device. The device must be in a corporate network or it must be connected to corporate VPN using the Internet.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- Exchange ActiveSync – configures an Exchange ActiveSync account with a Microsoft Exchange server. You can create a policy for users by specifying the user name, host name, and e-mail address, or only the host name; Users provide other values when they install the policy.
  Consider these items about user accounts:
  - If you specify the name, host name, and SSL settings in the policy, the user cannot change these settings on the device
  - The password data element cannot contain a percent (%) character.
  - Accounts that you add to a device by installing a policy can be deleted only by removing the policy from the device.
- Font – adds an additional font to an iOS device. You can include multiple font payloads, as needed.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- Generic – lets you select from any imported payloads created in any version of the iPhone Configuration Utility.
- Global HTTP Proxy – allows you to specify global HTTP proxy settings.
- Guided Access – locks the device to a single application until the payload is removed.
- LDAP – configures a connection to an LDAP server. You can specify multiple search bases for each directory and configure multiple connections.
- Mail – configures POP or IMAP e-mail accounts. To add a Microsoft Exchange account, use an Exchange ActiveSync policy.
- Managed Domains – defines the web domains that are under an enterprise's management.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- Organization Info – contains the name, address, phone, email, and other information of the organization that provided the profile.
- Passcode – defines passcode requirements, frequency of change, and other characteristics. When the configuration policy loads, the user must enter a passcode that satisfies the policy.
- Per App VPN – configures add-on VPN software.

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- Provisioning File – adds a provisioning file (.mobileprovision) to the device, which has a role in managing enterprise-signed applications.

- Restriction – defines restrictions for user access to certain features, such as device functionality, applications, SIRI, operations on iCloud, security, and content ratings.
- SCEP – configures settings that allow the device to obtain certificates over the air from a certificate authority (CA) server that is using SCEP (Simple Certificate Enrollment Protocol).
  Embedded SCEP requests or SCEP requests that are added in Wi-Fi or VPN policies do not appear in the SCEP policy list; they are accessible only through their containing policy. This does not apply in Afaria except in the cases of mobile configuration files imported into Generic policies.
- Setting – configures voice and data roaming.
- Subscribed Calendar – adds read-only calendar subscriptions to the device Calendar application.
- VPN – configures VPN networks. There are several supported VPN protocols and methods of authentication. Depending on the configuration settings you select, the options in the editor vary.
- Web Clip – adds Web clips to the device home screen. Web clips provide fast access to favorite Web pages. The URL must begin with `http://` or `https://`.
- Web Content Filter – affects web viewing to limit sites using permitted lists and black list, or by limiting sites to only a defined list (white list).

  > **i Note**
  >
  > This payload is supported only in iOS 8 and later.

- WiFi – configures Wi-Fi networks.
  Consider these items:
  - Password for WEP or WPA security authentication – if you do not specify a password in the policy, the user is prompted to enter one when connecting to the network.
  - Enterprise security types – expose additional settings for protocols, authentication, and trust.
  - Wi-Fi policies can configure and save a network definition on a device only when the device is detecting the network when it attempts configuration.

Advanced Payload [page 135]
: The Advanced payload defines the Access Point Name (APN) and cellular network proxy settings for devices. These settings define how devices connect to mobile networks.

AirPlay Payload [page 136]
: (iOS 8 and later) The AirPlay payload adds AirPlay destinations to available devices. Use AirPlay to stream music, photos, and video wirelessly to Apple TV and other AirPlay-enabled devices on the same Wi-Fi network as iOS devices.

AirPrint Payload [page 136]
: (iOS 8 and later) The AirPrint payload adds printers to a device's AirPrint. Use AirPrint to print wirelessly to an AirPrint-enabled printer, from apps such as Mail, Photos, and Safari. This makes it easier to support environments where the printers and the devices are on different subnets.

Calendar Payload [page 137]
: The Calendar payload defines the settings that devices use to connect to a calendar account on a server. After SAP Afaria applies the payload, the calendar data is available on devices.

Cellular Payload [page 138]
: The Cellular payload defines cellular network settings for devices. Only one Cellular payload can apply to each device, and a Cellular payload cannot be applied if an Advanced payload is already applied to a device.

Contacts Payload [page 139]
: The Contacts payload defines the settings that devices use to connect to a contacts account on a server. After SAP Afaria applies the payload, contact data is available on devices.

Credential Payload [page 139]
: The Credential payload adds certificates and identities to devices. Certificate files must be accessible from the machine that is running the Afaria Administration console. When installing credentials on devices, install all the intermediate certificates that link to a trusted certificate.

Enterprise SSO Payload [page 140]
: (iOS 8 and later) The Enterprise Single Sign-On (SSO) payload uses Kerberos SSO and authenticates user credentials only once to access corporate and application store applications on a devices. Devices must either be in a corporate network or be connected to the corporate VPN using the Internet.

Exchange ActiveSync Payload [page 141]
: The Exchange ActiveSync payload configures an Exchange ActiveSync account from a Microsoft Exchange server on devices.

Font Payload [page 143]
: (iOS 8 and later) A font payload adds a font to an iOS device. You can include multiple font payloads, as needed.

Generic Payload [page 143]
: The Generic payload includes payloads created in any version of the iPhone Configuration Utility and imported into Afaria.

Global HTTP Proxy Payload [page 144]
: The Global HTTP Proxy payload defines a Web proxy server for devices. Only one Global HTTP Proxy payload can apply, and only to supervised devices.

Guided Access Payload [page 144]
: (iOS 8 and later supervised devices) The Guided Access payload locks the device to a single application, on its current version, until the payload is removed. Once locked on an application, the application is not subject to version updates.

LDAP Payload [page 146]
: The LDAP payload configures devices to connect to an LDAP server and access directory information. You can specify multiple search bases for each directory, and configure multiple connections.

Mail Payload [page 147]
: The Mail payload configures POP or IMAP email accounts on devices.

Managed Domains Payload [page 149]
: The Managed Domains payload defines the Web domains that are under the management of an enterprise.

Organization Info Payload [page 150]
: The Organization Info payload defines and sends information about your company to devices.

Passcode Payload [page 150]
: The Passcode payload defines passcode requirements, frequency of change, and other characteristics on devices. When the configuration policy loads, the user must enter a passcode that satisfies the policy.

Per App VPN Payload [page 151]
: (iOS 8 and later) The per-app VPN payload defines one or more VPN connections that you can assign to specific applications on iOS devices. You can also define a VPN connection for the Safari browser app to use to access specified domains on your network.

Provisioning File Payload [page 154]

The Provisioning File payload adds a provisioning file (`.mobileprovision`) to devices, which has a role in managing enterprise-signed applications.

Restriction Payload [page 154]
The Restriction payload defines restrictions for user access to certain features, such as device functionality, applications, Siri, operations on iCloud, security, and content ratings.

SCEP Payload [page 158]
The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

Setting Payload [page 159]
The Setting payload configures voice and data roaming options on devices.

Subscribed Calendar Payload [page 159]
The Subscribed Calendar payload adds read-only calendar subscriptions to Calendar application on devices.

VPN Payload [page 160]
The VPN payload configures VPN connections for devices. There are several supported VPN protocols and methods of authentication. Depending on the configuration settings you select, the options in the editor vary.

Web Clip Payload [page 161]
The Web Clip payload adds Web clips to the device home screen. Web clips provide fast access to favorite Web pages.

Web Content Filter Payload [page 162]
(iOS 8 and later supervised devices) The Web Content Filter payload affects Web viewing to limit sites using permitted lists and black list, or by limiting sites to only a defined list (white list).

WiFi Payload [page 163]
The Wi-Fi payload allows you to configure one or more Wi-Fi profiles on your iOS devices. A Wi-Fi profile includes the required settings to allow the device to connect to a specified wireless network.

2.19.3.1.1 Advanced Payload

The Advanced payload defines the Access Point Name (APN) and cellular network proxy settings for devices. These settings define how devices connect to mobile networks.

Setting	Description
Enabled	Select whether SAP Afaria can send the Advanced payload to devices to define APN and cellular network proxy settings.
Access Point Name	Type or use substitution variables to define the Access Point Name for the cellular network that devices should use.

Setting	Description
Access Point User Name	Type or use substitution variables to define the user name that devices use to authenticate with the access point. If you do not define this setting, devices prompt users for it when the policy is applied.
Access Point Password	Type or use substitution variables to define the encoded password that devices use to authenticate with the access point. If you do not define this setting, devices prompt users for it when the policy is applied.
Proxy Server	(Optional) Type or use substitution variables to define the IP address or URL for the access point proxy.
Port	(Optional) Type the port number for the access point proxy.

2.19.3.1.2 AirPlay Payload

(iOS 8 and later) The AirPlay payload adds AirPlay destinations to available devices. Use AirPlay to stream music, photos, and video wirelessly to Apple TV and other AirPlay-enabled devices on the same Wi-Fi network as iOS devices.

Setting	Description
Enabled	Select whether SAP Afaria can send the AirPlay payload to devices.
Passwords	(Optional) Type or use substitution variables to define the device name and password for destination devices that require a password.
Whitelist	(Optional) Type or use substitution variables to define the AirPlay destinations by providing the device ID (MAC ID) in the format (xx:xx:xx:xx:xx:xx). This setting only applies to supervised devices.

2.19.3.1.3 AirPrint Payload

(iOS 8 and later) The AirPrint payload adds printers to a device's AirPrint. Use AirPrint to print wirelessly to an AirPrint-enabled printer, from apps such as Mail, Photos, and Safari. This makes it easier to support environments where the printers and the devices are on different subnets.

Setting	Description
Enabled	Select whether SAP Afaria can send the AirPrint payload to devices.

Setting	Description
Printers	Add printers by typing or using substitution variables to define the following information: • The IP Address is the address of the AirPrint destination. • The Resource Path is the path of the AirPrint destination. Resource path (rp) is a parameter of the `_ipps.tcp` Bonjour record. If the resource path has to be null, then import the AirPrint resource as a generic payload.

2.19.3.1.4 Calendar Payload

The Calendar payload defines the settings that devices use to connect to a calendar account on a server. After SAP Afaria applies the payload, the calendar data is available on devices.

Setting	Description
Enabled	Select whether SAP Afaria sends the Calendar payload to devices to define a connection to a calendar account on a server.
Description	(Optional) Type or use substitution variables to define the description of the calendar account.
Host Name	Type or use substitution variables to define the address of the server that hosts the calendar account.
Port	(Optional) Type the port that devices use to connect to the server.
Principal URL	(Optional) Type or use substitution variables to define the base URL for the calendar account.
User name	Type or use substitution variables to define the user name that devices use to authenticate with the server.
Password	(Optional) Type or use substitution variables to define the password that devices use to authenticate with the server.
Use SSL	Select whether devices use SSL to connect to the server.

2.19.3.1.5 Cellular Payload

The Cellular payload defines cellular network settings for devices. Only one Cellular payload can apply to each device, and a Cellular payload cannot be applied if an Advanced payload is already applied to a device.

Setting	Description
Enabled	Select whether SAP Afaria can send the Cellular payload to devices to define cellular network settings.
Name	Type or use substitution variables to define the name of the access point.
Authentication	Select the type of authentication that the access point uses: • PAP (default) • CHAP
User name	(Optional) Type or use substitution variables to define the user name that devices use to authenticate with the access point.
Password	(Optional) Type or use substitution variables to define the password that devices use to authenticate with the access point.
Non-attached Access Point	Click Add and enter the following information to configure additional access points: • In the Name field, type or use substitution variables to define the name of the access point. • In the Authentication field, select the type of authentication that the access point uses. • In the User Name field, type or use substitution variables to define the user name that devices use to authenticate with the access point. • In the Password field, type or use substitution variables to define the password that devices use to authenticate with the access point. • In the Proxy Server field, type or use substitution variables to define the network address of the proxy server. • In the Port field, type the port that the proxy server uses.

2.19.3.1.6 Contacts Payload

The Contacts payload defines the settings that devices use to connect to a contacts account on a server. After SAP Afaria applies the payload, contact data is available on devices.

Setting	Description
Enabled	Select whether SAP Afaria sends the Contacts payload to devices to connect to a contacts account on a server
Description	Type or use substitution variables to define a description for the contacts account.
Host name	Type or use substitution variables to define the address of the server that hosts the contacts account.
Port	Type the port that devices use to connect to the server.
Principal URL	(Optional) Type or use substitution variables to define the base URL for the contacts accounts.
User name	Type or use substitution variables to define the user name that devices use to authenticate with the server.
Password	Type or use substitution variables to define the password that devices use to authenticate with the server.
Use SSL	Select whether devices use SSL to connect to the server.

2.19.3.1.7 Credential Payload

The Credential payload adds certificates and identities to devices. Certificate files must be accessible from the machine that is running the Afaria Administration console. When installing credentials on devices, install all the intermediate certificates that link to a trusted certificate.

Setting	Description
Enabled	Select whether SAP Afaria sends the Credential payload to devices.
Certificate	Navigate to and add the file for the identity certificate.
Password	Type the password for the certificate.

2.19.3.1.8 Enterprise SSO Payload

(iOS 8 and later) The Enterprise Single Sign-On (SSO) payload uses Kerberos SSO and authenticates user credentials only once to access corporate and application store applications on a devices. Devices must either be in a corporate network or be connected to the corporate VPN using the Internet.

You can create multiple SSO payloads in a single iOS configuration policy.

Setting	Description
Enabled	Select whether SAP Afaria can send the payload to devices.
Principal Name	Type or use substitution variables to define the Kerberos principal name.
Realm	Type the Kerberos realm name. The realm name must be fully capitalized.
App Identifiers	(Optional) Add App Identifiers to allow applications to use the single sign-on credentials. • Select App ID to require that the application matches an application identifier to use the single sing-on credentials (whitelist). • Either select an application in the Select App Policy list or type an application identifier in the Enter App ID field. The application identifiers are case sensitive and must match the application bundle ID. The App ID can be an exact match (for example, `com.mycompany.myapp`) or a prefix match with the wildcard character (*). The wildcard character must be at the end of the string after a period character (.) (for example, `com.mycompany.*`). When a wildcard is given, any app with a bundle ID that begins with the prefix is granted access to the account. If app identifiers are not provided, then all apps are enabled for SSO.
URL Prefixes	(Optional) Add URL Prefixes to allow application to use the single sign-on credentials. Applications must match the URL prefixes to use the account for Kerberos authentication over HTTP. The URL matching patterns must begin with either `http://` or `https://`. A simple string match is performed, so the URL prefix `http://www.example.com/` does not match `http://www.example.com:80/`. The pattern `http://` and `https://` matches all HTTP and HTTPS URLs, respectively. If a matching pattern does not end in a slash (/), a slash (/) is appended to it by iOS. You might need to append a / to the end of the SSO resource URL used on the device to match the pattern specified in the Enterprise SSO policy.

Setting	Description
Identity Certificate	(Optional) Click *Add Certificate* to add an identity certificate that can be used to renew the Kerberos credentials without user interaction. You can also use the *Add Request* option to provide the details to create the identity certificate. The certificate payload must have either the 'com.apple.security.pkcs12' or the 'com.apple.security.scep' payload type. Both the Single Sign On payload and the identity certificate payload must be included in the same configuration profile.

2.19.3.1.9 Exchange ActiveSync Payload

The Exchange ActiveSync payload configures an Exchange ActiveSync account from a Microsoft Exchange server on devices.

Setting	Description
Enabled	Select whether SAP Afaria sends the Exchange ActiveSync payload to devices to add an Exchange ActiveSync account.
Name	Type or use substitution variables to define the name of the Exchange ActiveSync payload.
Host	Type or use substitution variables to define the host name or IP address of the Microsoft Exchange server.
Allow Move	Select whether users can move messages out of the email account, forward messages from another email account, or reply to message from another email account.
Allow Recent Address Syncing	Select whether the account is included in address syncing.
Use Only in Mail	Select whether users can use this account only in the Mail application (and not in third-party applications).
Use SSL	Select whether the Microsoft Exchange Server uses SSL.
Domain Host	Type or use substitution variables to define the host name or the IP address of the domain host.

Setting	Description
User	Type or use substitution variables to define the user name that devices use to authenticate with the Microsoft Exchange Server. If you do not define this setting, devices prompt users for it when the policy is applied. **i Note** Verify the user format on your Exchange server before continuing. Some Exchange servers may require a fully-qualified email address in the user field in the format `<user>@<domain>`. The incorrect format may result in a failure to configure the email account on the device. When using substitution variables: • If the Exchange server requires only the unqualified user name, use only the Exchange user system variable (`%S.ExchangeUser%`) • If the Exchange server requires a fully-qualified user name, use both the Exchange user and Exchange domain system variables separated by the @ symbol (`%S.ExchangeUser%@%S.ExchangeDomain%`)
Email Address	Type or use substitution variables to define the email address for the account.
Password	(Optional) Type or use substitution variables to define the password that devices use to authenticate with the Microsoft Exchange Server for encoded profiles.
Past Days to Sync	Select the number of days worth of past messages to sync to the device.
Identity Certificate	(Optional) Add the certificate for accounts that support authentication using certificates. • Click Add Request to make devices submit requests to the certificate authority for identity certificates. • Click Add Certificate to upload a certificate that SAP Afaria sends to devices.
Use S/MIME	(Optional; iOS 8 and later) Select whether the account supports S/MIME.
Use Per Message S/MIME	(Use S/MIME selected; iOS 8 and later) Select whether S/MIME encryption is enabled for individual e-mail addresses. If you enable this option, a lock icon appears against the e-mail addresses typed in the e-mail application on the device. The user can selectively encrypt the e-mail message, by enabling or disabling this option for a specific e-mail address.

Setting	Description
Signing Certificate	(Optional) Add the certificate for signing messages. • Click Add Request to make devices submit requests to the certificate authority for identity certificates. • Click Add Certificate to upload a certificate that SAP Afaria sends to devices.
Encryption Certificate	(Optional) Add the certificate for message encryption. • Click Add Request to make devices submit requests to the certificate authority for identity certificates. • Click Add Certificate to upload a certificate that SAP Afaria sends to devices.

2.19.3.1.10 Font Payload

(iOS 8 and later) A font payload adds a font to an iOS device. You can include multiple font payloads, as needed.

Setting	Description
Enabled	Select whether SAP Afaria can send the font payload to devices.
Font Name	(Optional) Type a name for the font.
Font File	Add the file that is uploaded and pushed to the device after the iOS configuration policy is applied. Supported font file formats include TrueType (`.ttf`) and OpenType (`.otf`). Collection font files (`.ttc` and `.otc`) are not supported. The maximum size of each font file cannot exceed 1 MB.

2.19.3.1.11 Generic Payload

The Generic payload includes payloads created in any version of the iPhone Configuration Utility and imported into Afaria.

2.19.3.1.12 Global HTTP Proxy Payload

The Global HTTP Proxy payload defines a Web proxy server for devices. Only one Global HTTP Proxy payload can apply, and only to supervised devices.

Setting	Description
Enabled	Select whether SAP Afaria can send the Global HTTP Proxy payload to devices to define a web proxy server.
Proxy	Select the type of proxy.: • Manual • Automatic If you select Manual, you must configure the server, port, username, and password for the proxy server. If you select Automatic, you must configure the server URL for the proxy auto-config (PAC) file.
Server	(Manual proxy type only) Type or use substitution variables to define the network address of the proxy server.
Port	(Manual proxy type only) Select the port for communication with the proxy server.
User Name	(Manual proxy type only) Type or use substitution variables to define the username that devices use to authenticate with the proxy server.
Password	(Manual proxy type only) Type or use substitution variables to define the password that devices use to authenticate with the proxy server.
Server URL	(Automatic proxy type only) Type or use substitution variables to define the URL for the PAC file.
Allow direct connection if PAC is unreachable	(Automatic proxy type only) Select whether devices can connect directly to SAP Afaria if the proxy auto-config (PAC) file is available to devices.
Allow bypassing proxy to access captive networks	Select whether devices can bypass the proxy to use Wi-Fi hotspots.

2.19.3.1.13 Guided Access Payload

(iOS 8 and later supervised devices) The Guided Access payload locks the device to a single application, on its current version, until the payload is removed. Once locked on an application, the application is not subject to version updates.

Only one of this payload type can be installed at any time.

Prerequisites

The application to lock or to set in the Guided Access mode must already be installed on the device and reported to the server as software inventory. You can install the application using SAP Afaria or another method. If you are using SAP Afaria to install and manage the application, ensure that the managed application has been installed on the device and reported to the server before applying and sending the Guided Access policy to the device.

Perform the following steps to configure a Guided Access MDM payload:

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *iOS*.
2. Enter a policy name.
3. Expand *MDM Payload* and select *Guided Access*.
4. (Optional) Deselect *Enabled* to not push the Guided Access MDM payload to the device. By default, Enabled is selected.
5. Enter the bundle ID of the application.
6. Enable or disable the following settings in the Administrator-enabled settings tab (applicable for iOS 8 and later):
   - Touch
   - Motion
   - Volume Buttons
   - Side Switch
   - Sleep/Wake Button
   - Auto-Lock
   - Speak Selection
   - Mono Audio
7. Enable or disable the following settings in the User-Enabled Settings tab (applicable for iOS 8 and later):
   - VoiceOver
   - Zoom
   - Invert Colors
   - AssistiveTouch
8. Click *Save* to save the payload in the iOS Configuration policy.

Setting	Description
Enabled	Whether SAP Afaria can send the guided access payload to devices.
Bundle ID	The bundle ID of the application.
Administrator-enabled Settings	This field specifies the Administrator-enabled settings for the following: • Touch • Motion • Volume Buttons • Side Switch • Sleep/Wake Button • Auto-Lock • Speak Selection • Mono Audio

Setting	Description
User-Enabled Settings	This field specifies the user-enabled settings for the following: • VoiceOver • Zoom • Invert Colors • AssistiveTouch

Updating an Application on a Guided Access Device [page 146]
Update the locked application on a device that has the Guided Access payload. A Guided Access payload locks the application at a single version and does not allow the application to update by conventional means.

2.19.3.1.13.1 Updating an Application on a Guided Access Device

Update the locked application on a device that has the Guided Access payload. A Guided Access payload locks the application at a single version and does not allow the application to update by conventional means.

Procedure

1. Remove the Guided Access payload from the device.

   For example, unlink the policy from the devices group, by disabling the payload in the configuration policy, and complete an apply policy command on the device.

   Device is restored to normal state, without being locked to an application.
2. Update the application on the device.

   For example, if the application is an Afaria managed enterprise application, then update the application policy with the new version and connect the device for a policy update.
3. Verify that the application is updated by reviewing the software inventory.
4. Deploy the Guided Access payload to the device.

2.19.3.1.14 LDAP Payload

The LDAP payload configures devices to connect to an LDAP server and access directory information. You can specify multiple search bases for each directory, and configure multiple connections.

Setting	Description
Enabled	Whether SAP Afaria can send the LDAP payload to devices

Setting	Description
Description	The description of the LDAP payload
User Name	The user name that devices use to authenticate with the LDAP server
Password	The password that devices use to authenticate with the LDAP server
Host name	The name of the LDAP server
Use SSL	Whether SSL is required
Note	(Optional) The description of the search settings
Scope	The scope of the search settings: • Base searches the immediate node • Onelevel searches the node and its immediate children • Subtree searches the node and all of its children
Search Base	The path to the node to which the search settings apply

2.19.3.1.15 Mail Payload

The Mail payload configures POP or IMAP email accounts on devices.

To add a Microsoft Exchange account, use an Exchange ActiveSync payload.

Setting	Description
Enabled	Whether SAP Afaria can send the Mail payload to devices.
Description	(Optional) The description of the email account. The description is visible in the Mail and Settings applications on devices.
Account Type	The protocol for the email account: • POP • IMAP
Path Prefix	The path prefix for IMAP accounts.
User Name	The user name for the email account.
Email Address	The email address for the account.
Allow Move	Whether users can move messages out of the email account, forward messages from another email account, or reply to message from another email account.

Setting	Description
Incoming Mail: Mail Server	The host name or IP address of the incoming mail server.
Incoming Mail: Port	The port number for connections to the incoming mail server.
Incoming Mail: User Name	The username that devices use to authenticate with the incoming mail server.
Incoming Mail: Authentication Type	The authentication type for the incoming mail server: • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest
Incoming Mail: Password	The password that devices use to authenticate with the incoming mail server.
Incoming Mail: Use SSL	Whether the connections to the incoming mail server use SSL.
Outgoing Mail: Mail Server	The host name or IP address of the outgoing mail server.
Outgoing Mail: Port	The port number for connections to the outgoing mail server.
Outgoing Mail: User Name	The username that devices use to authenticate with the outgoing mail server.
Outgoing Mail: Authentication Type	The authentication type for the outgoing mail server: • None • Password • MD5 Challenge-Response • NTLM • HTTP MD5 Digest
Outgoing Mail: Password	The password that devices use to authenticate with the outgoing mail server.
Outgoing Mail: Same Password	Whether the passwords for the incoming and outgoing mail servers are the same.
Outgoing Mail: Allow Recent Address Syncing	Whether the email account is permitted to sync recent addresses.
Outgoing Mail: Use only in Mail	Whether the email account can be used in the mail application only (that is, not in third-party applications).
Outgoing Mail: Use SSL	Whether connections to the outgoing mail server uses SSL.
Outgoing Mail: Use S/MIME	Whether the email account uses S/MIME.

Setting	Description
Outgoing Mail: Use Per Message S/MIME	(Use S/MIME selected; iOS 8 and later) Whether S/MIME encryption should be enabled for individual e-mail addresses. If you enable this option, a lock icon appears against the e-mail addresses typed in the e-mail application on the device. The user can selectively encrypt the e-mail message, by enabling or disabling this option for a specific e-mail address.
Outgoing Mail: Signing Certificate	The identifier for the signing certificate.
Outgoing Mail: Encryption Certificate	The identifier for the encryption certificate.

2.19.3.1.16 Managed Domains Payload

The Managed Domains payload defines the Web domains that are under the management of an enterprise.

This payload is supported only in iOS 8 and later versions.

Setting	Description
Enabled	Whether SAP Afaria can send the Managed Domains payload to devices.
Email Domain	An e-mail address whose suffix does not match one of the managed e-mail domains specified here, are considered out-of-domain and will be highlighted in the e-mail app on the device.
Web Domain	A document originating from a managed Web domain is treated as managed, and can be opened only using a managed app. You will not be able to open the document, if there are no managed apps pertaining to the document type, on the device. **i Note** To enable this feature, you must disable the following restrictions in the Restrictions payload: • Allow open from managed apps to unmanaged apps • Allow open from unmanaged apps to managed apps

The matching patterns for Managed Domains is summarized:

Format	Description
example.com	Any path under example.com is treated as managed, but not site.example.com/.
foo.example.com	Any path under foo.example.com is treated as managed, but not example.com/ or bar.example.com/.
*.example.com	Any path under foo.example.com or bar.example.com is treated as managed, but not example.com/.

Format	Description
Example.com/sub	example.com/sub and any path under it is treated as managed, but not example.com/.
Foo.example.com/sub	Any path under foo.example.com/sub is treated as managed, but not example.com, example.com/sub, foo.example.com/, or bar.example.com/sub.
*.example.com/sub	Any path under foo.example.com/sub or bar.example.com/sub is treated as managed, but not example.com or foo.example.com/.

If the domain string entry contains a port number, only addresses with that specific port number will be considered as managed. Otherwise, only the standard ports will be considered as managed (port 80 for HTTP and 443 for HTTPS).

2.19.3.1.17 Organization Info Payload

The Organization Info payload defines and sends information about your company to devices.

Setting	Description
Enabled	Whether SAP Afaria can send the Organization Info payload to devices
Name	The name of the organization
Address	The address of the organization
Phone	The phone number of the organization
Email	The email address of the organization
Other	Other information about the organization

2.19.3.1.18 Passcode Payload

The Passcode payload defines passcode requirements, frequency of change, and other characteristics on devices. When the configuration policy loads, the user must enter a passcode that satisfies the policy.

Setting	Description
Enabled	Whether SAP Afaria can send the Passcode payload to devices.
Allow simple value	Whether a simple password is permitted. A simple password contains repeated characters or character sequences.

Setting	Description
Require alphanumeric value	Whether the password requires letters as well as numbers.
Minimum passcode length	The minimum required length of the password.
Minimum number of complex characters	The minimum number of symbols required in the password.
Maximum passcode age	The maximum age of a password. When the password reaches the maximum age, the user must change the password.
Auto lock	The period of time for which devices can be inactive before locking automatically.
Passcode history	The number of unique passwords that must occur before a password can be repeated.
Grace period for device lock	The length of time for which devices can be unlocked without a password after locking.
Maximum number of failed attempts	The number incorrect password attempts before devices must be unlocked by connecting to iTunes.

2.19.3.1.19 Per App VPN Payload

(iOS 8 and later) The per-app VPN payload defines one or more VPN connections that you can assign to specific applications on iOS devices. You can also define a VPN connection for the Safari browser app to use to access specified domains on your network.

From this payload page, you can create one or more per-app VPN profiles which you can then assign to iOS apps using an application policy. When the user launches the app on their device, the device's VPN client establishes a VPN connection to your network using the settings in the profile. The application then uses this VPN connection to connect with servers on your network.

You can also create a profile to list domains on your network you want Safari users to access through VPN. You do not need to assign this profile using an app policy. When the user attempts to browse to a site or page on the domain, the device triggers the VPN client to establish the required VPN connection. Once the VPN connection has been established, requests for other sites including public sites are routed through the VPN connection.

For more information on per-app VPN, see Per-App VPN Considerations [page 184]. For information on assigning apps to a per-app VPN profile, see Adding a Per-App VPN Connection to an Application [page 184].

Setting	Description
Enabled	Whether SAP Afaria can send the per-app VPN payload to devices
Connection Name	The name of the VPN connection

Setting	Description
Safari Domains	Allows you to specify one or more domains behind your corporate firewall you want your users to be able to access using their Safari browser. Apple has defined a number of rules for matching a domain string you enter here to a host. For example, leading and trailing dots are ignored when the string is matched to a host. For more information, refer to the *Configuration Profile Key Reference* available from the iOS Developer Library .
App Enabled	Whether the per-app VPN connection starts automatically when the application starts: • Use on-demand Associated applications can use the VPN connections in accordance with the settings on the On Demand Rules tab. • Start manually Associated applications can use the VPN connections that users manually open. Applications ignore the settings on the On Demand tab. • Start automatically Associated applications start the VPN connections automatically when the applications start. Applications ignore the settings on the On Demand tab.
Connection Settings	The connection settings for the VPN including VPN server, account and connection type. The settings vary by connection type; refer to vendor documentation and your specific implementation. • IPSec (Cisco) • AnyConnect (Cisco) • SSL (Juniper) • SSL (F5) • SSL (Pulse Secure) • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile VPN • SSL (Custom)

Setting	Description
On Demand Rules	For connection types that use certificates for user authentication, these settings determine whether VPN on demand is available for devices. Network rules determine the actions devices take based on the connection type (Wi-Fi, cellular, or Ethernet). The Ethernet connection type does not apply to iOS devices, but it is included as an interface option in the payload: • Connect • Disconnect • Evaluate • Ignore • Allow When using the network rule "Evaluate", connection rules determine when devices use the network connections based on the domain to which devices are trying to connect: • If needed • Never To ensure that all network connections have an appropriate action associated with them, define a default behavior for connections that do not match your other rules. To do this, define a dictionary to be processed last that has an action but no rules. Disconnect on Idle sets the threshold for disconnection. **i Note** Apple's VPN On Demand feature has a set idle timeout of two minutes. Connections to Pulse Secure devices will timeout at two minutes unless the app using the VPN connection has a "keep-alive" feature enabled. With keep-alive enabled, the connection uses the timeout set in the iOS policy. For more information about the On Demand limitation, refer to the Pulse Secure Knowledge Base article #26954 at https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB26954 .
Proxy	The settings for the VPN proxy server. The settings vary based on the proxy type.

2.19.3.1.20 Provisioning File Payload

The Provisioning File payload adds a provisioning file (`.mobileprovision`) to devices, which has a role in managing enterprise-signed applications.

Setting	Description
Enabled	Whether SAP Afaria can send the Provisioning File payload to devices
Provisioning File	The location of the provisioning file

2.19.3.1.21 Restriction Payload

The Restriction payload defines restrictions for user access to certain features, such as device functionality, applications, Siri, operations on iCloud, security, and content ratings.

Setting	Description
Enabled	Whether SAP Afaria can send the Restriction payload to devices.
Enable Supervised Restrictions	Whether the restrictions that apply to devices in supervised mode are enabled.

Device Functionality Tab

Setting	Description
Allow installing apps	Whether the App Store is enabled on the device.
Allow AirDrop	(Supervised mode only) Whether AirDrop is enabled.
Allow removing apps	(Supervised mode only) Whether users can remove applications from devices.
Allow changes to cellular data use for apps	(Supervised mode only) Whether users can change the access that applications have to the cellular network.
Allow use of camera	Whether the camera is enabled on devices
Allow FaceTime	Whether FaceTime is enabled.
Allow screen capture	Whether users can save images of device screens.
Allow automatic sync while roaming	Whether devices can synchronize data automatically while roaming.
Allow Siri	Whether Siri is enabled.

Setting	Description
Allow Siri while device locked	(Allow Siri setting selected) Whether Siri is enabled when devices are locked. This setting is available when Allow Siri setting is selected.
Allow Siri profanity filter	(Supervised mode only; Allow Siri setting selected) Whether the Siri profanity filter is enabled.
Show user-generated content in Siri	(Supervised mode only; Allow Siri setting selected; iOS 8 and later) Whether querying user-generated content from the Web is allowed.
Allow iMessage	(Supervised mode only) Whether iMessage is enabled on devices.
Allow voice dialing	Whether voice dialing is enabled.
Allow bookstore	(Supervised mode only) Whether the iBook Store is enabled.
Allow erotica	(Supervised mode only; Allow bookstore settings are selected) Whether users can download content tagged as erotica in iBook.
Allow Passbook while device locked	Whether Passbook is enabled when devices are locked.
Allow In-App purchase	Whether users can make purchases from applications.
Force user to enter iTunes Store password for all purchases	Whether users must provide credentials for each purchase in iTunes.
Allow multiplayer gaming	Whether multiplayer gaming is enabled.
Allow adding Game Center friends	Whether users can add friends in Game Center.
Allow Configuration Profile Installation	(Supervised mode only) Whether users can install configuration profiles and certificates on devices.
Allow account changes	(Supervised mode only) Whether users can change accounts on devices.
Allow changes to Find My Friends	(Supervised mode only; iOS 8 and later) Whether users can make changes to the Find My Friends application.
Allow pairing with non-Configurator host	(Supervised mode only; iOS 8 and later) Whether users can pair devices with hosts. This setting does not prevent pairing with a supervision host.
Allow open from managed apps to unmanaged apps	(iOS 8 and later) Whether users can open documents from managed accounts and application in accounts and applications that are not managed.

Setting	Description
Allow open from unmanaged apps to managed apps	(iOS 8 and later) Whether users can open documents from unmanaged accounts and application in accounts and applications that are managed.
Allow automatic updates to certificate trust settings	(iOS 8 and later) Whether over-the-air public-key infrastructure updates are enabled on devices.
Show Control Center in lock screen	Whether Control Center is enabled to show up on the lock screen.
Show Notification Center in lock screen	Whether Notifications view in Notification Center is enabled on the lock screen.
Show Today view in lock screen	Whether Today view in Notification Center is enabled on the lock screen.
Allow Erase Content	(Supervised mode only) Whether 'Erase All Content And Settings' option in the Reset screen on the device is enabled.
Allow Spotlight Internet Results	(Supervised mode only) Whether Spotlight is enabled to return the Internet search results.
Allow Enabling Restrictions	(Supervised mode only) Whether 'Enable Restrictions' option in the Restrictions screen on the device is enabled.
Allow Activity Continuation	Whether activity continuation is enabled on the device.
Force Airplay outgoing request pairing password	(iOS 8 and later) If enabled, this forces all devices receiving AirPlay requests from the device to use a pairing password.
iCloud	
Allow backup	Whether devices can back up data to the cloud.
Allow document sync	Whether devices can synchronize documents to the cloud.
Allow Photo Stream	Whether Photo Stream is permitted on devices. Disabling Photo Stream can cause data loss.
Allow shared photo streams	(iOS 8 and later) Whether shared photo streams are enabled on devices.
Allow keychain sync	Whether devices can synchronize keychain data with other devices.
Allow managed app cloud sync	Whether managed application are enabled to use cloud sync.
Security and Privacy	
Allow diagnostic data to be sent to Apple	Whether devices can send diagnostic data to Apple.

Setting	Description
Allow user to accept untrusted TLS certificates	Whether devices prompt users to accept untrusted TLS certificates. If left blank, devices reject certificates without prompting users.
Force encrypted backups	Whether devices are required to encrypt backup data.
Force limited ad tracking	(iOS 8 and later) Whether devices limit ad tracking.
Allow Touch ID to unlock device	Whether devices can be unlocked using touch ID.
Allow apps to enter Guided Access mode	(Supervised mode only) The applications that can initiate Guided Access Mode on devices.

Apps Tab

Setting	Description
Allow use of YouTube	Whether the YouTube application is permitted on devices.
Allow use of iTunes Store	Whether the iTunes application is permitted on devices.
Allow use of Game Center	(Supervised mode only) Whether Game Center is permitted on devices.
Allow use of Safari	Whether Safari is permitted on devices. If Safari is disabled on devices, users cannot open web clips.
Enable autofill	Whether Safari can automatically fill out forms and other data fields.
Force fraud warning	Whether Safari must block fraudulent sites on devices.
Enable JavaScript	Whether Safari permits JavaScript.
Block pop-ups	Whether Safari blocks pop-ups.
Accept cookies	Whether Safari accepts cookies on devices: • Never • From visited sites • Always

Content Tab

Setting	Description
Allow explicit music, podcasts, & iTunes U	Whether devices allow explicit content in music, podcasts, or iTunes.
Ratings region	The region that determines the available ratings for movies, TV shows, and applications.

Setting	Description
Movies	The allowed content ratings for movies on devices.
TV Shows	The allowed content ratings for TV shows on devices.
Apps	The allowed content ratings for applications on devices.

2.19.3.1.22 SCEP Payload

The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

Setting	Description
Enabled	Whether SAP Afaria can send the SCEP payload to devices
CA	The certificate authority that processes the SCEP requests
Common Name	The common name of the certificate authority.
Name	The name of the certificate authority
Subject	The X.500 name, in array form, of the organization ID
Name type	The type of name that devices use for SCEP requests
Name value	The name of the SCEP request
NT Name	The NT name for the SCEP request
Challenge	The pre-shared secret for the SCEP request
Retries	The number of times that the device attempts the SCEP request
Retry Delay	The amount of time that must elapse before the device retries the SCEP request
Key Size	The size of the key in bits: • 1024 • 2048
Use as Digital Signature	Whether devices use the certificates from the SCEP requests as digital signatures
Use for key encipherment	Whether devices use the certificates from the SCEP requests to encipher keys

Setting	Description
Fingerprint	The fingerprint for the SCEP request. You can create a fingerprint from a certificate

2.19.3.1.23 Setting Payload

The Setting payload configures voice and data roaming options on devices.

Setting	Description
Enabled	Whether SAP Afaria can send the Setting payload to devices
Voice Roaming	Whether devices can make and receive calls when roaming
Data Roaming	Whether devices can access data services when roaming
Personal Hotspot	Whether devices can act as personal hotspots for other Wi-Fi devices

2.19.3.1.24 Subscribed Calendar Payload

The Subscribed Calendar payload adds read-only calendar subscriptions to Calendar application on devices.

Setting	Description
Enabled	Whether SAP Afaria can send the Subscribed Calendar payload to devices.
Description	(Optional) The description of the of the calendar.
URL	The address of the calendar server.
Username	The user name that devices use to authenticate with the calendar server.
Password	The password that devices use to authenticate with the calendar server.
Use SSL	Whether to use SSL when connecting to the calendar server.

2.19.3.1.25 VPN Payload

The VPN payload configures VPN connections for devices. There are several supported VPN protocols and methods of authentication. Depending on the configuration settings you select, the options in the editor vary.

Setting	Description
Enabled	Whether SAP Afaria sends the VPN payload to devices.
Connection Name	The user-defined name of the VPN connection.
Server	The name of the VPN server.
Account	The name of the account that devices use to authenticate with the VPN connection.
Connection Type	The settings for VPN connection types. The settings vary by connection type; refer to vendor documentation and your specific implementation. • L2TP • PPTP • IPSec (Cisco) • AnyConnect (Cisco) • SSL (Juniper) • SSL (F5) • SonicWALL Mobile Connect • Aruba VIA • Check Point Mobile VPN • SSL (Custom)

Setting	Description
On Demand Rules	The settings that determine whether VPN on demand is available for devices. Network rules determine the actions devices take based on the connection type (Wi-Fi, cellular, or Ethernet). The Ethernet connection type does not apply to iOS devices, but it is included as an interface option in the payload: • Connect • Disconnect • Evaluate • Ignore • Allow Connection rules determine when devices use the network connections based on the domain to which devices are trying to connect: • If needed • Never Disconnect on Idle sets the threshold for disconnection. **i Note** Apple's VPN On Demand feature has a set idle timeout of two minutes. Connections to Pulse Secure devices will timeout at two minutes unless the app using the VPN connection has a "keep-alive" feature enabled. With keep-alive enabled, the connection uses the timeout set in the iOS policy. For more information about the On Demand limitation, refer to the Pulse Secure Knowledge Base article #26954 at https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB26954 .
Proxy	The settings for the VPN proxy server. The settings vary based on the proxy type.

2.19.3.1.26 Web Clip Payload

The Web Clip payload adds Web clips to the device home screen. Web clips provide fast access to favorite Web pages.

Setting	Description
Enabled	Whether SAP Afaria can send the Web Clip payload to devices.
Label	The name of the web clip.
URL	The URL of the web clip. The URL must start with HTTP or HTTPS.

Setting	Description
Removable	Whether users can remove web clips from devices.
Icon	The icon for the web clip. The icon should be a PNG file of 59 x 60 pixels.
Precomposed Icon	Whether the icon is precomposed. The device does not add additional styles to precomposed icons.
Full Screen	Whether the web clip opens to full screen.

2.19.3.1.27 Web Content Filter Payload

(iOS 8 and later supervised devices) The Web Content Filter payload affects Web viewing to limit sites using permitted lists and black list, or by limiting sites to only a defined list (white list).

Perform the following steps to configure a Web Content Filter MDM payload:

> **i Note**
>
> URLs must begin with `http://` or `https://`. If necessary, separate entries must be made for `http://` and `https://` versions of the same URL.

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *iOS* .
2. Enter a policy name.
3. Expand *MDM Payload* and select *Web Content Filter*.
4. (Optional) Deselect *Enabled* to not push the Web Content Filter MDM payload to the device. By default, Enabled is selected.
5. (Optional) By default, Limit Adult Content is selected from the Allowed Websites list. In the Permitted URLs grid, click *Add* and enter the permitted URL. Click *Save*.
6. (Optional) In the Blacklisted URLs grid, click *Add* and enter the blacklisted URL. Click *Save*.
7. (Optional) If Specific Web Sites Only is selected from the Allowed Websites list, click *Add* in the Specific Websites group box.

   > **i Note**
   >
   > URLs specified in "Specific Web Sites Only" has precedence over the permitted and blacklisted URLs specified in "Limit Adult Content".

8. Enter the URL, bookmark path, and title. Click *Save*.
9. Click *Save* to save the payload in the iOS configuration policy.

Setting	Description
Enabled	Whether SAP Afaria can send the web content filter payload to devices.

Setting	Description
Allowed Websites	Set Allowed Websites to Limit Adult Content (default) or to Specific Web Sites Only. Enter the permitted URLs and blacklisted URLs. If Specific Web Sites Only is selected, enter the following information: • URL – URL of the bookmark. • Bookmark Path – (Optional) Contains the folder into which the bookmark should be added in Safari if Specific Web Sites Only is selected in the Allowed Websites field. For example, `/Interesting Topic Pages/Biology/`. If Specific Web Sites Only is not selected, the bookmark is added to the default bookmarks directory. • Title – title of the bookmark.

2.19.3.1.28 WiFi Payload

The Wi-Fi payload allows you to configure one or more Wi-Fi profiles on your iOS devices. A Wi-Fi profile includes the required settings to allow the device to connect to a specified wireless network.

To ensure the device is able to connect to a specified network, the Wi-Fi profile settings such as security and authentication protocol types must match your Wi-Fi network. Consult with your Wi-Fi admin to ensure you have the required connection settings before applying the payload.

Setting	Description
Enabled	Determines whether the Wi-Fi profile is included with the Wi-Fi payload when the configuration policy is applied to a device
Service Set ID	The Service Set ID (SSID) or network name of the Wi-Fi network as configured on the wireless router.
Priority	The connection priority for the profile if more than one Wi-Fi network is available where "1" is the highest priority. If you do not want to set a priority for the profile, leave the value set to "0".
Auto Join	Allows the device to connect automatically to the Wi-Fi network. If you set the profile to allow the device to automatically join an enterprise Wi-Fi network, do not enable Per-connection Password. The Per-connection Password setting requires the user to enter a password each time the device connects to the network and therefore overrides the Auto Join setting.
Hidden	Indicates that the Wi-Fi router does not broadcast its identity

Setting	Description
Security Type	The security standard or standards required by the Wi-Fi network. Options include both personal and enterprise versions of the WEP, WPA, and WPA2 protocols. Select *Any* to allow the device to use either WEP or WPA/WPA2 to authenticate with the network.
Network Type	The network type. Select *Standard* if the network does not use HotSpot or Passpoint (Hotspot 2.0) technology.
Authentication	Enter a password for the device to use to connect to a personal network. If you do not specify a password, the user is prompted to enter one when connecting to the network.
Protocols	Select the supported authentication methods and provide required settings for the enterprise network. If you do not specify a password, the user is prompted to enter one when connecting to the network. To prompt the user to provide a password every time they connect to the network, enable *Per-connection Password*. **i Note** If you enable this setting, the device cannot automatically join the network even if *Auto Join* is enabled. You can also add an identity certificate for the device or request one from your Certificate Authority. The device uses the identity certificate to authenticate with the network. **i Note** For iOS9, specifying TTLS as the EAP type for any of the enterprise security types provides for the selection of inner authentication protocols.
Trust	Add a trusted certificate and specify the names of trusted server certificates for an enterprise network.
Proxy	Configure Wi-Fi proxy settings for the network.
Passpoint	Configure Passpoint settings such as domain name, roaming consortium organization ID, and mobile country and network codes for an enterprise network. Contact your Mobile Network Operator for the appropriate values.

2.19.3.2 iOS NitroDesk TouchDown Configuration

NitroDesk TouchDown for iOS provides access to Microsoft Exchange e-mail messages, contacts, and calendars using ActiveSync technology. You can either install TouchDown directly on the device or use Afaria to push the TouchDown application to the device.

2.19.3.2.1 Installing NitroDesk TouchDown on an SAP Afaria Managed iOS Device

Install and configure the NitroDesk TouchDown application on an Afaria enrolled iOS device to connect to an enterprise Microsoft Exchange environment.

Procedure

1. Create a configuration policy with TouchDown settings and assign the policy to the device.
2. Create an iOS enterprise application policy to deploy TouchDown application and assign the policy to the device.

   The TouchDown application is sent down to the device during the next apply policy connection. You can also install TouchDown directly on the device.

3. On the device, open Afaria.

   Afaria connects to the Enrollment Server, gets the TouchDown settings, and passes them to the pasteboard on the device.
4. Launch the TouchDown application on the device.

   The TouchDown application configures the user's e-mail account, based on the settings retrieved from the pasteboard.

> **i** Note
>
> To configure TouchDown on the device, the user must launch Afaria before launching TouchDown.

2.19.3.2.2 Installing SAP Afaria and NitroDesk TouchDown Simultaneously on an iOS Device

Install the SAP Afaria client and the NitroDesk TouchDown application on an iOS device, and configure TouchDown to connect to an enterprise Microsoft Exchange environment.

Procedure

1. Create a configuration policy with the TouchDown settings, and link the policy to a group.
2. Create an iOS enterprise application policy and link it to the same group, to deploy TouchDown to the iOS device.

   The TouchDown application is sent down to the device during the next apply policy connection. You can also install TouchDown directly on the device.
3. Create an enrollment policy for the iOS device.
4. Navigate to the Group page and select the group to which the application and configuration policies are linked.

   The device receives the group's linked policies.
5. Install Afaria on the device and enroll the device in management, either directly or using the Self-Service Portal.

   Afaria connects to the Enrollment Server, retrieves the TouchDown settings, and passes them to the pasteboard on the device.

   If you are using an application policy to deploy TouchDown, it is installed on the device after enrollment is complete.
6. On the device, launch TouchDown.

   TouchDown configures the user email account, based on the settings retrieved from the pasteboard.

2.19.3.2.3 Configuring NitroDesk TouchDown Settings for iOS Devices

Define an iOS configuration policy to configure the NitroDesk TouchDown application on the device.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *iOS*.
2. On the *NitroDesk* > *Account Configuration* page, click *Add*.
3. Enter the license key, as purchased from NitroDesk, and define other account configuration details.
4. (Optional) To override Microsoft Exchange ActiveSync settings with more restrictive values, select *NitroDesk* > *EAS Overrides*.
5. (Optional) To define additional security settings for TouchDown, select *NitroDesk* > *Security Settings*.
6. (Optional) To define additional settings for TouchDown, select *NitroDesk* > *Calendar Options*, *NitroDesk* > *Email Options*, or *NitroDesk* > *User Settings*.
7. Save and publish the policy, link it to a group profile, then connect the device.
8. On the device, at the conclusion of the Afaria session, launch TouchDown and complete the configuration steps.

   The device connects to the email server, when the configuration completes.

> **i Note**
>
> Manually invoke the TouchDown configuration wizard on the device, if required, to configure settings other than account configuration details.

2.19.3.2.4 iOS NitroDesk – Account Configuration

Account configuration sets properties for the NitroDesk TouchDown application, when the user launches TouchDown on the device.

- Account License Key – license key for TouchDown, as purchased from NitroDesk.
- Username – user Id for the user Exchange account.
- (Optional) Password – password for the user's Exchange account. If not provided, the user is prompted to enter a value.
- Email Address – email address for the user's Exchange account.
- Domain – network domain where the Exchange server resides.
- Exchange Server – fully qualified domain name for the server that hosts the ActiveSync service.
- Use SSL – whether to use secure protocol for Exchange sessions.

2.19.3.2.5 iOS NitroDesk – Calendar Options

Define calendar properties for the NitroDesk TouchDown application user.

- Show Tasks in Agenda View – shows the calendar tasks in the agenda.

  > **i Note**
  >
  > This feature is not supported when the TouchDown client is configured through Afaria 7 SP4 client. This was tested against TouchDown V3.1.0 available in iOS App Store.

- Default Reminder – adds a default reminder time for all new events.
- Default Privacy – adds a default privacy status for all new events.
- Default Status – adds a default availability status for all new events.
- Zoom – shows the day and week views in larger size and fonts.
- Week Start – indicates the first day of the week to show in the calendar.
- Week End – indicates the last day of the week to show in the calendar.
- Work Day Start – indicates the start time of the workday.
- Work Day End – indicates the end time of the workday.

  > **i Note**
  >
  > 'Work Day Start' and 'Work Day End' features are not supported when the TouchDown client is configured through Afaria 7 SP4 client. This was tested against TouchDown V3.1.0 available in iOS App Store.

2.19.3.2.6 iOS NitroDesk – EAS Overrides

Override the Exchange ActiveSync settings values with values that are more restrictive.

- Suppress Application PIN Prompting –TouchDown does not show the EAS PIN prompt.
- TouchDown Password – specify values for parameters such as minimum password length and password expiration days, if the password option is enabled.
- Maximum Inactivity Time TouchDown Lock (seconds) – the inactivity time interval after which TouchDown locks automatically.
- Require TouchDown Encryption – indicates whether TouchDown must be encrypted on the device.

  > **i Note**
  >
  > This feature is not supported when the TouchDown client is configured through Afaria 7 SP4 client.

- Attachments – enables or disables attachments in the e-mail message.
- Maximum Attachment Size (bytes) – maximum size allowed for the attachment.
- Maximum Calendar Age Filter – maximum number of days to synchronize past events.
- Maximum Email Age Filter – maximum number of days to synchronize past e-mail messages.
- Maximum Email Body Size – maximum size allowed for the e-mail message body.
- Allow HTML Email – allows e-mail messages to be sent in HTML format.

2.19.3.2.7 iOS NitroDesk – Email Options

Define additional e-mail properties for the NitroDesk TouchDown application user.

- Highlight Sender – highlights the name of the sender of an e-mail message.
- Move to Any Folder – moves e-mail messages to any folders, including the ones that are not synchronized. If not selected, the user can move messages only to folders that are synchronized.
- Confirm Deletes – shows a confirmation window when deleting an e-mail message.
- Confirm Move – shows a confirmation window when moving messages to folders.
- After Delete Go – indicates where the control should move to, after deleting a message.

2.19.3.2.8 iOS NitroDesk – Security Settings

Define additional security settings for the NitroDesk TouchDown application on the device.

- Disable Update to Phonebook – do not copy contacts to the device phone book.
- Hide Email Information on Notification Bar – do not show email data on the notification bar.
- Hide Calendar Information on Notification Bar – do not show calendar data, indicating approaching appointments.
- Hide Task Information on Notification Bar – do not show task details on the notification bar.
- Disable Change Signature – disables changing of the signature line.
- Disable Reconfiguration – disables reconfiguration, except through the MDM client.
- Set Suppressions – list of suppression codes that prevent TouchDown from displaying certain options to the user.

  > **i Note**
  >
  > The list of codes should be comma separated, with at least one comma in the string.

- Disable Copy Paste – disables copying data from email messages or pasting data to email messages.
- Set Email Text Signature – sets the signature on the application to be used with plain text e-mail messages.
- Forced SMIME PIN Timeout – sets the time interval for TouchDown to prompt for a PIN, before using an SMIME certificate for signing or decryption.

> **i Note**
>
> 'Disable Reconfiguration' and 'Disable Copy Paste' features are not supported when the TouchDown client is configured through Afaria 7 SP4 client. This was tested against TouchDown V3.1.0 available in iOS App Store.

2.19.3.2.9 iOS NitroDesk – User Settings

Define general properties for the NitroDesk TouchDown client user.

- Enable Push Email – enables push e-mail messaging.

- Email History (days) – defines date range for e-mail messages to synchronize. Default is 3 days.
- Calendar History – defines the date range for appointments to synchronize.
- Email Body Style – defines the fonts, sizes, colors, and styles for composing new messages in HTML mode.
- Notify on Password Failure – sends a notification when password is incorrect.
- Notify on New Email – sends a notification when new messages are received.
- Enable HTML Email – downloads and shows e-mail messages in HTML format.
- Do Not Delete Emails on Server – deleting e-mail messages on the device does not remove them from the server.
- Do Not Mark Read on Server – reading e-mail messages or marking them as read/unread on the device does not mark them as read/unread on the server.
- Sync Updates to Phonebook – updates contact information on the device when detected on the server.
- Always BCC Myself – sends a copy of all outgoing e-mail messages to the configured e-mail address.
- Email View Text Size – text size to use when viewing e-mail messages.
- Email Download Size – download size of the e-mail messages from the server during synchronization.
- Notify on Appointments – shows notification for calendar reminders.

> **i** Note
>
> The features 'Enable HTML Email' and 'Email View Text Size' are not supported when the TouchDown client is configured through Afaria 7 SP4 client. This was tested against TouchDown V3.1.0 available in iOS App Store.

2.19.3.3 Sending Multiple Configuration Policies to Devices

Afaria combines multiple policies into a single delivery payload before sending them to a device. Apple designed iOS management to support multiple instances of some policy types and support only a single instance of other policy types. Apple reserves the right to change requirements without notice.

The following policy types are limited to a single instance on a device:

- Advanced
- AirPlay
- AirPrint
- Exchange ActiveSync
- Guided Access
- Passcode
- Restrictions
- Web Content Filter

2.19.3.4 The SSL Option in Policies

If you plan to use the SSL option in any policy that includes SSL as an option, the device may require a certificate with appropriate credentials. For some policy types, you can select the appropriate certificate from within the policy editor to define credentials. For other policy types, define a separate Credentials policy.

2.19.3.5 Embedded SCEP Requests as Identity Certificates

Wi-Fi and VPN policies include an option to define and embed a SCEP request to obtain an identify certificate when the policy is deployed.

- Embedded SCEP requests always use the certificate authority configured for Afaria operations, as defined on the *Server* > *Configuration* > *Certificate Authority* page.
- All required data elements in the SCEP request are populated with values from the CA profile you select from the enrollment or package server drop-down list.
- To edit the SCEP request subject data, open the Certificate Authority page, navigate to the required CA profile, and update the details.
- For a Wi-Fi with SCEP policy, on a device *General* > *Settings* > *Profiles* page, the policy Contains list includes a SCEP enrollment request item and a Wi-Fi Network item.
- For a VPN with SCEP policy, on a device *General* > *Settings* > *Profiles* page, the policy Contains list includes a SCEP enrollment request item and a VPN Settings item.
- For a Mail with SCEP policy, on a device *General* > *Settings* > *Profiles* page, the policy Contains list includes a SCEP enrollment request item and a Mail Settings item.
- For an Exchange ActiveSync with SCEP policy, on a device *General* > *Settings* > *Profiles* page, the policy Contains list includes a SCEP enrollment request item and an ActiveSync Settings item.

2.19.3.6 Importing iOS Device Configuration Policies

Import Apple iPhone (iOS) configuration policies or exported Afaria policies to make them available as SAP Afaria configuration policies.

Procedure

1. On the *Policy* > *List* page, on the top toolbar, click *Import iOS mobile configuration file*.
2. Click *Browse* to navigate to the source file (`.mobileconfig`).
   The policy name and source file information is automatically updated.
3. You can either import the selected payload into one generic policy or import the selected payload into an individual policy.
4. If you click the *Import selected payload into individual policy*, the Edit button is enabled.

5. Click *Edit*.
6. Click *Import* and select the required policy or a generic policy.
    - If you are importing a valid file, it is uploaded as per the option selected by the Administrator.
    - If you are importing an invalid file, it could be due to the following reasons:
        - Invalid file extension
        - File size is zero
        - XML keys/tags are not as per the IPCU format
        - Administrator is not allowed to proceed with upload (Error message is displayed).
7. Click *OK*.
   The process imports a snapshot of the policy. Once imported, Afaria assumes management of the policy, and subsequent changes to the original target policy file do not impact the policy.

2.19.3.7 iOS Policies from the Apple iPhone Configuration Utility

As an alternative to using the Afaria Administration console to create device configuration policies, you can import policies that you export from the Apple iPhone Configuration Utility. From the utility, export and save policies as individual files (`.mobileconfig`). From the Afaria Administration console Administration Policy page, import policies.

Export Security Requirement

Policies that you export from the Apple iPhone Configuration Utility for importing into Afaria cannot be encrypted or signed. Therefore, select None as the security method when exporting policies from the configuration utility.

2.19.4 Creating an Enrollment Policy for iOS

Create a policy for enrolling iOS devices in Afaria management.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *iOS*.
2. On the Summary page, enter the policy name and a description for the policy.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Self-Service Portal 6.6 and 7 servers.
3. In the Code field, click *Add* and define the following code properties:
   - State – indicate whether devices are prevented from enrolling if the code is disabled at enrollment time. If you do not want to use the code yet, set the state to disabled and enable it later.
   - Portal Only – indicate whether the code is valid only when used with Self-Service Portal enrollment.
   - URL Service – select your preferred URL shortening service, as enabled on the *Server* > *Configuration* > *Enrollment Code* page.
     The Google service produces case-sensitive codes.
   - (Optional) Expiration Date – by default, expiration occurs at the end of the selected day. If you do not specify a date, the code does not expire. Devices are prevented from enrolling if the code is expired at enrollment time.
4. In the Code field, at the end of the line you are editing, click the *Save* icon to generate an enrollment code and a creating date.
5. On the General page, define the policy for enrolling the devices.
   - New device – if your server is configured on the *Server* > *Configuration* > *Server* > *Security* page to not automatically approve new devices, select to override the server configuration and automatically approve enrolling devices. If your server is configured for automatic approval, deselecting the check box does not override the server setting.
   - (Optional) Certificate – select to generate an identity certificate after the initial connection to Afaria server, and use this certificate for future authentications against the server. Identity certificates are supported with the Afaria managed authentication option for the Enrollment and Package Servers. Identity certificates use only the Certificate Authority server assigned to the enrollment server, and require the enrollment server to be configured as the CA proxy. This option is not available in the Afaria Administration console, and is available in `<EnrollmentServer>\program files\AIPS\bin\ServerSCEPtest.exe`. It is set to On, by default, on new installations and upgrades.

     > **i Note**
     >
     > Identity certificates are supported only on 2008 CA servers, for iOS versions 4.2 and above. To support identity certificates, Afaria on the device must be version SP3 or above.
   - Allow activation lock (Supervised only) – Select to allow supervised devices to apply activation lock when the user sets up Find My iPhone. Activation lock prevents unauthorized people from disabling Find My iPhone, erasing the device, and reactivating it. Activation lock can only be turned off by the user using their Apple ID or by an Afaria admin using the *Clear Activation Lock* button on the Device page of the Afaria Administration console. See *Performing Security Actions on Devices* in the *Device Administration* section for more information.
   - Access Control Domain – domain node of the e-mail address, expressed as a fully qualified domain.
   - Access Control Policy – accept (use default policy) or override (use explicit policy) the enterprise default policy for iOS, as defined on the iOS tab on the *Server* > *Configuration* > *Access Control Option* page.

- If automatically creating a name for enrolling devices, select naming options:
  - Optional Prefix – enter a prefix to use for the name. For example "Sales_".

    > **Note**
    >
    > The optional prefix is temporary for Android devices. This prefix is removed from the device ID during the next device connection.

  - Data Column – select a data item to concatenate with the prefix. The list includes predefined columns, the user name variable, and any additional user-defined substitution variables you defined. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
    If you select a data item that is based on a user's response to a user prompt that you add to the enrollment policy, the user's response forms the name, even if it is inaccurate. For example, if you prompt for an e-mail address and the user incorrectly types the address, the name contains the incorrect address, even if the correct address is later stored in inventory.

  Selecting an item that requires user prompts automatically adds the variable to the policy's Variable page.
- (Optional) Consent text – a message that appears during MDM profile installation while enrolling an iOS device. You could customize this field to add agreement or legal verbiage to have the end-user read and accept before proceeding with MDM enrollment.
  Select the *Enable consent text* checkbox to add consent text in any of the specific languages and set it as the default language. You can add consent text in multiple languages.

  > **Note**
  >
  > The language in which the text appears depends on the language configured on the device. If the consent text is not available in the language the device is configured for, the default language is used.

- If you plan to deploy optional enterprise applications, define a shortcut to the portal for the Afaria application list:
  - Title – user-facing title.
  - Description – user-facing description.
  - URL – address for the portal that is configured with the enrollment policy.

6. On the Group page, select any groups to populate when devices enroll.

   A device receives the group's linked policies.

   Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of that group's definition criteria. Upon execution of the Dynamic Group Refresh schedule, if the device does not meet the group criteria, the device is removed from the group.
7. On the Variable page, click *Add* to select any variables to populate during enrollment. Users are prompted on the device during enrollment.

   Define the variable prompts:
   - Variable – from the database, the variable to populate with the user's response.
   - Device Prompt – the text for the user-facing prompt.
   - Entry Mask – select yes or no to indicate whether the entry at the device is masked with asterisk (*) characters as the user types.
8. At the end of the line you are editing, click the *Save* icon to save the variable selection.

Updating Enrollment Policies for MDM-First Enrollment [page 175]

To update an enrollment policy created in a previous version of SAP Afaria to support MDM-first enrollment for iOS 8 or later devices, you must open the policy in SAP Afaria 7 SP4. When you open the enrollment policy, SAP Afaria generates an MDM-first enrollment URL for the policy.

iOS Enrollment Policy Settings [page 175]

2.19.4.1 Updating Enrollment Policies for MDM-First Enrollment

To update an enrollment policy created in a previous version of SAP Afaria to support MDM-first enrollment for iOS 8 or later devices, you must open the policy in SAP Afaria 7 SP4. When you open the enrollment policy, SAP Afaria generates an MDM-first enrollment URL for the policy.

Procedure

1. In the Policy list, select the enrollment policy.
2. Click *Edit*.
3. Click *Save* to update the database with the enrollment policy data.

2.19.4.2 iOS Enrollment Policy Settings

Summary Page [page 175]

General Page [page 176]

Group Settings [page 177]

Variable Settings [page 177]

2.19.4.2.1 Summary Page

Setting	Description
Policy	The name of the enrollment policy.
Note	The description of the policy.

Setting	Description
State	The state of the enrollment policy. • Published • Unpublished
Last Modified	The date when the policy was last modified.
Type	The type of the policy.
OS	The device operating system to which the policy applies.
MDM Enrollment	The link that iOS 8 and higher devices use for MDM enrollment.

2.19.4.2.2 General Page

Setting	Description
Automatically approve	Whether SAP Afaria approves devices automatically after enrollment.
Enable jailbroken devices	Whether the enrollment policy works with jailbroken devices.
Client app use X.509 certificate for authentication and SSL	Whether devices use a certificate for authentication and SSL connections.
Domain	The fully qualified domain name node for the email address.
Use default policy	Whether to use the default policy for access control.
Use explicit policy	Whether to use an explicit policy for access control.

Explicit Policy	The settings for the explicit policy.
	• Always allow
	• Always block
	• Allow when
	  ○ Administered by mobile device management
	  ○ Afaria installed
	  ○ Assigned policy delivered
	  ○ Device hardware encrypted
	  ○ Device uncompromised

Optional Prefix	The prefix for the automatic name of the devices that use this enrollment policy.

Setting	Description
Data Column	The data that SAP Afaria uses when creating automatic names for enrolled devices.
Title	The title for the self-service portal.
Description	The description for the self-service portal.
URL	The URL for the self-service portal.

2.19.4.2.3 Group Settings

Setting	Description
Available Groups	• List of available groups to which you can link the policy
Selected Groups	• List of groups to which the policy is already linked

2.19.4.2.4 Variable Settings

Setting	Description
Variable	• Information that the variable represents
Device Prompt	• Text that the device displays as a user prompt
Entry Mask	• Whether devices mask the value

2.19.5 Volume Purchase Program Licensed Application Policies for iOS Devices

The Volume Purchase Program (VPP) from Apple provides a simple and efficient method to purchase iOS apps from the App Store in bulk, for distribution within your organization. iOS VPP licensed application policies define which Apple VPP store apps can be installed on the devices in your enterprise.

You can create these policies automatically after uploading the service token file (sToken) for the purchased apps, in the Afaria Administration console.

Volume Purchase Program License Management [page 178]

Volume Purchase Program app licensing enables enterprises to assign apps to users, while retaining full control and ownership on the apps. Employees can enroll for the program using their personal

iTunes ID, and app licenses are assigned to the VPP-enrolled users, under the control of the administrator for the enterprise.

Preparing to Distribute VPP Apps [page 178]
In the Afaria Administration console, upload the sToken for the purchased apps, then create iOS VPP application policies to deploy the apps on the device.

Creating a Volume Purchase Program Licensed App Policy [page 179]
Create a policy for an application that has been purchased from the Apple Volume Purchase Program store.

Deploying VPP Apps on the Device [page 182]
To participate in the VPP program, users must register themselves with the program using the Invite to Program command that is sent to the device either during or after enrollment.

Viewing License Details and User Status for VPP App Policies [page 182]
View tenant-specific license details and status information for VPP in the policy inspector panel.

Revoking License for VPP Apps [page 183]
You may need to revoke app licenses from VPP users for security reasons when, for example, a user is leaving the organization, if a device is not compliant or not under MDM control, and so on. You can make revoked licenses available to other users.

Retiring a VPP User [page 183]
Retire VPP users who are leaving the organization and revoke the app licenses allocated to them.

2.19.5.1 Volume Purchase Program License Management

Volume Purchase Program app licensing enables enterprises to assign apps to users, while retaining full control and ownership on the apps. Employees can enroll for the program using their personal iTunes ID, and app licenses are assigned to the VPP-enrolled users, under the control of the administrator for the enterprise.

Volume Purchase Program lets you search for apps, determine the quantity needed, and complete the purchase with a corporate credit card or procurement card. To start buying apps in volume, you must enroll in the program and create a volume purchasing account with Apple. Once you have enrolled, you can purchase apps from the VPP Web site.

2.19.5.2 Preparing to Distribute VPP Apps

In the Afaria Administration console, upload the sToken for the purchased apps, then create iOS VPP application policies to deploy the apps on the device.

Prerequisites

1. 1. Enroll in the VPP program at http://www.apple.com/business/vpp .
2. 2. Once the enrollment is complete, visit https://vpp.itunes.apple.com/store to purchase apps for distribution in the organization.

3. 3. Download the service token (sToken) used for authenticating app assignments.

Context

VPP apps can be deployed only using MDM.

> ⚠ Caution
>
> - When a device is moved from one tenant to another, the VPP users on the device are retired only if the destination tenant has a different sToken. If a tenant is deleted, all VPP users associated with the tenant are retired.
> - sTokens expire after one year. You will need to install a new sToken once a year. When logged in to the VPP store, go to your account summary and download an sToken to link your MDM server with your VPP account.
> - If multiple tenants are using the same sToken, the license details may not be accurate within each tenant. We recommend that you do not share sTokens across tenants.

Procedure

1. On the *Server* > *Configuration* > *iOS Volume Purchase* page, upload the sToken you obtained from the Apple VPP Web site.

   You see a list of all the apps you have purchased that are associated with the specified sToken.
2. To automatically create VPP licensed app policies, select the apps and click *Create Policies (+)* .

   You can also manually create VPP app policies in the *Policy* > *Application* > *iOS VPP Licensed App* page, by providing the app store number and other details.
3. Link the policies with the required groups, for distribution.

2.19.5.3 Creating a Volume Purchase Program Licensed App Policy

Create a policy for an application that has been purchased from the Apple Volume Purchase Program store.

Prerequisites

The device user must have an iTunes account. Complete the procedure to prepare for a VPP store licensed application, which includes recording the App Store number and the country code for the application.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

The Configuration page in the policy is reserved for application onboarding data provisioning and is not part of this procedure. For more details, see Application Onboarding section.

> **i** Note
>
> If you change the service token (sToken) associated with an iOS VPP Licensed Application policy, devices will still display the applications from the original sToken, but users will be unable to install the applications from the original sToken.

Procedure

1. On the Policy list page in the top toolbar, click *New* > *Application* > *iOS VPP Licensed App*.
2. On the Summary page, enter the policy name and note, and indicate whether the policy is published or unpublished.

   Connecting devices receive only published policies.
3. (Optional) Select *Featured* to tag the application as featured.
4. On the General page, enter the app name in the Search by App Name field.
   You see a dynamic list of all apps from the App Store that match the app name you enter.
5. Enter a valid Country Code to use the Search by App Name feature or to retrieve an app using AppStore Number and Bundle ID. The default value for Country Code is 'US'.
6. Select the desired app from the results list.
   The fields AppStore Number, Bundle ID, and Information are automatically populated with information.
7. Alternatively, if you do not want to use the Search by App Name feature, you can type in the AppStore Number or Bundle ID, and click *Update* to retrieve the desired app and its corresponding details.

   > **i** Note
   >
   > Country Code is required in order to retrieve app details using AppStore Number or Bundle ID.

   - AppStore Number – application number from the Apple VPP store, which is located in the URL for the application. You must provide the App Store number or the Bundle ID for the purchased app.
   - Country Code – country code for the Apple VPP store. The default value for Country Code is 'US'.
   - (Optional) Bundle ID – bundle identifier for the application on the Apple VPP store. The bundle identifier populates automatically when you click *Update* after entering a valid App Store number.
   - Deploy using MDM protocol – VPP apps must be deployed using MDM.
     - Prevent data backup – do not allow the iTunes backup utility to back up data for this application from the device to the iTunes backup. This option is automatically selected, but can be edited.
     - Remove with MDM relationship – if the device is removed from MDM control, the application is removed from the device. This option is automatically selected, but can be edited.
   - Per-App VPN – select the VPN profile if the application uses one. You can create VPN profiles using configuration policies.

- Install – choose optional or required.
- B2B App – enable this option if the application is a business-to-business application.
- App Icon – click *Browse* and select the icon for the B2B application. App icon supports JPG, JPEG, and PNG formats with a resolution of 57x57 pixels.
- ArtWork – click *Browse* and select the Artwork image for the application. Artwork supports JPG, JPEG, and PNG formats with a resolution of 512x512 pixels.
- VPP License Distribution:

  User (Apple ID needed) Select to license the app to a specific user. This will require an Apple ID to complete.

  Device Serial Number Select to license the app to a specific device. You apply the policy to push the app to the device in the *Devices* tab.

> **i Note**
>
> If you switch an app from a user to a device and the user has the app on multiple devices, or multiple users have the app on their devices, the app will be removed from all devices when the policy is applied, with the exception of the device specified in the policy.

8. (Optional) On the Categories page, select one or more categories to be associated with the policy.

   Click *Add* to add a new category.
9. (Optional) Select *Yes* or *No* to indicate if the selected category is a featured category.
10. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note.

> **i Note**
>
> The maximum length allowed for the file name is 258 characters, and the maximum image size allowed is 1MB. It is recommended that you use smaller image files of size up to 100KB, to enable easy download and to minimize data traffic.

11. (Optional) On the Description Detail page, enter a description for the application and modify the display name.

    The display name of the application is automatically updated when you upload the application package on the General page.

    For more details on the settings for the various pages like Summary and General, refer to the iOS App Store policy pages.

2.19.5.4 Deploying VPP Apps on the Device

To participate in the VPP program, users must register themselves with the program using the Invite to Program command that is sent to the device either during or after enrollment.

Procedure

1. Enroll the device in Afaria, and associate the device with a group for which VPP is enabled.

   Afaria verifies that the user is a registered VPP user.
2. If it is the intial access for the user, register him or her for VPP with a valid Apple ID.

   VPP service returns an Invitation URL, which associates the registered VPP user with the user's iTunes account.
3. During enrollment, Afaria sends an Invite to Program command to the device.
4. The user clicks the Invite to Program icon and accepts the agreement.

   iTunes informs VPP about the association of the VPP user with the iTunes account. Any licenses allocated to the VPP user are automatically reflected in the associated iTunes account.
5. Apply the policy for the device.

   Based on availability, licenses are allocated for the apps, and the apps appear in the purchase history of the iTunes account.

   > **i** Note
   >
   > One license is allocated to all VPP users using the same iTunes account. For example, using the same iTunes ID on both an iPad and an iPhone, consumes only one license.

2.19.5.5 Viewing License Details and User Status for VPP App Policies

View tenant-specific license details and status information for VPP in the policy inspector panel.

Procedure

1. On the Policy list page, select a VPP licensed app policy.
2. On the left toolbar, click *Show/Hide Inspector*.
3. On the Inspector panel top toolbar, click *VPP License View*.

   The Inspector panel shows details, such as the number of licenses purchased, number of licenses consumed, and the remaining number of licenses. You can also view the device ID, user name, license number, and the license issue date.

4. On the Device list page, select the device to which the VPP policy is applied.
5. On the left toolbar, click *Show/Hide Inspector* to view the VPP user status in the Inspector panel Summary page.

2.19.5.6 Revoking License for VPP Apps

You may need to revoke app licenses from VPP users for security reasons when, for example, a user is leaving the organization, if a device is not compliant or not under MDM control, and so on. You can make revoked licenses available to other users.

Context

Licenses for VPP apps are revoked in Afaria when:

- A policy or a device is unlinked from the group (to learn about Groups, see the *Device Administration Guide* in the Help Portal)
- Remove control is initiated for the device
- Remote wipe is initiated for the device

Procedure

1. Unlink the VPP app policy from the group or remove the device from the VPP group.
2. During the next apply policy connection, Afaria detects that the app should be removed from a particular user, and requests the VPP store to revoke the license.
3. VPP informs iTunes about the license revocation; iTunes in turn informs the user.
4. Afaria sends the remove command to the device, and the apps are removed from the device.

2.19.5.7 Retiring a VPP User

Retire VPP users who are leaving the organization and revoke the app licenses allocated to them.

Procedure

1. When a VPP user leaves the organization, the Afaria Administrator initiates a delete action for the device.
2. Afaria informs VPP to revoke all the licenses allocated to the user.
3. VPP removes all the apps from the purchase history of the iTunes account of the user.

When a device is moved from one tenant to another, the VPP users on the device are retired only if the destination tenant has a different sToken. If a tenant is deleted, all VPP users associated with the tenant are retired.

2.19.6 Per-App VPN Considerations

Per-app VPN profiles help you to secure application data, control access to your corporate network, and control use of your corporate VPN.

You can use per-app VPN profiles to restrict the transmission of application data to a VPN connection. Associating a per-app VPN profile with an application allows the application to establish a VPN connection based on the settings in the Per App VPN payload.

You can also use a per-app VPN profile to allow Safari users on iOS devices to access domains on your network through VPN.

When creating per-app VPN profiles, or moving from VPN connections to per-app VPN connections, consider completing the following tasks:

- Verify with the VPN vendor that the VPN client and server are current and support per-app VPN.
  - Review the vendor's current documentation that describes the per-app VPN feature.
  - Prepare to use certificate-based authentication.
  - Ask the VPN vendor for a sample `.mobileconfig` file for the per-app VPN.
  - Determine the values in the VendorConfig dictionary to add as custom data to the connection settings. They are specific to the vendor's product and your VPN implementation.
- Know how to analyze and validate the traffic on the VPN server.
- Test the connectivity with a VPN profile before attempting to use a per-app VPN profile.
- Remove VPN profiles from devices before deploying the per-app VPN profile.
- Create a credentials payload with the certificate that the per-app VPN profile uses.
- For the application policy, meet the requirements of using a Webkit-based application as the application subject.

Adding a Per-App VPN Connection to an Application [page 184]
You can add a per-app VPN connection to applications on iOS devices.

2.19.6.1 Adding a Per-App VPN Connection to an Application

You can add a per-app VPN connection to applications on iOS devices.

Prerequisites

- Configure a VPN in your enterprise for mobile device connectivity.
- Select a VPN client.
- Identify applications for per-app VPN use.

Procedure

1. In the Afaria Administration console, create a configuration policy for iOS devices and configure the Per App VPN payload.
   a. In the *App Enabled* field, select *Start automatically*.
   b. In the *Connection Type* field, select the VPN vendor.
   c. Configure the user authentication.
   d. Configure additional settings and custom data according to vendor guidance.
   e. If applicable, configure On Demand and Proxy settings for the VPN.
2. Create an application policy for iOS devices to deploy the VPN client:
   a. On the *General* page of the application policy, select *Deploy using MDM protocol*.
   b. In the *Install* list, select *Required*.
3. Create an application policy for iOS devices to deploy the application that uses the per-app VPN:
   a. On the *General* page of the application policy, select *Deploy using MDM protocol*.
   b. In the *Per-App VPN* field, select the Per App VPN payload from the configuration policy.
4. Link all of the policies to a group.
5. Enroll a device in SAP Afaria management and add the device as a member of the group with the linked policies. You can define the group in the enrollment policy or link the device to the group after enrollment.
6. On the device, open the SAP Afaria client and connect to SAP Afaria at least once.
7. On the device, open the VPN client to enable device settings, accept terms of use, etc.
8. Launch the application that uses the per-app VPN. Observe the VPN indicator on the device to verify application activity.
   If the VPN indicator shows activity, the application has been successfully associated with the VPN connection. However, if you do not get the communication results you expect, use VPN diagnostics to troubleshoot the network communications.

Related Information

Creating an Application Policy for iOS App Store Apps [page 112]
Creating a Configuration Policy for iOS [page 130]

2.20 Windows Policies

Creating a Configuration Policy for Windows [page 186]
Create a policy for scheduling device connections, collecting inventory, and configuring device settings for Windows computers.

Creating an Enrollment Policy for Windows Vista, 2008, or 7 [page 188]
Create a policy and Afaria client for enrolling Windows Vista, Windows 2008, or Windows 7 devices. Use this task also for Windows 8 and 8.1 devices.

2.20.1 Creating a Configuration Policy for Windows

Create a policy for scheduling device connections, collecting inventory, and configuring device settings for Windows computers.

Context

The policy includes multiple pages, such as Summary and Schedule. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *Windows*.
2. On the Summary page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.
3. Enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished. Connecting devices receive only published policies.
   - Priority – set a user-defined value used to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
   - Authentication – require the server to verify the connecting user's identity against your authentication authority before allowing the channel to run. This option is available only if you have authentication enabled on the server, as defined on the *Server* > *Configuration* > *Security* page.
   - Inventory – select the inventory type to collect. You can view inventory information on the Device page Device Inspector.
     - None – no inventory collection.
     - Hardware – scan collects data relating to the device physical components, such as processors and memory cards.
     - Hardware and Software – scan collects hardware data and data for installed software.
4. On the Schedule page, you can select, edit, create, or delete schedules to define a schedule basic type and time properties.

   In the selected schedule click *Retries* to define the number of times the server should retry the scheduled task, if the task fails. The retry interval is the time to wait before the next retry attempt. Retry attempts cease if the scheduled task succeeds.

   Enter the following details to create a new schedule:
   - Schedule – a meaningful name for the schedule.
   - Note – description of the scheduled task.
   - Type – type of schedule:
     - For “Daily” or “Weekly” type, select the days of the week.
     - For “Monthly” type, select the months of the year.

- For “Once” type, select Immediately for the earliest available day at specified time, or select a specified date/time schedule.

- Setting – change the start date, time, repeat, or retry preferences by changing the settings for each individually listed schedule.
  - Rate – enter the start time and days for the schedule and indicate whether to run the schedule at start-up if the server was not running at the defined start time. The options displayed here are based on the schedule type selected.
  - Range – indicate whether to run the schedule always or enter the starting and the ending date range for the schedule.
  - Repeat – enter the parameters for repeating the scheduled task. You can repeat until a certain time or day, or for a duration.
  - Randomize – enter the parameters for randomizing the start time for the scheduled task.

2.20.1.1 Summary Page

Setting	Description
Policy	Type a name for the policy.
Note	Type a description for the policy.
State	View the status of the policy.
Last Modified	View when the policy was last modified.
Type	View the type of the policy.
OS	View the operating system to which the policy applies.
Priority	Select the priority of the policy.
Authentication	Select whether the policy requires user authentication.
Inventory	Select whether SAP Afaria collects inventory data about devices and what kind of data it collects.

2.20.1.2 Schedule Page

Setting	Description
Selected Schedule	View the schedule associated with the policy.
Schedule Table	Add or edit existing schedules.

2.20.2 Creating an Enrollment Policy for Windows Vista, 2008, or 7

Create a policy and Afaria client for enrolling Windows Vista, Windows 2008, or Windows 7 devices. Use this task also for Windows 8 and 8.1 devices.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Windows Vista, Windows 2008, or Windows 7*.
2. On the Summary page, enter the policy name and a description for the policy.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.
3. On the General page, define the policy for enrolling the devices.
   - Server Address – Afaria server address or relay server address. The value, which you can change here, is initially populated by the Address for Client Communication value, as defined on the *Server* > *Configuration* > *Device Communication* page.
   - Name – type a user-friendly name for the server.
   - (Optional) Channel – default channel or channel set for the devices to request when they connect to the Afaria server. For devices to appear on the list, the channels must exist and must be published. “None” may be an appropriate choice if you are using API instructions to control connections.
   - (Optional) Optional Prefix – if automatically creating a client name for enrolling devices, enter a prefix to use for automatically naming the client. For example "Sales_".
   - (Optional) Data Column – if automatically creating a client name for enrolling devices, select a data item to concatenate with the prefix for automatically naming the client. The list includes predefined columns, the user name variable, and any additional user-defined substitution variables you defined. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named clients.
4. On the Group page, select any groups to populate when devices enroll.

   A device receives the group's linked policies.

   Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of that group’s definition criteria. Upon execution of the Dynamic Group Refresh schedule, if the device does not meet the group criteria, the device is removed from the group.

5. On the Advanced page, define the following device properties.
    - Device Connect –define a setting to have the device initiate a connection to the Afaria server without requiring user interaction. Windows devices request the server's listing channel. Windows Mobile Professional and Standard devices request the channel previously selected or the server's listings channel if there was no previous selection.
      Some delay may occur before initiating the connection if connectivity is not available or if device resources are dedicated to another task that may not be related to processing.
        - Immediately – initiate a connection to the server soon after the device installation is complete.
        - Time Picker – specify a time for the device to initiate a connection to the server.
    - Device Install – select the preferences for the visibility of the Device Install interface and device reboot prompt.
    - Device Option – select the optional components for the device.
        - Desktop shortcut – create a shortcut to the Afaria server on the device desktop.
        - Start menu shortcut – create a shortcut to the Afaria server on the device Start menu.
        - System tray icon during session – create a system tray icon while the session is in progress.
        - Outbound listener and firewall – enable outbound listener and firewall settings on the device so that the Afaria server can initiate connection with the device.
    - Device Binary Path – define a complete path on the planned client computer to serve as the default installation path during the installation at the client. The installer can change the path to a non-default value at installation time.
    - Device Data Path – define a complete path on the planned computer to serve as the default path for storing Afaria data during device operations. The installer can change the path to a non-default value at installation time.
    - User Context – define the user context in which the scheduled sessions should run.
        - None – the device runs only with the service settings
        - From installation account – use the same user name and domain credentials as the logged on user that is installing the device
        - From user – the user that installs the device must supply a user name and domain for the user context. The user name and domain do not need to belong to the installing user.
        - Specifically as – define values that become the user context for all devices installed with the current device package. Enter a user name and domain for the context.
6. To download the application, return to the Summary page and click *Download*.

2.21 Windows CE Policies

Creating an Enrollment Policy for Windows CE [page 190]

Create a policy and installable Afaria application for enrolling Microsoft Windows CE devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

2.21.1 Creating an Enrollment Policy for Windows CE

Create a policy and installable Afaria application for enrolling Microsoft Windows CE devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the toolbar, click *New* > *Enrollment* > *Windows CE*.
2. On the Summary page, enter the policy name and a description for the policy.

   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.
3. On the General page, define the policy for enrolling the devices.
   - Server Address – Afaria server address or relay server address. The value, which you can change here, is initially populated by the Address for Client Communication value, as defined on the *Server* > *Configuration* > *Device Communication* page.
   - (Optional) Optional Network – type a connection name that you want devices to use to connect to the Afaria server when an active connection is not already available on the device. The client device must have a connection defined with the same name. Some values are valid only for iAnywhere Mobile Office client devices.
   - (Optional) Channel – default channel or channel set for the devices to request when they connect to the Afaria server. For devices to appear on the list, the channels must exist and must be published.
   - If automatically creating a name for enrolling devices, select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
   - Define the user properties.
     - User Name – prompt users to enter a network user name. The prompt occurs during or after the installation process, depending on device type. The information is used for user authentication when required for a session.
     - Configuration – allow users to edit the Afaria configuration settings on their hand-held devices. Configuration settings include the Afaria server address and port, and the default channel to run.
4. On the Group page, you can assign the device to one or more static groups if you have already used the Afaria Administration console to create any group. Only static groups are eligible for assignments in this manner. Select one or more groups and click -> to move the groups from Available Groups box to Selected Groups box.

5. On the Advanced page, define the configuration policies.
    - Configuration Policy – select the Configuration Policy that matches the Afaria device type you are creating. You can select a single policy or you can choose "none". The policy you select executes during the device installation, thereby allowing you to establish device settings prior to the device's first connection to the Afaria server. Choosing "none" indicates that you are not including a policy in the device install.
    - Device Connect – select the preferences to indicate how the device connects to the Afaria server after device installation.
        - After ActiveSync synchronization – connect to Afaria when ActiveSync is synchronizing.
        - Require no user information – define a setting to have the device initiate a connection to the Afaria server without requiring user interaction.
        - Hours between connections – indicate the number of hours that should elapse after an Afaria session completes before the ActiveSync relationship invokes another Afaria session.
        - After device installation – define options for connecting the device to the Afaria server after installation.
          Some delay may occur before initiating the connection if connectivity is not available or if device resources are dedicated to another task that may not be related to Afaria processing.
            - Immediately – initiate a connection to the server soon after the device installation is complete.
            - Time Picker – specify a time for the device to initiate a connection to the server.
    - Device Reboot – prompt for device reboot, after the installation is complete.
        - Required – prompt the user to notify that a reboot is required. Allow only for the user to accept; do not allow the user to cancel. The user can save data and close applications before accepting the reboot action.
        - Optional – prompt the user to notify that a reboot is required. Allow the user to accept or cancel. The user can save data and close applications before accepting the reboot action.
        - None – do not prompt the user; do not execute a reboot action. The installation becomes complete the next time users reboot their devices.
6. To download the application, return to the Summary page and click *Download*.

Enrollment Policy Settings [page 191]

2.21.1.1 Enrollment Policy Settings

Summary Page [page 192]
The summary page includes information about the policy.

General Page [page 192]
The general page includes connection information for devices that use the policy.

Group Page [page 193]
The group page lists the groups that are both available and assigned to the policy.

Advanced Page [page 193]
The advanced page includes device connection settings.

Certificate Page [page 193]
The certificate page includes settings to define the SSL certificate.

2.21.1.1.1 Summary Page

The summary page includes information about the policy.

Setting	Description
Policy	Type a name for the policy.
Note	Type a description for the policy.
State	View the status of the policy.
Last Modified	View when the policy was last modified.
Type	View the type of the policy.
OS	View the operating system to which the policy applies.
Processor type	Select the processor to which the policy applies. Click *Download CAB* to download the installation files.

2.21.1.1.2 General Page

The general page includes connection information for devices that use the policy.

Setting	Description
Address	Type the address of the SAP Afaria server or relay server. By default, the field shows the address that you configure for device communication in the server configuration.
Optional Network	(Optional) Type the name of the connection that devices use to connect to the SAP Afaria server or relay server. You must define a connection with the same name on the devices.
Channel	(Optional) Select the channel that devices request when connecting to the SAP Afaria server.
Optional Prefix	(Optional) Type a prefix that SAP Afaria adds to the data column to form the names of devices.
Data Column	Select the data that SAP Afaria uses as names for devices.
User Name	Select whether SAP Afaria prompts users for their user names during enrollment.

Setting	Description
Connection	Select whether users can edit configuration settings on devices. Configuration settings include server address, port, and channel.

2.21.1.1.3 Group Page

The group page lists the groups that are both available and assigned to the policy.

Setting	Description
Available Groups	View and select the groups to which you can assign the policy.
Selected Groups	View and remove the groups to which the policy is assigned.

2.21.1.1.4 Advanced Page

The advanced page includes device connection settings.

Setting	Description
Device Connect	Select when the device connects.

2.21.1.1.5 Certificate Page

The certificate page includes settings to define the SSL certificate.

Setting	Description
Path and File Name	Type the path and file name of the SSL certificate.
Password	Type the password that is associated with the SSL certificate.

2.22 Windows Mobile Policies

Creating an Enrollment Policy for Windows Mobile Professional [page 194]
Create a policy and Afaria application for enrolling Windows Mobile Professional devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Creating an Enrollment Policy for Windows Mobile Standard [page 196]
Create a policy and Afaria application for enrolling Microsoft Windows Mobile Standard devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Creating a Configuration Policy for Windows Mobile [page 198]
For Windows Mobile Professional or Windows Mobile Standard devices, create a policy for scheduling device connections, collecting inventory, and configuring device settings.

2.22.1 Creating an Enrollment Policy for Windows Mobile Professional

Create a policy and Afaria application for enrolling Windows Mobile Professional devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Windows Mobile Professional*.
2. On the Summary page, enter policy name and a description for the policy.
   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.
3. In the Code field, click *Add* and define the code properties.
   - State – indicate whether devices are prevented from enrolling if the code is disabled at enrollment time. If you do not want to use the code yet, you can set the state to disabled and enable it later.
   - Portal Only – not applicable.
   - URL Service – select your preferred URL shortening service, as enabled on the *Server* > *Configuration* > *Enrollment Code* page.
     The Google service produces case-sensitive codes.
   - (Optional) Expiration Date – by default, expiration occurs at the end of the selected day. If you do not specify a date, the code does not expire. Devices are prevented from enrolling if the code is expired at enrollment time.

4. In the Code field, at the end of the line you are editing, click the *Save* icon to generate an enrollment code and a creating date.
5. Select an Afaria installation kit type, based on your device or enterprise requirements for installing signed or unsigned applications.
    - Signed without seed data – signed by a trusted public certificate authority. Seed data, which includes the settings from the enrollment policy, is distributed as a separate file. When the seed file is stored on the device with the application, the application can apply the seed data settings, such as the Afaria server address.
    - Unsigned with seed data – unsigned and includes seed data, which includes the settings from the enrollment policy, such as the Afaria server address.
6. On the General page, define the policy for enrolling the devices.
    - Server Address – Afaria server address or relay server address. The value, which you can change here, is initially populated by the Address for Client Communication value, as defined on the *Server* > *Configuration* > *Device Communication* page.
    - (Optional) Optional Network – type a specific connection name that you want the device to use to connect to the Afaria server when an active connection is not already available on the device. The device must have a connection defined with the same name. Some values are valid only for iAnywhere Mobile Office devices.
    - (Optional) Channel – default channel or channel set for the devices to request when they connect to the Afaria server. For devices to appear on the list, the channels must exist and must be published. “None” may be an appropriate choice if you are using API instructions to control connections.
    - If automatically creating a name for enrolling devices, select naming options:
        - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
        - (Optional) Data Column – select a data item to concatenate with the prefix. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
    - Define the user properties.
        - User Name – select to prompt users to enter a network user name. The prompt occurs during or after the installation process, depending on device type. The information is used for user authentication when required for a session.
        - Configuration – select to allow users to edit configuration settings on their hand-held devices. Configuration settings include the Afaria server address and port, and the default channel to request.
7. On the Group page, select any groups to populate when devices enroll.

    A device receives the group's linked policies.

    Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of that group’s definition criteria. Upon execution of the Dynamic Group Refresh schedule, if the device does not meet the group criteria, the device is removed from the group.
8. On the Advanced page, define the following device properties:
    - Configuration Policy – select the Configuration Policy that matches the device type you are creating. You can select a single policy or you can choose "none". The policy you select runs during the device installation, thereby allowing you to establish device settings prior to the device's first connection to the Afaria server. Choosing "none" indicates that you are not including a policy in the device install.
    - Device Connect – indicate how the device connects to the Afaria server after device installation.
        - After ActiveSync synchronization – connect when ActiveSync is synchronizing.

- Require no user information – define a setting to have the device initiate a connection without requiring user interaction.
- Hours between connections – indicate the number of hours that should elapse after an Afaria session completes before the ActiveSync relationship invokes another session.
- After device installation – define options for connecting the device to the Afaria server after installation
  Some delay may occur before initiating the connection if connectivity is not available or if device resources are dedicated to another task that may not be related to Afaria processing.
  - Immediately – initiate a connection to the server soon after the device installation is complete.
  - Time Picker – specify a time for the device to initiate a connection to the server.

- Device Reboot – prompt for device reboot, after the installation completes.
  - Required – prompt the user that a reboot is required. Allow only for the user to accept; do not allow the user to cancel. The user can save data and close applications before accepting the reboot action.
  - Optional – prompt the user that a reboot is required. Allow the user to accept or cancel. The user can save data and close applications before accepting the reboot action.
  - None – do not prompt the user; do not execute a reboot action. The installation completes the next time the user reboots his device.

9. To download the application, return to the Summary page and click *Download*.

2.22.2 Creating an Enrollment Policy for Windows Mobile Standard

Create a policy and Afaria application for enrolling Microsoft Windows Mobile Standard devices. After creating or editing the policy, download and distribute the application when you want users to install it for enrollment.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Windows Mobile Standard*.
2. On the Summary page, enter the policy name and a description for the policy.
   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.
3. In the Code field, click *Add*, and define the code properties:
   - State – indicate whether devices are prevented from enrolling if the code is disabled at enrollment time. If you do not want to use the code yet, set the state to disabled and enable it later.

- Portal Only – not applicable.
- URL Service – select your preferred URL shortening service, as enabled on the *Server* > *Configuration* > *Enrollment Code* page.
  The Google service produces case-sensitive codes.
- (Optional) Expiration Date – by default, expiration occurs at the end of the selected day. If you do not specify a date, the code does not expire. Devices are prevented from enrolling if the code is expired at enrollment time.

4. In the Code field, at the end of the line you are editing, click the *Save* icon to generate an enrollment code and a creating date.
5. Select an Afaria installation kit type, based on your device or enterprise requirements for installing signed or unsigned applications.
   - Signed without seed data – signed by a trusted public certificate authority. Seed data, which includes the settings from the enrollment policy, is distributed as a separate file. When the seed file is stored on the device with the application, the application can apply the seed data settings, such as the Afaria server address.
   - Unsigned with seed data – unsigned and includes seed data, which includes the settings from the enrollment policy, such as the Afaria server address.
6. On the General page, define the policy for enrolling the devices.
   - Server Address – Afaria server address or relay server address. The value, which you can change here, is initially populated by the Address for Client Communication value, as defined on the *Server* > *Configuration* > *Device Communication* page.
   - (Optional) Optional Network – type a connection name that you want devices to use to connect to the Afaria server when an active connection is not available on the device. The device must have a connection defined with the same name. Some values are valid only for iAnywhere Mobile Office devices.
   - (Optional) Channel – default channel or channel set for the devices to request when they connect to the Afaria server. It must be created and published to appear on the list. “None” may be an appropriate choice if you are using API instructions to control connections.
   - If automatically creating a name for enrolling devices, select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. Selecting something meaningful to your organization can help facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
   - Define the user properties.
     - User Name – prompt users to enter a network user name. The prompt occurs during or after the installation process, depending on device type. The information is used for user authentication when required for a session.
     - Configuration – allow users to edit configuration settings on their hand-held devices. Configuration settings include the Afaria server address and port and the default channel to run.
7. On the Group page, you can assign the device to one or more static groups if you have already used the Afaria Administration console to create any group. Only static groups are eligible for assignments in this manner. Select one or more client groups and click -> to move client groups from Available Groups box to Selected Groups box.
8. On the Advanced page, define the configuration policies.
   - Configuration Policy – select the Configuration Policy that matches the device type you are creating. You can select a single policy or you can choose "none". The policy you select runs during the device

installation, thereby allowing you to establish device settings prior to the device's first connection to the Afaria server. Choosing "none" indicates that you are not including a policy in the device install.

- Device Connect – indicate how the device connects to the Afaria server after device installation.
  - After ActiveSync synchronization – connect to Afaria when ActiveSync is synchronizing.
  - Require no user information – define a setting to have the device initiate a connection to the Afaria server without requiring user interaction.
  - Hours between connections – indicate the number of hours that should elapse after an Afaria session completes before the ActiveSync relationship invokes another session.
  - After device installation – define options for connecting the device to the Afaria server after installation.
    Some delay may occur before initiating the connection if connectivity is not available or if device resources are dedicated to another task that may not be related to Afaria processing.
    - Immediately – initiate a connection to the server as soon after the device installation is complete as possible.
    - Time Picker – specify a time for the device to initiate a connection to the server.
- Device Reboot – prompt for device reboot, after the installation completes.
  - Required – prompt the user that a reboot is required. Allow only for the user to accept; do not allow the user to cancel. The user can save data and close applications before accepting the reboot action.
  - Optional – prompt the user that a reboot is required. Allow the user to accept or cancel. The user can save data and close applications before accepting the reboot action.
  - None – do not prompt the user; do not execute a reboot action. The installation completes the next time the user reboots his device.

9. To download the application, return to the Summary page and click *Download*.

2.22.3 Creating a Configuration Policy for Windows Mobile

For Windows Mobile Professional or Windows Mobile Standard devices, create a policy for scheduling device connections, collecting inventory, and configuring device settings.

Context

To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the *Policy* page, on the top toolbar, click *New* > *Configuration* > *Windows Mobile Professional* or *New* > *Configuration* > *Windows Mobile Standard*.
2. On the *Summary* page, enter the policy name.
   You can specify duplicate policy names across tenants and within a tenant for all policy types. Changes made in Afaria to support duplicate policy names are compatible with Afaria 6.6 and 7 servers.

3. Enter or select the remaining properties.
    - Note – add a description for the policy.
    - State – indicate published or unpublished. Connecting devices receive only published policies.
    - Priority – set a user-defined value Afaria uses to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
    - Authentication – require the server to verify the connecting user's identity against your authentication authority before allowing the channel to run. This option is available only if you have authentication enabled on the server, as defined on the *Server* > *Configuration* > *Security* page.
    - Inventory – select the inventory type to collect. You can view inventory information on the *Device* page's *Device Inspector*.
        - None – no inventory collection.
        - Hardware only – scan collects data relating to the device's physical components, such as processors and memory cards.
        - Hardware and Software – scan collects hardware data and data for installed software.
4. On the *Schedule* page, you can select, edit, or create schedules for tasks performed by the server on a regular basis.

    Enter the following details to create a new schedule:
    - Schedule – a meaningful name for the schedule.
    - Note – description of the scheduled task.
    - Type – type of schedule: Daily, Weekly, Monthly, or Once.
    - Setting – the start date, time, repeat preferences, and other properties for the schedule.
        - Rate – enter the start time and days for the schedule and indicate whether to run the schedule at start-up if the server was not running at the defined start time. The options displayed here are based on the schedule type selected.
        - Range – indicate whether to run the schedule always or enter the starting and the ending date range for the schedule.
        - Repeat – enter the parameters for repeating the scheduled task. You can repeat until a certain time or day or for a certain duration.
        - Randomize – enter the parameters for randomizing the start time for the scheduled task.
5. (Optional) Configure additional pages according to your requirements.

    Connection Properties [page 200]
    Specify connection properties such as dialing methods, dialing locations, network details, DNS and IP settings, roaming controls, and port controls.

    Device Properties [page 205]
    Specify device properties such as owner details, device sounds, and executable file properties.

    Format Properties [page 208]
    Specify format properties for language, numbers, currency, time, and date.

    Device Configuration CSP Properties [page 209]
    Specify device configuration properties such as e-mail settings, synchronization settings and other device configuration details.

    Network CSP Properties [page 211]
    Specify network properties such as GPRS details, proxy details, VPN details, and WiFi properties for the device.

2.22.3.1 Connection Properties

Specify connection properties such as dialing methods, dialing locations, network details, DNS and IP settings, roaming controls, and port controls.

General Page [page 200]
Specify connection options such as dialing methods, local and remote phone numbers for dialup, and area codes.

Dialing Locations Page [page 201]
Specify dialing options and set default location.

DNS/IP Page [page 202]
Configure network adapter, DNS, IP, or WINS settings.

Network Property Page [page 202]
Set properties for network connections.

Roaming Control Property Page [page 202]
Sets properties for roaming controls.

Port Control Property Page [page 203]
Sets properties for port controls and data transfer.

2.22.3.1.1 General Page

Specify connection options such as dialing methods, local and remote phone numbers for dialup, and area codes.

You can also specify dialing patterns and TCP/IP settings used for RAS connections. You can set the following options on the Connection property page:

- Name – specifies a name for the RAS connection profile.
- Delete this RAS entry on the Client – permanently removes this RAS connection profile on the device. When you select this option, the RAS connection settings options become unavailable. Selecting this option disables all the property settings on the Connection page.
- Type – specifies modem for the RAS connection. You can also enter the modem name exactly as it appears on the device.
- Username – specifies the account user name for the device.
- Password – specifies the account password for the device.
- Domain – specifies the domain to which the client device belongs.
- Country code – if devices must dial a country code to complete a connection, this option specifies the country code in the area provided.
- Area code – specifies the correct area code in the area provided if devices must dial a 10-digit number.
- Phone number – specifies the phone number devices must dial to connect.
- Baud rate – specifies the baud rate (in bits per second) for the RAS connection.
- Data bits – specifies the number of data bits to use for each character that is transmitted and received in this RAS connection.
- Parity – specifies the level of error checking for this RAS connection.
- Stop bits – determines the number of stop bits to tell the system a packet of information has been sent.

- Flow Control – specifies whether to use hardware or software to control the flow of data between the modem and the computer.
- Use terminal before connecting – determines whether the user can type commands directly to the modem before dialing.
- Use terminal after connecting – determines whether the user can type commands directly to the modem after dialing.
- Enter dialing commands manually – allows the device user to enter dialing commands manually on the device.
- Cancel call if time-out occurs – ends the call automatically if it does not connect after the amount of time you specify.
- Wait for dial tone before dialing – specifies whether the device should wait for a dial tone.
- Wait for credit card tone (seconds) – specifies the number of seconds the device should wait for a tone before entering a credit card or calling card number.
- Extra dial-string modem commands – this area lets you enter any extra dial-string modem commands.

> **i Note**
>
> The options in this area are unavailable unless you specify a RAS connection profile.

- Use server-assigned name server addresses – specifies whether the device should use server-assigned name server addresses. If you select No, you must manually enter the DNS or WINS addresses in the areas provided. If you select Yes, the DHCP server will set the addresses.
- Use SLIP – specifies whether to use SLIP as the primary TCP/IP protocol for the connection.
- Compression – specifies a compression type for the connection.

2.22.3.1.2 Dialing Locations Page

Specify dialing options and set default location.

You can set the following options on the Dialing locations page:

- When dialing from – lets you create a profile for a specific location. You can choose a location from the list, or create your own locations, such as “Local” or “Remote.” When you select this option, all the remaining options become available.
- Set as default dialing location – sets the location you specify as the default on the device.
- Delete this dialing location on the Client – permanently removes the dialing location profile from the device. When you delete a dialing location profile, the remaining options become unavailable.
- Local area code – specifies the correct area code in the area provided, if devices must dial a 10-digit number.
- Local country code – specifies the country code in the area provided, if devices must dial a country code to complete a connection.
- Dialing method – specifies the correct dialing mode, Tone or Pulse.
- Disable call waiting – you can disable call waiting on the device. If you disable call waiting, select or enter the string that disables this feature on the device.
- Local dial pattern – specifies a dialing pattern for local calls. For instance, if devices must dial 9 and then a 10-digit number, the local dial pattern would be 9,FG.
- Long distance dial pattern – specifies a dialing pattern for long-distance calls. For instance, if devices can dial a long distance number directly, the pattern would be 1FG.

- International dial pattern – specifies a dialing pattern for international calls. For instance, if devices must dial 9 and then the number, the pattern would be 9,011, EFG.

2.22.3.1.3 DNS/IP Page

Configure network adapter, DNS, IP, or WINS settings.

The IP addresses used on this page are for the network interface on the device. For dial-up settings, use the Connection page.

- Network Adapter – select the network adapter for your device from the list or type in a custom adapter name. The custom name must match either that adapter type's display name (example: Socket LP-E Driver) or the exact adapter name in the registry (example: SOCKETLPE1). This option is available only for Windows Mobile Professional.
- Obtain IP information – if you select to obtain IP information automatically, the device will use DHCP to obtain the IP address. If you select to obtain IP information manually, the Subnet Mask and Gateway options become available. You can select either or both of these options to help the TCP/IP layer make a decision about when to forward requests to computers outside the local network.

  > **i** Note
  >
  > Setting a manual IP does not set the specific IP address on a device. Set up separate policies for each device needing a manual IP address assigned. If the IP information is obtained automatically, the primary and secondary DNS and WINS settings are applied as alternate DNS/INS addresses after those obtained through DHCP.

- Primary/Secondary DNS – use this option to resolve any host names into IP addresses within the network.
- Primary/Secondary WINS – use this option to resolve NetBIOS names to IP addresses within the network.

2.22.3.1.4 Network Property Page

Set properties for network connections.

2.22.3.1.5 Roaming Control Property Page

Sets properties for roaming controls.

SAP Afaria relies on the phone's native capabilities to recognize the roaming state. Supported device types – Windows Mobile Professional 5.0 or later and Windows Mobile Standard.

- Enable roaming controls – enforces all selected roaming control options while the device is roaming. If not selected, the device's current settings are used.
- Disable all GPRS/CDMA data connections – disables all connections that use General Packet Radio Service or Code Division Multiple Access protocol. The device can continue to use WiFi connections.

- Disable email attachments – disables automatic e-mail attachment downloading when synchronizing e-mail with the Microsoft Exchange Server. The user can download attachments manually by opening the e-mail and selecting an attachment.
- Disable Afaria connections – disables all Afaria connections that use GPRS/CDMA, except for connections initiated by an outbound notification from the server. The device can continue to use WiFi connections. This option only blocks connections; it does not disable any Afaria setup options.

  > **i Note**
  >
  > If you disable both GPRS/CDMA connections and Afaria connections, outbound notifications cannot initiate a connection to the server.
  >
  > Configuration Manager's Port Control page includes setting "Disable WiFi radio." If the setting is selected on the Port Control page, it disables WiFi continuously.

- (Windows Mobile 6.1 or later) Disable IMAP and POP3 – disables using IMAP or POP3 e-mail accounts.

  > **i Note**
  >
  > Configuration Manager's Port Control page includes setting "Disable IMAP/POP3." If the setting is selected on the Port Control page, it disables the IMAP and POP3 e-mail continuously.

- Display message when entering roaming – displays the specified message when a device enters the roaming state.
- Display message when exiting roaming – displays the specified message when a device exits the roaming state.
- Number of seconds to delay roaming transactions – defines the length of time a roaming state must be sustained before roaming control actions are enforced.

2.22.3.1.6 Port Control Property Page

Sets properties for port controls and data transfer.

Supported devices – Windows Mobile Professional 5.0 and later, Windows Mobile Standard

By regulating the use of hardware ports, you can enforce the availability of key device features, such as Bluetooth connectivity, data transfer methods, and the use of external data cards.

> **i Note**
>
> "Enforce" means the device holder is not able to change the settings you establish.

Attempting to use a disabled feature on a device results in a notification message informing the device holder that the system administrator has disabled the feature. However, attempting to use a disabled camera or infrared (IR) port does not generate a notification message.

Use the following settings to determine port control behavior:

- Enable Port/Device Control – enables the configuration and enforcement of port control options.
- Show disabled device list – provides the device holder with a list of device features you have disabled. The disabled list displays during an Afaria connection and at device startup. The list includes only the disabled features that are installed on a device. Disabled features that do not exist on a device, for example, a camera, infrared port, etc., do not appear in the list.

Data transfer settings control the availability of Bluetooth connectivity and other data transfer modes:

- Bluetooth radio – determines if the device can communicate with other Bluetooth devices. A disabled Bluetooth radio prevents all Bluetooth communication.
- Discoverable – broadcasts the device's connection availability to other Bluetooth devices that are actively searching for a connection. When you disable this feature, connections are still possible if devices that try to connect know the device's ID. For complete information about the discovery options supported by a device, see its related documentation.

> **i Note**
>
> Enabling the discoverable mode may create a conflicting setting for devices that are using a discoverable mode time out setting. The conflict causes frequent notifications to the users, one each time Configuration Manager restarts discoverable mode. Users can set the time out value to never time out to resolve the conflict.
>
> Disabling Bluetooth connections by device type is not possible for all Bluetooth protocol stacks. For Bluetooth protocols supplied by some vendors, you may need to disable the Bluetooth radio. See the Afaria system requirements for vendor-specific details.

The following table shows the Bluetooth profiles associated with each device type.

Device type	Bluetooth profiles included	Profile acronym
Miscellaneous device	Object Push Profile	OPP
Computer	File Transfer Profile	FTP
	Phone Book Access Profile	PBAP
	Synchronization Profile	SYNCH
Phone	Cordless Telephone Profile	CTP
	Subscriber Identity Module (SIM) Access Profile	SAP, SIM
LAN Access Point	Common Integrated Services Digital Network (ISDN) Access Profile	CIP
	Dial-Up Networking Profile	DUN
	LAN Access Profile	LAP
Audio Video	Advanced Audio Distribution Profile	A2DP
	Audio/Video Remote Control Profile	AVRCP
	Hands-Free Profile	HFP
	Headset Profile	HSP
	Intercom Profile	ICP
	Video Distribution Profile	VDP
Peripheral	Basic Printing Profile	BPP
	Fax Profile	FAX
	Hard Copy Cable Replacement Profile	HCRP
	Human Interface Device Profile	HID

Device type	Bluetooth profiles included	Profile acronym
Imaging	Basic Imaging Profile	BIP
Unclassified	Any profile not associated with another device type.	n/a

- Disable infrared port – determines if the IR port can be used to send and receive data. A disabled IR port remains in a powered off state and will no longer be accessible via the device's Control Panel or data transfer application.
- Disable WiFi radio – determines if access to a wireless LAN via a WiFi connection is possible. When you disable the WiFi radio, all wireless network access is blocked.
- Disabling the WiFi radio, while also provisioning a WiFi connection in the same policy, results in an alert message to tell you of a configuration conflict. Disabling the WiFi radio overrides WiFi provisioning.
- Disable USB communications – determines if a USB connection can be used to send and receive data. A device with USB communications disabled cannot utilize any type of USB connection. If Afaria detects that a USB device has connected, it is disabled immediately.

Use the following settings to manage the availability of device features:

- Disable external data cards – controls the ability of the device to access an external data card. Use of an external card for reading or writing data will not be possible on the device.
- Disable camera – determines if the device camera can be used. When disabled, starting the camera has no effect.
  Disable camera implementation intercepts camera driver activity on a device. Disabling the camera is not possible for devices that interface directly with the camera, that is, without the use of drivers.

Supported devices – Windows Mobile Professional 6.1 and later, Windows Mobile Standard 6.1 and later

Mobile Device Management settings enable you to control the types of messaging available on the device. Select from the following options:

- Disable IMAP and POP3 – when using a Microsoft e-mail client application, synchronization with IMAP or POP3 e-mail servers is blocked.

> **i Note**
>
> This setting applies only to Microsoft e-mail applications.
>
> This setting applies only to e-mail that has not yet been downloaded.

- Disable MMS and SMS – when using text messaging native to the operating system, the ability to send and receive Multimedia Messaging Service (MMS) and Short Message Service (SMS) messages is blocked.

> **i Note**
>
> This setting applies only to Microsoft messaging applications.

2.22.3.2 Device Properties

Specify device properties such as owner details, device sounds, and executable file properties.

General Page [page 206]

Sets properties for desktop connection and power.

Owner Property Page [page 206]
Sets properties for owner identification.

Sound Property Page [page 206]
Sets properties for device sounds.

User Access Property Page [page 207]
Sets properties for executable files.

Windows Mobile Update Property Page [page 208]
Configure and enforce how software and security updates issued by Microsoft are applied to the device.

2.22.3.2.1 General Page

Sets properties for desktop connection and power.

You can enter a unique description for the device, which may help you differentiate between devices and/or users.

- Device Description – a suitable description for the device.
- Allow connection to desktop PC when attached – enables the device to connect through a companion PC. You can select a connection method from the Connect to desktop PC using drop-down list, or enter the connection name exactly as it is listed on the device.
- On battery power, suspend after idle for – specifies the number of minutes a device can remain idle before suspending battery power.

  > **i Note**
  >
  > This option is available only for Windows Mobile Professional.

- Suspend while on external power – if you enable this option, you can determine the number of minutes after which the device should suspend external power.

2.22.3.2.2 Owner Property Page

Sets properties for owner identification.

Owner information is not displayed in the same manner on all Windows Mobile devices. Some information items may be unavailable on some devices. The sample user interface depicted here is for a Windows Mobile Professional or a Windows Mobile Standard device.

2.22.3.2.3 Sound Property Page

Sets properties for device sounds.

Supported device types – Windows Mobile Professional (including Windows CE) and Windows Mobile Standard

You can set the following options on the Sound page:

- Main sound volume – determine the volume level on the device.
- Event sounds – enable or disable event sounds (such as errors) on the device.
- Program sounds – enable or disable program sounds for the device. If you enable Program sounds, the Notification sounds option becomes available.
- Key click sounds – enable or disable key click sounds for the device.
- Screen tap sounds – enable or disable screen tap sounds for the device.

You can also select for users to be notified of specific events on their device. For example, if you select the check box next to ActiveSync: Begin sync, users will hear the sound you select to signify that ActiveSync has started. You can change options in the Sound, Msg, or Flash categories by clicking the item in the column that you want to change; a drop-down menu appears and lets you select another item.

2.22.3.2.4 User Access Property Page

Sets properties for executable files.

You can set the following options on the User Access page:

- Prevent user from accessing the Run Dialog – determines if the user can access the run dialog on the device.
- Disallow loading of external executables – (Windows Mobile Professional) determines whether users can run an executable from its location, copy an executable from its location, and open any non-executable files from its location. This setting does not impact the user's ability to manually copy non-executable files from its external location to another location for use.

  > **i Note**
  >
  > This option is available only for Windows Mobile Professional.

- Disallow autorun executables on storage cards – if an "autorun.exe" file is on the storage card, this setting determines whether it runs when the card is inserted. This setting does not impact the user's ability to manually run executables or open non-executable files on the card.
- Locked-out applications – select the Locked-out applications check box and type the names of the applications (for example, game1.exe) that you want to prevent from running on the device. Use a semicolon (;) to delimit multiple application names. This value overwrites the existing Locked-out Applications value on the device, rather than creating a cumulative list.

A single application may have different ways of being invoked. For example, you may be able to launch a calendar application by pressing a specific button on a handheld device or by navigating to the program file on the device's file system and running the file. If these different user launch points launch different processes or applications, then define each launching application or process in your policy to effectively prevent an application from running.

> **i Note**
>
> You can use a bogus value to effectively remove the current Locked-out Applications list from the device, without causing an adverse effect. Clearing the value or clearing the check box does not send a value to the device and therefore, does not have the effect of removing the current Locked-out applications list from the device.

2.22.3.2.5 Windows Mobile Update Property Page

Configure and enforce how software and security updates issued by Microsoft are applied to the device.

Supported devices – Windows Mobile Professional 6 and later, Windows Mobile Standard 6 and later.

> **i** Note
>
> "Enforce" means the device holder cannot change the settings you establish.

Select from the following options:

- Choose Windows Mobile update schedule – check automatically for device updates from Microsoft or only when manually requested by the device holder.
- Use my data plan to check for and download updates – use the subscribed data service plan when checking for and downloading updates.

2.22.3.3 Format Properties

Specify format properties for language, numbers, currency, time, and date.

Language preset – Using this option, you can determine the default settings for a particular language. When you select a language from the drop-down list, the default settings for that language appear in any area that applies. If you select this check box and do not configure any of the other options on the related Formats pages, the formats on the devices are set to the defaults for the language you selected.

On the Numbers page, you can configure the formatting for number properties, such as decimal placements, negative number formats, and measurement systems. This feature is useful is you have devices from several different countries that need to communicate with your server.

On the Currency page, you can set options such as the currency symbol and position, the decimal format, and the negative number format. This feature is useful when you have devices traveling to or working in countries with other currency formats.

On the Time page, you can configure the way devices keep and report time on the device. This feature is especially useful when devices from other time zones communicate with the server; you can configure all devices to use the same time format for reporting purposes, or you can set the time format on the devices to synchronize with the time on the server, for communication purposes. Note that these formats are pre-determined by the language you choose on the Formats page; you can override this default setting by selecting the check box and choosing the format you want to use from the list box.

On the Date page, you can configure the way devices report the date. This is useful when devices working in or traveling to other countries communicate with the server. Note that these formats are pre-determined by the language you choose on the Formats page; you can override this default setting by selecting the check box and choosing the format you want to use from the list box.

2.22.3.4 Device Configuration CSP Properties

Specify device configuration properties such as e-mail settings, synchronization settings and other device configuration details.

Favorites Page [page 209]
: Manage favorite URLs on devices.

E-Mail Page [page 209]
: Configure the Internet protocol e-mail services on your Windows Mobile devices.

Sync Page [page 210]
: Configure synchronization settings on the device.

Custom Page [page 210]
: Specify device configuration options specific or unique to your supported device. Palm and Symbian devices do not support custom provisioning.

2.22.3.4.1 Favorites Page

Manage favorite URLs on devices.

To add a favorite to the device:

Click *Add* to enter a favorite name and a URL. The favorite is added to the device when the device runs the policy.

To remove a favorite from the device:

Clear the URL field value to remove a previously defined favorite. The favorite is removed from the device when the device runs the policy.

2.22.3.4.2 E-Mail Page

Configure the Internet protocol e-mail services on your Windows Mobile devices.

You can set the following options:

- GUID – lets you generate a valid new GUID.
- Delete this e-mail entry on the Client – permanently deletes this e-mail setting on the device.
- Connection ID – lets you select a connection ID type from the drop-down list box.
- Service name – lets you provide a service name for e-mail on the device.
- Service type – lets you determine the type of incoming e-mail service from the server from the drop-down list box.
- Logon name – lets you provide a login name for e-mail on the device.
- Password – lets you provide a password for e-mail on the device.
- Domain – lets you provide a domain name for e-mail on the device.
- Display name – lets you set an e-mail a display name on the device.

- User's e-mail address – lets you set a user e-mail address on the device.
- Incoming e-mail server – lets you set an incoming e-mail server name on the device.
- Outgoing e-mail server – lets you set an outgoing e-mail server name on the device.
- Server requires authentication – determines whether authentication is required from the server.
- Days of e-mail to retrieve – lets you set the number of days of e-mail to retrieve.
- Maximum message size – lets you set the maximum message size to retrieve.
- Maximum attachment size – lets you set the maximum attachment size to retrieve.

2.22.3.4.3 Sync Page

Configure synchronization settings on the device.

You can set the following options on the Sync page:

- Auto-sync when cradled – set whether to perform active sync when the device is cradled.
- Maximum size of notes – allows you to set the maximum size of notes for the device.
- Conflict resolution – select how synchronization conflicts are handled.
- Device addressing method – allows you to select how the devices are addressed.
- Device phone number – specifies the phone number for the modem to use when synchronizing the device.
- Device SMS address – allows you to set the SMS address for the device.
- Disconnect when done – set whether the device will disconnect when synchronization is complete.
- Sync during off-peak hours – allows you to select when to synchronize the device during a pre-determined off-peak hour.
- Sync during peak hours – allows you to select when to synchronize the device during a pre-determined peak hour.
- Outbound mail delay (minutes) – allows you to set the time, in minutes, before sending outbound messages.
- Peak start time (24h format) – specifies what time of the day to start using peak service synchronization settings.
- Peak end time (24h format) – specifies what time of the day to stop using peak service synchronization settings.
- Send mail immediately – allows you to send messages immediately upon synchronization.
- Sync time when cradled – allows you to set a specific sync time when the device is cradled.
- Sync when roaming – allows you to specify how to synchronize when roaming.
- Peak Days area – use the peak days area to select the days of the week considered to be peak periods.

2.22.3.4.4 Custom Page

Specify device configuration options specific or unique to your supported device. Palm and Symbian devices do not support custom provisioning.

Customized configuration settings you create are included on the device when the policy is run on the device. You can set the following options on the Custom page:

- Custom provisioning XML – check this box to enable the provisioning text box where you can write your XML information or paste it in from another tool used to create your XML data file. You can use any of the

sample provisioning files in the MSDN library on Microsoft's Web site to help build your files, or you can follow the example owner.xml file below:

- ```
  owner.xml<wap-provisioningdoc>
  <characteristic type="Registry">
  <characteristic type="HKCU\ControlPanel\Owner">
  <parm name="Name" value="Name" datatype="string" />
  <parm name="Notes" value="Notes" datatype="string" />
  <parm name="Telephone" value="telephone number" datatype="string" />
  <parm name="E-Mail" value="email address" datatype="string" />
  </characteristic>
  </characteristic>
  </wap-provisioningdoc>
  ```

  > **i** Note
  >
  > Do not add the <wap-provisioningdoc> tags around the XML in the provisioning text box.
  >
  > You must create separate XML files for each configuration task you want to accomplish on the device. For example, if you want to set owner information on the device and also set browser favorites for the device, you must have a separate XML file for each task; for instance, owner.xml and addfavorite.xml.

- Additional PXML files – check this box to include one or more XML provisioning files created using another tool used to create your XML data. Use full path names and separate each file name with semicolons (example: C:\XML\file1.xml;C:\XML\file2.xml).

2.22.3.5 Network CSP Properties

Specify network properties such as GPRS details, proxy details, VPN details, and WiFi properties for the device.

GPRS Page [page 212]
: Configure your General Packet Radio Service (GPRS) communications entries on the device.

GPRS Advanced Page [page 212]
: Use the Advanced page in conjunction with the GPRS page to set General Packet Radio Service (GPRS) properties on the device. The GPRS Advanced page is only enabled when you place a check next to the Entry name field on the GRPS page and you must also provide an entry name on the GPRS page.

Cellular TAPI Page [page 213]
: Use the GPRS Cellular TAPI page in conjunction with the GPRS page to set GPRS properties on the device.

Networks Page [page 214]
: Configures additional network entries, such as ActiveSync Desktop Pass-through (DTPT), and metanetworks, such as the Internet, on the device.

Planner Page [page 214]
: Configure the preferred connections for each network, including pending connection requests, and active connections available on the device.

PPP Page [page 215]
: Configure point-to-point entries on the device.

Proxy Page [page 215]
: Configure proxy connections on the device.

WAP Proxies Page [page 215]
  ```

Configure wireless proxy settings on the device and add one or more proxies on the device.

VPN Page [page 216]
Configure Virtual Private Network (VPN) entries on the device.

WiFi Network Page [page 217]
Configure wireless local network associations with private or Internet network on the device.

NAPDEF Page [page 217]
Modify, add, and delete Wireless Application Protocol (WAP) network access point definitions and their associated settings using standard Windows Mobile Professional or WAP techniques on the device.

2.22.3.5.1 GPRS Page

Configure your General Packet Radio Service (GPRS) communications entries on the device.

You can set the following options on the GPRS page:

- Entry Name – identifies a name for the GPRS entry. A blank value is invalid when this box is checked.
- Delete this GPRS entry on the Client – permanently deletes the GPRS entry on the device.
- Destination – the location where the GPRS communication is being sent.
- Access point name – the name you provide to access the GPRS access point.
- Username – specifies the GPRS user name for the device.
- Password – specifies the GPRS password for the device. A blank value is invalid when this box is checked.
- Domain – specifies the domain to which the GPRS device belongs.

2.22.3.5.2 GPRS Advanced Page

Use the Advanced page in conjunction with the GPRS page to set General Packet Radio Service (GPRS) properties on the device. The GPRS Advanced page is only enabled when you place a check next to the Entry name field on the GRPS page and you must also provide an entry name on the GPRS page.

You can set the following options on the GPRS Advanced page:

- Enable this entry – allows you to enable the option on the GPRS page.
- Use specific name servers – enables the primary and alternate DNS and WINS options.
- Primary/Alternate DNS – allows you to manually enter the DNS addresses in the area provided.
- Primary/Alternate WINS – allows you to manually enter the WINS addresses in the area provided.
- Country code – allows you to provide a country code for the GPRS connection.
- Area code – allows you to provide and area code for the GPRS connection.
- Use country and area codes – determines whether to use both county and area codes when establishing a GPRS connection.
- Phone number – specifies the phone number to use for the GPRS connection for the device.
- Device name – allows you to specify the device name for the connection.
- Device type – allows you to specify a device type for the connection.
- Dial as local call – determines if the number should be dialed as a local call.
- Frame Size – allows you to determine the frame size for your device display.

- Framing – determines the frame speed for your device display.
- SW data compression – determines whether to use SW data compression.
- IP header compression – determines whether to use IP header compression.
- Require data encryption – determines whether to require data encryption.
- Require password – determines whether to require a password for your connection.
- Require encrypted password – determines whether an encrypted password is required for your connection.
- Require MS encrypted password – determines whether a Microsoft encrypted password is required for your connection.
- Script (full path) – allows you to provide the full path name for the script running on your device.

2.22.3.5.3 Cellular TAPI Page

Use the GPRS Cellular TAPI page in conjunction with the GPRS page to set GPRS properties on the device.

> **i Note**
>
> The GPRS Cellular TAPI page is only enabled when you place a check next to the Entry name field on the GRPS page; and you must also provide an entry name on the GPRS page.

You can set the following options on the GPRS Cellular TAPI page:

- Bearer info valid – determines whether bearer information is used for your device.
- Bearer info connection element – allows you to select the bearer information type.
- Bearer info service – allows you to select the bearer information service type.
- Bearer info speed – allows you to select the speed for the bearer information connection.
- GPRS info valid – allows you to validate your GPRS information.
- Protocol type – allows you to specify the GPRS protocol type for the device.
- L2 protocol type – allows you to specify the GPRS L2 protocol type for the device.
- Address – allows you to specify the packet address to use for the connection.
- Info data compression – allows you to indicate data compression information as off, on, or unknown.
- Info header compression – allows you to indicate off, on, or unknown.
- GPRS info parameters – allows you to specify protocol-specific values when defining a GPRS context.
- Compression info direction – allows you to specify the transmit or receive direction for the connection.
- Compression max dict entries – allows you to control the maximum number of dictionary entries for data compression.
- Compression max string length – allows you to control the maximum string length for data compression.
- Compression info required – determines whether compression information is required.
- Compression info valid – determines whether compression information is valid.
- Info QOS delay class – allows you to specify the Quality of Service (QOS) delay profile value.
- Info QOS mean throughput – allows you to specify the Quality of Service (QOS) mean throughput value.
- Info QOS peak throughput – allows you to specify the Quality of Service (QOS) peak throughput value.
- Requested QOS profile precedence – allows you to specify the Quality of Service (QOS) profile precedence value.
- Requested QOS reliability – allows you to specify the Quality of Service (QOS) profile reliability value.

- QOS info is valid – determines whether the Quality of Service (QOS) information is valid.
- Info min QOS delay class – allows you to specify the minimum Quality of Service (QOS) delay profile value.
- Info min QOS mean throughput – allows you to specify the minimum Quality of Service (QOS) mean throughput value.
- Info min QOS peak throughput – allows you to specify the minimum Quality of Service (QOS) peak throughput value.
- Requested min QOS profile precedence – allows you to specify the requested minimum Quality of Service (QOS) profile precedence value.
- Requested min QOS reliability – allows you to specify the requested minimum Quality of Service (QOS) profile reliability value.
- Min QOS info is valid – determines whether the minimum Quality of Service (QOS) information is valid.

2.22.3.5.4 Networks Page

Configures additional network entries, such as ActiveSync Desktop Pass-through (DTPT), and metanetworks, such as the Internet, on the device.

2.22.3.5.5 Planner Page

Configure the preferred connections for each network, including pending connection requests, and active connections available on the device.

You can set the following options on the Planner page:

- Name – allows you to provide a name for the Internet connection for the device.
- GUID – allows you to provide a valid GUID in the proper format.
- Cache time – allows you to specify the default time, in seconds, for which the planner caches released connections.
- Retry count – allows you to specify the number of times the planner attempts to retry failed connection attempts.
- Bandwidth coeff. – allows you to set a bandwidth coefficient, in 16.16 fixed point, for planner path calculations.
- Cost coeff. – allows you to set a cost coefficient, in 16.16 fixed point, for planner path calculations.
- Latency coeff. – allows you to set a latency coefficient, in 16.16 fixed point, for planner path calculations.
- Failover default – determines whether you can set the default value for the failover prompt.
- Failover prompt – allows you to determine whether the planner sets a yes/no prompt before using a non-preferred connection.

2.22.3.5.6 PPP Page

Configure point-to-point entries on the device.

You can set the following options on the PPP page:

- Entry name – identifies a name for the PPP connection entry. A blank value is invalid when this box is checked.
- Delete this PPP connection on the Client – permanently deletes this PPP connection on the device.
- Destination – identifies where the PPP communication is being sent.
- Device name – allows you to specify the device name for the connection.
- Country code – specifies the country code to use for the PPP connection.
- Area code – specifies the area code to use for the PPP connection.
- Phone number – specifies the phone number to use for the PPP network connection for the device.
- User name – specifies the user for the PPP network connection.
- Password – allows you to provide a password for the PPP connection on the client.
- Domain – specifies the domain for the PPP connection on the client.
- Use specific name servers – determines whether to use specific primary and alternate name servers.
- Primary/Alternate DNS – allows you to manually enter the DNS addresses in the areas provided.
- Primary/Alternate WINS – allows you to manually enter the WINS addresses in the areas provided.
- Enable entry – allows you to enable or disable a connection entry without removing it from the system.

2.22.3.5.7 Proxy Page

Configure proxy connections on the device.

You can set the following options on the Proxy page:

- Name – specifies the name of the proxy setting.
- Delete this proxy on the Client – permanently deletes this proxy on the device.
- Type – allows you to select the type of proxy connection.
- Source – allows you to select the source of location for the proxy connection.
- Destination – locates where the proxy communication is being sent.
- Proxy server – specifies the name of the proxy server on the device.
- Proxy port – specifies the port for the proxy connection.
- User name – specifies the user name required for the proxy connection on the device.
- Password – allows you to provide a password for the proxy connection on the device.

2.22.3.5.8 WAP Proxies Page

Configure wireless proxy settings on the device and add one or more proxies on the device.

You can set the following options on the WAP Proxies page:

- Proxy ID – specifies the ID for the WAP proxy connection on the device.

- Name – allows you to type the name of proxy connection in the area provided.
- Delete this WAP proxy entry on the Client – permanently deletes this WAP proxy entry on the device.
- Start page – specifies the start Web page for the proxy connection on the device.
- Domains – specifies the domain for the proxy connection on the device.
- Start page user ID – specifies the user ID for the WAP proxies start Web page on the device.
- Start page password – allows you to provide a password for the WAP proxy start page connection on the device.
- Push operations – allows you to enable or disable push operations on the device.
- Enable trust for physical proxies – allows you to define whether or not the physical proxies in this logical proxy are trusted.
- Physical proxies – allows you to add one or more physical proxies on the device. To add a proxy, click *Add* to display an area for including a new proxy entry in the Proxy ID column. Type a name in the field, then type a valid address in the Address column. Select a proxy type from the Type drop-down list, and type valid NAP ID, Port 1, Port 2, and Services in their respective columns.

To exclude a proxy or all proxies, select the specific proxy or all the proxies and click *Exclude*.

2.22.3.5.9 VPN Page

Configure Virtual Private Network (VPN) entries on the device.

You can set the following options on the VPN page:

- Entry name – identifies a name for the GPRS entry. A blank value is invalid when this box is checked.
- Delete this VPN connection on the Client – permanently deletes this VPN connection on the device.
- Source – allows you to select the source of location for the proxy connection from the drop-down list box.
- Destination – locates where the VPN communication is being sent.
- Host Address – allows you to provide the host address for the connection.
- User name – specifies the VPN account user name for the device.
- Password – allows you to provide a password for the VPN connection on the device.
- Domain – allows you to provide a domain name for the VPN connection on the device.
- Use specific name servers – specifies whether the device should use server-assigned addresses.
- Primary/Alternate DNS – allows you to manually enter the DNS addresses in the areas provided.
- Primary/Alternate WINS – allows you to manually enter the WINS addresses in the areas provided.
- Enable entry – allows you to enable or disable a connection entry without removing it from the system.
- Type – allows you to select the VPN connection type for the device.
- Authentication – allows you to select authentication type.
- Preshared key – allows you to define the key.

2.22.3.5.10 WiFi Network Page

Configure wireless local network associations with private or Internet network on the device.

You can set the following options on the WiFi page:

- Name – allows you to provide a name for the WiFi connection on the device.
  Provisioning a WiFi connection, while also disabling the WiFi radio in the same policy, results in an alert message to tell you of a configuration conflict. Disabling the WiFi radio overrides WiFi provisioning.
- Destination ID – allows you to select a destination ID for the WiFi connection on the device.

2.22.3.5.11 NAPDEF Page

Modify, add, and delete Wireless Application Protocol (WAP) network access point definitions and their associated settings using standard Windows Mobile Professional or WAP techniques on the device.

You can set the following options on the NAPDEF page:

- NAP ID – allows you to provide a NAP ID name for the wireless connection on the device.
- Permanently delete this NAPDEF entry on the Client – permanently deletes the NAPDEF entry on the device.
- Name – allows you to set a NAP ID name.
- Address – allows you to enter an address for wireless connection on the device.
- Address Type – allows you to select a NAP address type.
- Authentication Type, Name, and Password – allows you to set a name address and password for the NAP connection.

2.23 Windows Phone Policies

Windows Phone App Store Application Policies [page 218]
App Store application policies for Windows Phone define the Windows Store applications that appear on the Afaria app list, and are therefore available for installation.

Windows Phone Enterprise Application Policies [page 221]
Windows Phone enterprise application policies define the enterprise-signed applications that are available for devices to install.

Creating a Configuration Policy for Windows Phone [page 225]
Create a policy to define the settings for MDM payloads, such as Exchange ActiveSync and passcodes.

Creating an Enrollment Policy for Windows Phone [page 238]
Create an enrollment policy to enroll a Windows Phone device. The enrollment code URL used to enroll the device is generated automatically based on the enrollment server settings.

2.23.1 Windows Phone App Store Application Policies

App Store application policies for Windows Phone define the Windows Store applications that appear on the Afaria app list, and are therefore available for installation.

Commercial applications are delivered from the Windows Phone commercial market. An application package includes information that identifies the application.

Enroll Windows Phone devices in management before deploying any applications.

Preparing for Windows Store Application Management [page 218]
Use a Web search or other means to locate and record an application name, as defined by the developing entity.

Creating an Application Policy for Windows Phone App Store Applications [page 219]
Create an application policy for the Windows Store app.

Deploying Windows Store Applications [page 220]
Deploy Windows Phone applications automatically by deploying the application policy to a device using the MDM protocol option, or allow a user to browse the app list on his or her device and install the application.

2.23.1.1 Preparing for Windows Store Application Management

Use a Web search or other means to locate and record an application name, as defined by the developing entity.

You can search the Windows Store site from your desktop, to discover the package name by selecting an application and extracting the package name from the URL. For example, if the Windows Store app URL is www.windowsphone.com/en-us/store/app/sap-bydesign-fp3-0/40b3959e-3f31-43f7-84c5-48e206b9d589, then:

- Windows Store ID – 40b3959e-3f31-43f7-84c5-48e206b9d589
- Country code – en-us
- Package name – sap-bydesign-fp3-0

You can also click the Windows Store URL available in the App Store application policy screen, to navigate to Windows Store and select the required app.

2.23.1.2 Creating an Application Policy for Windows Phone App Store Applications

Create an application policy for the Windows Store app.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy list page, top toolbar, click *New* > *Application* > *Windows Phone App Store*.
2. On the Summary page, enter the policy name and description, and indicate whether the policy is published or unpublished.

   Connecting devices receive only published policies. You can specify duplicate policy names across tenants and within a tenant for all policy types.
3. (Optional) Select Featured to tag the application as featured.
4. On the General page, enter the app name in the Search by App Name field.
   A dynamic list of all apps from the App Store that match the entered app name is displayed.
5. Enter a valid Country Code in order to use the Search by App Name feature or retrieve an app using Windows Store Number. The default value for Country Code is 'US'.
6. Select the desired app from the results list.
   The fields Windows Store Number, Windows Package Name, and Information are automatically populated with information.
7. Alternatively, if you do not want to use the Search by App Name feature, you can type in the Windows Store Number, and click *Update* to retrieve the desired app and its corresponding details.

   > **i Note**
   >
   > Country Code is required in order to retrieve app details using Windows Store Number.

   - Windows Store Number – provide the Windows Store ID for the app. Click the Windows Store URL to navigate to the Windows Store and select the required app. The last part of the app URL constitutes the Windows Store ID.
   - Country Code – enter the country code from the app URL. The default value is "en-us".
   - Windows Package Name – enter the package name from the app URL.

   For example, if the Windows Store app URL is www.windowsphone.com/en-us/store/app/sap-bydesign-fp3-0/40b3959e-3f31-43f7-84c5-48e206b9d589, then:
   - Windows Store ID – 40b3959e-3f31-43f7-84c5-48e206b9d589
   - Country code – en-us

- Package name – sap-bydesign-fp3-0

8. (Optional) On the Categories page, select one or more categories to associate with the policy. Move categories from the Available Categories table to the Selected Categories table.
9. (Optional) Click *Add* to add a new category.
10. (Optional) Select *Yes* or *No* to indicate if the selected category is a featured category.
11. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note.

    The maximum length for the file name is 258 characters, and the maximum image size is 1MB. To enable easy download and minimize data traffic, use smaller image up to 100KB.
12. (Optional) On the Description Detail page, enter a description for the application and modify the display name, if required.

    The display name of the application is automatically updated when you upload the application package on the General page.

2.23.1.3 Deploying Windows Store Applications

Deploy Windows Phone applications automatically by deploying the application policy to a device using the MDM protocol option, or allow a user to browse the app list on his or her device and install the application.

Prerequisites

To download apps from the Windows Store, device users must have an account with Microsoft. Microsoft user account agreements and costs are independent of Afaria operations.

Procedure

1. On the Policy page, link the Windows Store application policy to a group.
2. On the Group page, connect the group's devices to apply policies.
3. Enroll the devices in Afaria management.

   The SAP Afaria client is silently installed on the device.
4. Launch Afaria on the device and browse the list of applications on the Apps page.

   If you use the optional category attribute, applications are grouped by category.
5. On the device, click *Install* to install an app.

   The device connects to the Windows Store, where the user can initiate the installation.

2.23.2 Windows Phone Enterprise Application Policies

Windows Phone enterprise application policies define the enterprise-signed applications that are available for devices to install.

Enterprise-signed applications are produced by third-party entities and are delivered from the Afaria package server. An application package includes information that identifies the application.

2.23.2.1 Working with Windows Phone Enterprise Applications

To install Windows Phone enterprise applications, enterprises must establish an account with Windows Phone Dev Center, and employees must enroll their phones for app distribution from the company.

Procedure

1. The company must register with the Windows Phone Dev Center and acquire an enterprise mobile code-signing certificate from Microsoft.

   This certificate is required to generate the application enrollment token (AET) to sign the enterprise apps.
2. Export a PFX file from the code-signing certificate, and use the AETGenerator tool provided by Windows Phone SDK 8.0 to generate an application enrollment token (AET).
3. Precompile the assemblies into native code, and sign the app using the PFX file you exported from the enterprise certificate.
4. In the Afaria Administration console, upload the AET file and the signed Afaria application. See *Uploading the Application Enrollment Token and Signed Afaria Application* for details.

   If the uploaded AET file has expired, then Windows Phone enrollment will not be successful.
5. Enroll the devices in Afaria.

The AET file and the signed Afaria application are pushed to the device during enrollment.

6. Sign the enterprise applications using the same code-signing certificate used to generate the AET file.
7. Use enterprise application policies to deploy the apps on the device.

   For more details about creating a company account, generating enrollment tokens, and code-signing applications, refer the Windows Phone Dev Center documentation.

2.23.2.2 Uploading the Application Enrollment Token and Signed Afaria Application

Upload the Application Enrollment Token (AET) generated using the code-signing certificate for the enterprise, and the Afaria application (.XAP) signed by the same code-signing certificate.

Prerequisites

For more details about creating a company account, generating enrollment tokens, and code-signing applications, refer to the Windows Phone Dev Center documentation.

Procedure

1. On the Home page Server tile, navigate to the *Configuration* > *Component* > *Windows Phone* page.
2. In the AET File field, click *Browse* and select the AET file to upload.
3. Download the unsigned Afaria application (.XAP) file.
4. Sign the Afaria application using the same code-signing certificate used to generate the AET file.
5. Click *Browse* to select and upload the signed Afaria application.

   The Afaria application is silently installed on the Windows Phone device, when the device enrolls in management.

   > **i** Note
   >
   > If the uploaded AET file has expired, then Windows Phone enrollment will not be successful.

2.23.2.3 Preparing for Windows Phone Enterprise Application Management

For each enterprise-developed application, use Windows Phone development procedures to make compiled applications available for Afaria use.

Make a copy of the compiled application (.xap) available to the administrator who is responsible for creating application policies.

Before accessing the apps, ensure that the application enrollment token (AET) for the enterprise is available on the device. Enterprise apps must also be signed by the same code-signing certificate used to generate the AET.

2.23.2.4 Creating an Application Policy for Windows Phone Enterprise Applications

Create a policy for optional or required enterprise-signed applications for Windows Phone devices.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy list page on the top toolbar, click *New* > *Application* > *Windows Phone Enterprise*.
2. On the Summary page, enter the policy name and note, and indicate whether the policy is published or unpublished.

   Connecting devices receive only published policies. You can specify duplicate policy names across tenants and within a tenant for all policy types.
3. (Optional) Select Featured to tag the application as featured.
4. On the General page, define the application details.
   - Install – choose optional or required. MDM protocol is mandatory for required apps. Applications configured with the MDM protocol option are automatically pushed to the device when the device connects next. Optional apps are pushed to the device when the application policy is applied the next time a device connects. Users can browse to and manually install the optional apps in their Afaria apps lists.
   - XAP – click *Browse* to locate and upload the application package file (.xap). The file path is relative to the administrator user's workstation. The application icon and the details related to the application appear in the Information field.
   - Artwork (512*512px) – click *Browse* to locate and upload the image that appears as the featured application icon on the device.

Artwork supports PNG and JPEG formats with a resolution of 512x512 pixels.

5. (Optional) On the Categories page, select one or more categories to associate with the policy.
6. (Optional) In the Available Categories list, click *Add* to add a new category.
7. (Optional) Select *Yes* or *No* to indicate whether the selected category is a featured category.
8. (Optional) Click *Browse* and select the image file (.JPG or .PNG) to be associated with the category and enter any additional note.

> **i Note**
>
> The maximum length for the file name is 258 characters, and the maximum image size is 1MB. To enable easy download and to minimize data traffic, use smaller image files up to 100KB.

9. (Optional) On the Description Detail page, modify the display name of the application and enter a description for the application.

   The display name and the version of the application are automatically updated when you upload the application package on General page.
10. (Optional) Click *New* to browse to and select the application screen shot that appears on the device.

    You can upload as many as eight screen shots from which you can select the application image to appear on the device.

> **i Note**
>
> The appearance of the uploaded image may change, depending on the size of the image and the browser settings. The maximum image size is 1MB.

2.23.2.5 Deploying Windows Phone Enterprise Applications

Deploy Windows Phone enterprise applications by deploying the application policy. Launch Afaria application on the device, browse the application list and install the enterprise applications.

Prerequisites

Before accessing the apps, ensure that the application enrollment token (AET) for the enterprise is available on the device. The enterprise apps must also be signed by the same code-signing certificate used to generate the AET.

Procedure

1. On the Policy page, link the Windows Phone Enterprise application policy to a group.
2. On the Group page, connect the group's devices to apply policies.
3. Enroll the devices in Afaria management.

   Afaria is silently installed on the device.

4. Launch the Afaria application on the device, and browse the list of applications on the Apps page.

   The device displays the list of applications from the Package Server. If you use the optional category attribute, applications are grouped by category.
5. On the device, click *Install* to install an app.

   Afaria connects to the Package Server, downloads the application, and initiates the installation.

2.23.3 Creating a Configuration Policy for Windows Phone

Create a policy to define the settings for MDM payloads, such as Exchange ActiveSync and passcodes.

Context

To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the *Policy* page, on the top toolbar, click *New* > *Configuration* > *Windows Phone*.
2. On the *Summary* page, enter the policy name.

   You can specify duplicate policy names across tenants and within a tenant for all policy types.
3. Enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished. Connecting devices receive only published policies.
   - Priority – set a user-defined value to determine which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
   - Inventory – select the inventory type to collect. You can view inventory information on the *Device* page's *Device Inspector*.
     - Do not collect inventory – no inventory collection.
     - Hardware only – collects data related to the device's physical components, such as processors and memory cards.
     - Software and Hardware – collects data related to the device's physical components as well as the details of the enterprise apps, signed by the same code-signing certificate.

     > **i Note**
     >
     > The device management client on the Windows Phone device is responsible for sending the software inventory related information to the Afaria server, during device refresh. The refresh interval is pre-programmed in to the device management client at the time of enrollment.
4. On the *App Restrictions* page, maintain a list of the denied or allowed apps.
5. On the *Assigned Access* page, select the applications and settings to provide a customized locked down user experience on the device.

6. On the *Certificate* page, browse and upload the certificate for authenticating the Windows Phone device.
7. On the *Exchange ActiveSync* page, configure an Exchange ActiveSync account to connect to the corporate Exchange server.

   You can create the account by specifying the user name, host name, and e-mail address, or only the host name. Users provide other values when they install the policy. If an Exchange policy with a blank password field is synchronized with the device, you cannot add the password later by editing the policy.

   For password, if you use a directory substitution variable, you cannot decrypt the credentials on the Active Directory domain and the user will not receive e-mail messages, until the user adds the password field in the Exchange account. If any of the variables do not have the right values defined under the attributes for Active Directory, the device may not be able to configure the e-mail account successfully.
8. On the *Passcode* page, define the minimum password length, password expiration days, and other password characteristics.

   It is recommended to use a complex password policy for a Windows Phone device. When the configuration policy loads, the user must enter a passcode that satisfies the policy. If the Exchange security settings are more secure than the passcode policy, the user may be forced to change the password on the device, once the Exchange policy is sent down and configured.
9. On the *Restrictions* page, define the restrictions for users to access certain features such as user experience, security settings, account settings, application management etc. Select the check box corresponding to a feature to disable it.
10. On the *SCEP* page, configure the settings to allow devices to obtain certificates over the air from a certificate authority server that uses SCEP.
11. On the *WiFi* page, configure connections to WiFi networks.

Windows Phone Configuration Policy MDM Payloads [page 226]
: Windows Phone configuration policy MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and certificates for Windows Phone devices.

Related Information

Substitution Variables [page 29]

2.23.3.1 Windows Phone Configuration Policy MDM Payloads

Windows Phone configuration policy MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and certificates for Windows Phone devices.

App Restrictions [page 227]
: The App Restrictions payload maintains a list of apps that are allowed or denied on the device. You can define either a denied item list or an allowed item list. The restrictions are maintained based on the app details, or the publisher details.

Assigned Access [page 228]

Enterprise Assigned Access enables an enterprise to provision a device to a locked down user experience. The administrator can customize the start screen with pinned applications, control the visibility of certain system settings, and configure custom launch actions for buttons.

Certificate [page 230]
The Certificate payload uploads the root or intermediate certificate for Windows Phone device authentication.

Exchange ActiveSync [page 230]
The Exchange ActiveSync payload determines how Windows Phone devices interact with Microsoft Exchange servers.

Passcode [page 231]
The passcode payload defines the passcode requirements on the device.

Restriction [page 232]
The Restriction payload defines the restrictions for users to access certain features such as account settings, application management, security settings, user experience, etc.

SCEP [page 233]
The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

WiFi [page 234]
The Wi-Fi payload configures connections to Wi-Fi networks on Windows Phone devices.

VPN [page 236]
By establishing a VPN connection, corporate mobile users can securely access critical business information from a corporate network through any public network.

2.23.3.1.1 App Restrictions

The App Restrictions payload maintains a list of apps that are allowed or denied on the device. You can define either a denied item list or an allowed item list. The restrictions are maintained based on the app details, or the publisher details.

Setting	Description
Enabled	Whether Afaria can send the app restrictions payload to allow or restrict apps on the device.
Denied Items	Maintain a denied item list.
Allowed Items	Maintain an allowed item list.
Apps and Publishers: App	Maintain the denied or allowed list based on app details.
App Name	Name of the allowed or denied app.
Product ID	Product ID of the allowed or denied app. You can also view the app details from the Windows Phone Store using the link provided.
Apps and Publishers: Publisher Name	Maintain the denied or allowed list based on publisher name.
Allowed Apps under Publisher	Llist of allowed apps from a denied publisher.

Setting	Description
Denied Apps under Publisher	Llist of denied apps from an allowed publisher.

> **i** Note
>
> When you edit the payload to change a denied list to an allowed list, or vice versa, the items that already exist on the list are also moved.

2.23.3.1.2 Assigned Access

Enterprise Assigned Access enables an enterprise to provision a device to a locked down user experience. The administrator can customize the start screen with pinned applications, control the visibility of certain system settings, and configure custom launch actions for buttons.

Assigned Access should be used together with Application Restriction policy controls. You may still be able to deep link in to settings or applications based on file handling. Once Assigned Access has been provisioned to a device, the only way to remove this functionality is to reset the device to factory settings.

> **⚠** Caution
>
> This feature may cause the device to fail or lose connectivity and require that the device be serviced at a Nokia-authorized repair center to reset to factory settings. Microsoft is not liable for any damage to the device or any loss of productivity that results from use of this feature.

Setting	Description
Enabled	Whether Afaria can send the assigned access payload to provision the device for a locked down user experience.
Apps	
Third Party Apps	Click *Add* to configure the settings for third party store apps.
Search by App Name	Search for the app by providing the app name. App details are retrieved based on the app name entered.
Windows Store App Name	The name of the third party app.
Windows Store Product ID	The product ID of the app. You can also get it from the Windows Phone Store.
Country Code	The country code of the application. You can get it from the Windows Phone Store URL for the app.
Pin to start	Pin the application to the start screen on the device.
Tile size	Tile size for the application icon on the start screen.

Setting	Description
First Party Apps	Select the first party apps or the default apps such as Calculator and Calendar, that should be allowed on the device. Indicate if the app must be locked to the start screen, and select the tile size for pinning the app. Only the apps selected here are visible on the device.
Settings	
System Settings	Select any system setting to disable it on the device. All the system settings are allowed by default.
Application Settings	Select any application setting to disable it on device. All the application settings are allowed by default.
Button Lockdown and Remap	
Button Lockdown	Lock the button down to prevent it from executing or starting the normal functionality. You can enable this option for the Camera, Start, and Search buttons, and can also indicate the event that triggers the lockdown action.
Button Remap	Remap the search button functionality to perform a specific action. Remap option is available only for the search button.
Remap Search button to an app	Select this option to remap the search button to launch an application.
Button Event	Select the button event that triggers the remapped action.
Type of mapped app for Press event	Indicate the type of app to launch for the button press event.
Select the first party remap app	Select the first party app to launch for the button press event.
Type of mapped app for PressAndHold event	Indicate the type of app to launch for the button press and hold event.
Select the first party remap app	Select the first party app to launch for the button press and hold event.
General	
Disable Action Center	Disable the action center that includes settings and notifications that users can quickly access.
Disable Menu Items	Disable the start screen allows menu that helps the user to configure and customize the start screen.
Select Start Screen Size	Select the start screen size from the options provided: small or large. Large screen represents a 3-column start view, which enables six small tiles to be pinned in one row. Small screen allows four small tiles in one row.

2.23.3.1.3 Certificate

The Certificate payload uploads the root or intermediate certificate for Windows Phone device authentication.

Setting	Description
Enabled	Whether Afaria can send the certificate payload to devices for authentication.
Certificate type	Type of the certificate used for authentication • Root – the root certificate from the certificate authority. • Intermediate – the intermediate certificate from the certificate authority.
Certificate	Browse and upload the certificate for authentication.
Issued to	The party to which the certificate is issued to. This is automatically updated when the certificate is uploaded.
Expires on	Expiry date of the certificate. This is automatically updated when the certificate is uploaded.

2.23.3.1.4 Exchange ActiveSync

The Exchange ActiveSync payload determines how Windows Phone devices interact with Microsoft Exchange servers.

Setting	Description
Enabled	Whether SAP Afaria sends the Exchange ActiveSync payload to devices to add an Exchange ActiveSync account.
Name	The name of the Exchange ActiveSync payload.
Host	The host name or IP address of the Microsoft Exchange server.
Use SSL	Whether the Microsoft Exchange Server uses SSL.
Domain Host	The host name or the IP address of the domain host.
User	The user name that devices use to authenticate with the Microsoft Exchange Server. If you do not define this setting, devices prompt users for it when the policy is applied.
Email Address	The email address for the account.
Password	(Optional) The password that devices use to authenticate with the Microsoft Exchange Server for encoded profiles.

Setting	Description
Download new content	The time interval to download new content.
Download email from	The duration in days for which the emails are downloaded.
Email	Select to synchronize e-mail.
Contacts	Select to synchronize contacts.
Calendar	Select to synchronize calendar details.
Tasks	Select to synchronize task details.

2.23.3.1.5 Passcode

The passcode payload defines the passcode requirements on the device.

Setting	Description
Enabled	Whether SAP Afaria can send the passcode payload to devices.
Allow simple value	Whether a simple password, which contains repeated characters or character sequences, is permitted.
Require alphanumeric value	Whether the password requires letters as well as numbers.
Minimum passcode length	The minimum required length of the password.
Minimum number of complex characters	The minimum number of symbols required in the password.
Maximum passcode age	The maximum age of a password. When the password reaches the maximum age, the user must change it.
Auto lock	The period of time during which devices can be inactive before locking automatically.
Passcode history	The number of unique passwords that must occur before a password can be repeated.
Maximum number of failed attempts	The number incorrect password attempts allowed before the device gets locked.

2.23.3.1.6 Restriction

The Restriction payload defines the restrictions for users to access certain features such as account settings, application management, security settings, user experience, etc.

The entire set of restrictions are supported by Windows Phone 8.1 or higher devices.

> ⚠ Caution
>
> Certain combinations of settings in this feature may cause the device to fail or lose connectivity, and require that the device be serviced at a Nokia-authorized repair center to reset to factory settings.

Setting	Description
Enabled	Whether SAP Afaria can send the Restriction payload to devices.
Disable WiFi	Disables Wi-Fi on the device.
Disable Internet Sharing	Disables sharing of your cellular data connection over Wi-Fi.
Disable Auto Connect To WiFi Sense Hotspots	Disables automatic connection to Wi-Fi networks using Wi-Fi Sense hotspot.
Disable WiFi Hot Spot Reporting	Disables reporting of the Wi-Fi hotspots.
Disable Manual WiFi Configuration	Disables manual configuration of Wi-Fi settings.
Disable NFC	Disables near field communication
Disable Bluetooth	Disables Bluetooth.
Disable VPN Roaming Over Cellular	Disables VPN policies over cellular connections, while roaming.
Disable VPN Over Cellular	Disables VPN policies over cellular connections.
Disable USB Connection	Disables USB connections to the device.
Disable Cellular Data Roaming	Disables roaming of cellular data.
Disable Use Of Storage Card	Disables the use of storage card on the device.
Disable Telemetry	Disables telemetry or app usage information collection.
Disable Location	Disables location collection.
Disable User To Reset Phone	Disables phone reset. The user cannot perform even a hard reset.
Disable Copy paste	Disables copying and pasting of content.
Disable Screen Capture	Disables screen capture.
Disable Voice Recording	Disables voice recording.
Disable SaveAs of Office Files	Disables saving of Office files.
Disable Sharing of Office Files	Disables sharing of Office files.
Disable Cortana	Disables Cortana.
Disable SyncMySettings	Disables syncing of settings across your Microsoft devices.

Setting	Description
Disable Manual MDM Unenrollment	Disables unenrollment from MDM.
Disable Microsoft Account Connection	Disables creation of a Microsoft account (store account). Accounts that are already created will not be disabled.
Disable Adding Non Microsoft Accounts Manually	Disables creation of non-Microsoft accounts such as Google, Facebook etc. Accounts that are already created will not be disabled.
Disable Manual Root Certificate Installation	Disables manual installation of Root certificate.
Require Device Encryption (Requires UEFI secure boot enabled device)	Enforces device encryption.
Disable Store	Disables accessing the store apps.
Disable Developer Unlock	Disables unlocking the device for debugging and testing Windows Phone apps.
Disable Search To Use Location	Restricts Bing search from accessing the device location.
Require Safe Search Permissions	Sets Safe Search permission to 'strict'. You cannot change this setting.
Disable Storing Images From Vision Search	Disables storing images from Bing Vision search.
Disable Browser	Disables the default browser.
Disable Camera	Disables camera.
Disable Action Center Notifications	Disables action center notifications from appearing on the device lock screen.

2.23.3.1.7 SCEP

The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

Setting	Description
Enabled	Whether Afaria can send the SCEP payload to devices.
CA	Certificate authority that processes SCEP, SCEP Challenge, Entrust and Microsoft Native requests. **i Note** Microsoft Native configured CA's require the below templates: • Exchange Enrollment Agent (Offline Request) with key usage set to Digital Signature. • CEP Encryption key usage set to KeyEncipherment.
Subject Name	X.500 name of the organization ID, in array form.

Setting	Description
Subject Alternative Name: Type	Type of the subject alternative name. Windows Phone 8.1 supports only the following alternative name types: • User Principle Name • Registered ID • Name URL • DNS Name • Email Address
Subject Alternative Name: Name	Value of the subject alternative name.
Use as Digital Signature	Whether the device uses the certificates from SCEP requests as digital signatures.
Use for Encryption	Whether the device uses the certificates from SCEP requests for encryption.
Encryption	Encryption mechanism used.
Key Protection	Restriction method that determines what a certificate can be used for. This allows the administrator to issue certificates to be used for specific tasks, or for a broad range of functions.
Key Length	Size of the key, in bits: • 1024 • 2048 **i Note** Key length 4096 is not currently supported.
Retry Count	Number of times that the device attempts the SCEP request.
Retry Delay	Period of time that must elapse between retry attempts.

2.23.3.1.8 WiFi

The Wi-Fi payload configures connections to Wi-Fi networks on Windows Phone devices.

Setting	Description
Enabled	Whether SAP Afaria can send the Wi-Fi payload to devices.
Select Service Set ID	The SSID of the Wi-Fi network.
Connection Mode	The Connection Mode element indicates whether connection to a wireless LAN should be automatic or initiated by the user. Windows Phone 8.1 and Windows Phone 10 support Manual and Auto connection modes.
Hidden	Whether the Wi-Fi network is hidden.

Setting	Description
Security Authentication Type	The security that the Wi-Fi network uses: • Open • WPA / WPA 2 Personal • WPA / WPA 2 Enterprise
Encryption	Encryption options are: • None • WEP • TKIP • AES
Authentication	The authentication settings for the Wi-Fi network, available for these security types: • WPA / WPA 2
Protocol	The Protocol settings for the Wi-Fi network, available for these security types: • WPA / WPA 2 Enterprise
Proxy	The proxy settings for the Wi-Fi network.
Trust	The Trust settings for the Wi-Fi network, available for these security types: • WPA / WPA 2 Enterprise
PMK Cache	The Trust settings for the Wi-Fi network, available for these security types: • WPA 2 Enterprise • The PMKCacheMode element indicates whether PMK caching will be used. • The PMKCacheTTL element indicates the length of time, in minutes, that a PMK cache will be kept. • The PMKCacheSize element specifies the number of entries in the PMK cache on the client. • The Pre Auth Mode element indicates whether pre-authentication will be used by the client. • The Pre Auth Throttle element specifies the number of pre-authentication attempts to try on neighboring APs.

Supported Wi-Fi Combinations

Device Type	Connection Type	Connection Mode	Security Authentication Type	Encryption
Windows Phone 8.1or higher	ESS	Manual/Auto	Open	None
			Open	WEP
			WPAPSK	TKIP

Device Type	Connection Type	Connection Mode	Security Authentication Type	Encryption
			WPA2PSK	TKIP
			WPAPSK	AES
			WPA2PSK	AES

2.23.3.1.9 VPN

By establishing a VPN connection, corporate mobile users can securely access critical business information from a corporate network through any public network.

Setting	Description
Enabled	Whether SAP Afaria can send the VPN payload to devices.
Connection Name	Provide a name for the VPN connection.
Substitution (Optional)	If you include user-defined substitution variables in policies that are planned for this device, define values for the appropriate variables. If the variable is not yet on the list, click Add to enter the variable name and value for the current device, as appropriate for your requirements. The variables on the list are global for the current tenant. The values you define for the variables are for only the current device.
Connection > Connection Type	Choose the VPN connection type. The settings vary by connection type; for detailed information, see the vendor documentation for your specific implementation. • Native • F5
Server Address	Provide the Afaria server address or relay server address.
DNS Suffix	Provide the DNS suffix for the client computer.
User Authentication	Choose one of the following authentication methods: • Password • Certificate • Password and certificate
App Product ID	Provide the product identity of the allowed or denied app. You can also view the app details from the Windows Phone Store using the link provided.

Setting	Description
Namespace	Define one or more namespaces so that all requests to the configured namespaces are secured over VPN. Otherwise, applications continue to connect directly. Define namespaces using this format: *.corp.contoso.com. Restrictions such as * or *.* or *.com.* are not allowed.
Networks	Set POLICIES/SPLITTUNNEL to true for IKEv2 profile. Define one or more IP a range so all traffic to these IP ranges is secured over VPN. Applications connecting to "protected resources" that match this list are secured over VPN. Otherwise, applications continue to connect directly to the VPN. Define IP ranges using this format: 10.0.0.0/8.
Proxy (Optional)	Choose Manual to set up a proxy server and enter the following details: • Select to enable the bypass proxy for local servers • Enter the server address • Set the port number
Policies > Connection Type	Choose the VPN connection type. The settings vary by connection type; for detailed information, see the vendor documentation for your specific implementation. • Triggering • Manual • Always On **i Note** Always On is supported by Windows Phone GDR2 and above.
Remember Credentials	Save the login credentials
Split Tunnel	Specifies whether the VPN connection allows split tunneling, which allows the user to access a public network directly rather than through the VPN server
Bypass for Local	Avoid any active proxies when accessing local resources
Trusted Network Detection	Automatically disconnect a VPN connection when the user is inside the corporate network (the trusted network), and reestablish the VPN connection when the user is outside the corporate network (the untrusted network)

2.23.4 Creating an Enrollment Policy for Windows Phone

Create an enrollment policy to enroll a Windows Phone device. The enrollment code URL used to enroll the device is generated automatically based on the enrollment server settings.

Prerequisites

Configure a certificate authority (CA) server, on the *Server* > *Configuration* > *Certificate Authority* page, for the device enrollment to work properly.

Context

The policy includes multiple pages, such as Summary and General. You can complete the pages in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Windows Phone*.
2. On the Summary panel, enter the policy name and a description for the policy.
   The MDM Enrollment URL that the users use to enroll the device is auto-generated based on the enrollment server settings on the *Server* > *Component* > *Enrollment Server* page. If the enrollment server is not configured, the user sees an error message.
3. On the General page, define the policy for enrolling devices.
   - New Device – if your server is configured on the *Server* > *Configuration* > *Server* > *Security* page to not automatically approve new devices, select this option to override the server configuration and automatically approve enrolling devices. If your server is configured for automatic approval, unselecting this option does not override the server setting.
   - If automatically creating a name for enrolling devices, select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for automatically naming the client. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. UserName is currently the only option available.
   - Certificate Renewal Alert Before – specify the number of days before certificate expiry that the renewal alert message appears on the device. The default value is 42 days and the minimum value is one day. When the device connects to the server, the user gets an attention prompt for certificate renewal, based on the number of days specified.

     > **i Note**
     >
     > For Windows Phone devices, certificate renewal does not happen if the CA server is SCEP-enabled. The user should reenroll the device, in this case.

- Certificate Key Size – select the certificate key size that the device uses for communicating with the CA server and also for enrollment. The default key size is 2048 bytes.
- Connection Schedule – define the frequency for an inbound connection schedule to connect to the Windows phone server. The default connection interval is eight hours.

4. On the Group page, select any groups to populate when devices enroll.

   A device receives the group's linked policies.

   Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of the group's definition criteria. If the device does not meet the group criteria, when the Dynamic Group Refresh schedule is executed, it is removed from the group.

5. (Optional) On the Variables page, click *Add* to select any variables to populate during enrollment. Users are prompted on the device during enrollment.

   Define the variable prompts:
   - Variable – select the variable from the database, to appear on the device for user response.
   - Device Prompt – enter the text for the user-facing prompt.
   - Entry Mask – indicate whether the entry at the device is masked with asterisk (*) characters as the user types.

> **i Note**
>
> The variable prompts, if configured, appear for user input only if the enrollment happens through the Self-Service Portal.

Enrollment Policy Settings [page 239]

2.23.4.1 Enrollment Policy Settings

Summary Settings [page 239]

General Settings [page 240]

Group Settings [page 177]

Variable Settings [page 177]

2.23.4.1.1 Summary Settings

Setting	Description
Policy	• Name of the policy
Note	• Description of the policy

Setting	Description
State	• State of the policy • Published policies are available for linking to devices and groups • Unpublished policies are not available
Last Modified	• Date when the policy was last modified
Type	• Type of the policy
OS	• Operating system to which the policy applies
MDM Enrollment	• Link that Windows Phone devices to enroll in SAP Afaria management
Enrollment Code	• Code that Windows Phone devices use to authenticate with the SAP Afaria Enrollment Server • Share this code with users prior to enrollment

2.23.4.1.2 General Settings

Setting	Description
New Device	• Whether SAP Afaria approves new devices automatically
Optional Prefix	• The prefix that SAP Afaria adds to device names • 512 characters is the limit
Data Column	• The data that SAP Afaria uses as device names • UserName is the default value
Certificate Renewal Alert Before	• The number of days prior to the expiry of the certificate that devices alert users • 42 days is the default value
Certificate Key Size	• The size of the certificate key that devices use for enrollment and to communicate with the certificate authority • 2048 bytes is the default value
Connect Every	• How often device must connect to SAP Afaria • 8 hours is the default value • 168 hours is the maximum value

2.23.4.1.3 Group Settings

Setting	Description
Available Groups	• List of available groups to which you can link the policy
Selected Groups	• List of groups to which the policy is already linked

2.23.4.1.4 Variable Settings

Setting	Description
Variable	• Information that the variable represents
Device Prompt	• Text that the device displays as a user prompt
Entry Mask	• Whether devices mask the value

2.24 Windows DM Policies

2.24.1 Creating an Enrollment Policy for Windows DM

Create an enrollment policy to enroll a Windows DM device in Afaria. The enrollment code for the device is generated automatically, based on the enrollment server settings.

Prerequisites

Configure a certificate authority (CA) server, on the *Server* > *Configuration* > *Certificate Authority* page.

Context

The policy includes multiple pages, such as Summary and General. Complete them in any order. To save changes on all pages, click *Save* at the top of any page.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Enrollment* > *Windows DM*.
2. On the Summary page, enter a description for the policy.

   The enrollment code is generated automatically based on the enrollment server settings.
3. On the General page, define the policy for enrolling devices.
   - New Device – if your server is configured on the *Server* > *Configuration* > *Server* > *Security* page to not automatically approve new devices, select this option to override the server configuration and automatically approve enrolling devices. If your server is configured for automatic approval, unselecting this option does not override the server setting.
   - If automatically creating a name for enrolling devices, select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for automatically naming the client. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. UserName is currently the only option available.
   - Certificate Renewal Alert Before – specify the number of days before certificate expiry that the renewal alert message appears on the device. The default value is 42 days and the minimum value is one day. When the device connects to the server, the user gets an attention prompt for certificate renewal, based on the number of days specified.
   - Certificate Key Size – select the certificate key size that the device uses to communicate with the CA server and also for enrollment. The default key size is 2048 bytes.
   - Connection Schedule – define the frequency for an inbound connection schedule to connect to the Windows DM server. The default connection interval is 8 hours.

     > **i Note**
     >
     > The connection interval is taken as eight hours, irrespective of the value you define here.
4. On the Group page, select any groups to populate when devices enroll.

   A device receives the group's linked policies.

   Selecting a dynamic group forces a newly enrolled device into the group without any evaluation of that group's definition criteria. Upon execution of the Dynamic Group Refresh schedule, if the device does not meet the group criteria, it is removed from the group.

2.24.2 Creating a Configuration Policy for Windows DM

Create a configuration policy to define the settings for MDM payloads, such as Certificate, SCEP, Passcode, and WiFi.

Context

A configuration policy includes multiple pages, such as Summary and MDM Payload. You can complete the pages in any order. To save changes on all pages, click Save at the top of any page.

Windows DM configuration policy supports directory substitution variables for certain fields.

Procedure

1. On the Policy page, on the top toolbar, click *New* > *Configuration* > *Windows DM*.
2. On the Summary page, enter the policy name, and enter or select the remaining properties.
   - Note – add a description for the policy.
   - State – indicate published or unpublished. Connecting devices receive only published policies.
   - Priority – set a user-defined value that determines which configuration policy prevails when multiple policies define the same default settings. The lower the numeric value, the higher the priority.
   - Inventory – select the inventory type to collect.You can view inventory information on the Device page's Device Inspector.
     - Do not collect inventory – no inventory collection.
     - Hardware only – collects data that is related to the device's physical components, such as processors and memory cards.
3. On the Certificate page, browse and upload the certificate for authenticating the Windows DM device.
4. On the Passcode page, define minimum password length, password expiration days, and other password characteristics.
5. On the SCEP page, configure the settings to allow devices to obtain certificates over the air from a certificate authority (CA) server that is using SCEP.
6. On the WiFi page, configure the settings for WiFi networks.

Windows DM Configuration Policy MDM Payloads [page 243]
Windows DM configuration policy MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and certificates for Windows DM devices.

2.24.2.1 Windows DM Configuration Policy MDM Payloads

Windows DM configuration policy MDM payload data allows you to manage device settings for items such as Wi-Fi, passwords, and certificates for Windows DM devices.

Certificate [page 244]
The Certificate payload uploads the root or intermediate certificate for Windows DM device authentication, and stores the certificate in the desired location.

Exchange ActiveSync [page 244]
The Exchange ActiveSync payload determines how Windows DM interacts with Microsoft Exchange servers.

Passcode [page 231]
The passcode payload defines the passcode requirements on the device.

WiFi [page 246]
The Wi-Fi payload configures connections to Wi-Fi networks on Windows DM devices.

SCEP [page 247]

The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

2.24.2.1.1 Certificate

The Certificate payload uploads the root or intermediate certificate for Windows DM device authentication, and stores the certificate in the desired location.

Setting	Description
Enabled	Whether Afaria can send the certificate payload to devices for authentication.
Store certificate in	Select the location in which to store the certificate: • User account – certificate store is available only to the specific user logged in to a device. • Computer account – certificate store is available to all users of the device.
Certificate type	Type of the certificate used for authentication: • Root – the root certificate from the certificate authority. • Intermediate – the intermediate certificate from the certificate authority.
Certificate	Browse and upload the certificate for authentication.
Issued to	The party to which the certificate is issued. This is automatically updated when the certificate is uploaded.
Expires on	Expiry date of the certificate. This is automatically updated when the certificate is uploaded.

2.24.2.1.2 Exchange ActiveSync

The Exchange ActiveSync payload determines how Windows DM interacts with Microsoft Exchange servers.

Setting	Description
Enabled	Whether SAP Afaria sends the Exchange ActiveSync payload to devices to add an Exchange ActiveSync account.
Name	The name of the Exchange ActiveSync payload.
Host	The host name or IP address of the Microsoft Exchange server.
Use SSL	Whether the Microsoft Exchange Server uses SSL.

Setting	Description
Domain Host	The host name or the IP address of the domain host.
User	The user name that devices use to authenticate with the Microsoft Exchange Server. If you do not define this setting, devices prompt users for it when the policy is applied.
Email Address	The email address for the account.
Password	(Optional) The password that devices use to authenticate with the Microsoft Exchange Server for encoded profiles.
Download new content	The time interval to download new content.
Download email from	The duration in days for which the emails are downloaded.
Email	Select to synchronize e-mail.
Contacts	Select to synchronize contacts.
Calendar	Select to synchronize calendar details.
Tasks	Select to synchronize task details.

2.24.2.1.3 Passcode

The passcode payload defines the passcode requirements on the device.

Setting	Description
Enabled	Whether SAP Afaria can send the passcode payload to devices.
Allow simple value	Whether a simple password, which contains repeated characters or character sequences, is permitted.
Require alphanumeric value	Whether the password requires letters as well as numbers.
Minimum passcode length	The minimum required length of the password.
Minimum number of complex characters	The minimum number of symbols required in the password.
Maximum passcode age	The maximum age of a password. When the password reaches the maximum age, the user must change it.
Auto lock	The period of time during which devices can be inactive before locking automatically.

Setting	Description
Passcode history	The number of unique passwords that must occur before a password can be repeated.
Maximum number of failed attempts	The number incorrect password attempts allowed before the device gets locked.

2.24.2.1.4 WiFi

The Wi-Fi payload configures connections to Wi-Fi networks on Windows DM devices.

Setting	Description
Enabled	Whether SAP Afaria can send the Wi-Fi payload to devices.
Select Service Set ID	The SSID of the Wi-Fi network.
Connection Mode	Whether connection to a wireless LAN should be automatic or initiated by user.
Auto Switch	(Optional) Determines the roaming behavior of an auto-connected network when a more preferred network is in range. This element is optional.
Hidden	Whether the Wi-Fi network is hidden.
Security Authentication Type	The security that the Wi-Fi network uses: • Open • WPA / WPA 2 Personal • WPA / WPA 2 Enterprise
Encryption	Encryption options are: • None • WEP • TKIP • AES The available encryption options differ, based on the security authentication type.
FIPS Mode	Indicates whether Federal Information Processing Standards (FIPS) mode is enabled. The FIPS Mode settings for the Wi-Fi network are available only for: • WPA 2 Enterprise (with AES)
Trust	The Trust settings for the Wi-Fi network, available for: • WPA / WPA 2 Enterprise

Setting	Description
PMK Cache	The Trust settings for the Wi-Fi network, available for: • WPA 2 Enterprise • The PMKCacheMode element indicates whether PMK caching will be used. • The PMKCacheTTL element indicates the length of time, in minutes, that a PMK cache is kept. • The PMKCacheSize element specifies the number of entries in the PMK cache on the client. • The Pre Auth Mode element indicates whether pre-authentication is used by the client. • The Pre Auth Throttle element specifies the number of preauthentication attempts to try on neighboring access points.

Supported Wi-Fi Combinations

Connection Type	Connection Mode	Security Authentication Type	Encryption
ESS	Manual	Open	None
		Open	WEP
		Shared	None
		Shared	WEP
		WPAPSK	TKIP
		WPA2PSK	TKIP
		WPAPSK	AES
		WPA2PSK	AES

2.24.2.1.5 SCEP

The SCEP payload configures settings that allow devices to obtain certificates over the air from a certificate authority (CA) server that uses SCEP (Simple Certificate Enrollment Protocol).

> **i Note**
>
> If the Windows DM device is enrolled in one domain and SCEP is on another domain, then the SCEP policy will not be pushed to the device.

Setting	Description
Enabled	Whether SAP Afaria can send the SCEP payload to devices
CA	The certificate authority that processes the SCEP requests.
Store Location	Select the location in which to store the certificate: • User account – certificate store is available only to the specific user logged in to a device. • Computer account – certificate store is available to all users of the device.
Subject Name	The name to which the certificate is to be issued by the CA. The allowed values are: • An email address • Substitution variable • %s.UserName% • %s.EUSSPUser% (works only if the enrollment happens through Self-Service Portal)
Use as Digital Signature	Whether devices use the certificates from the SCEP requests as digital signatures.
Use for Encryption	Whether devices use the certificates from the SCEP requests to encrypt keys.
Key Protection	Indicate where to store the encrypted key details: • Install to TPM_Fail If Not Present • Install to TPM if Present • Install to Software Key Storage Provider
Key Length	The size of the key in bits: • 512 • 1024 • 2048
Retry Count	The number of times that the device attempts the SCEP request.
Retry Delay	The amount of time that must elapse before the device retries the SCEP request.
Fingerprint	The fingerprint for the SCEP request. You can create a fingerprint from a certificate. The fingerprint should be of the root certificate of the CA server that issues the certificate to the device.

3 Access Control

Access control regulates synchronization requests to email servers.

Access Control can prevent synchronization requests that do not meet the access control policies in SAP Afaria. Access control policies include a list of known devices, their associated policies, any remediation actions, and any defined polices for unknown devices.

In addition to synchronization requests from devices, Access Control Filter can regulate synchronization requests from desktop and Web email clients.

3.1 Default Access Control Policies

Access control policies define the conditions that devices must meet to connect to messaging servers in an organization.

Access control policies can apply to both known and unknown devices.

Administrators should communicate access control policies to users to establish accurate expectations towards device synchronization and compliance.

Define a default access control policy for a local email to manage e-mail synchronization for devices that do not enroll in SAP Afaria management.

Creating Access Control Policies for Domains [page 254]
: You can create an access control policy in the Afaria Administration console to regulate synchronization requests to specific domains.

Creating Access Control Policies for Groups [page 255]
: You can create an access control policy in the Afaria Administration console to regulate synchronization requests from groups.

Access Control Device List [page 256]
: SAP Afaria displays access control devices and policy assignments in different locations of the Afaria Administration console, depending upon the device type.

Viewing Access Control Information for Devices [page 256]
: You can view access control information for devices in the Afaria Administration console.

3.1.1 Creating Access Control Policies for Android Devices

You can create an access control policy in the Afaria Administration console to regulate synchronization requests from Android devices.

Context

To use access control to manage email on an Android device, ensure the Exchange account is configured through SAP Afaria. Email from unmanaged accounts is blocked by default. For Samsung devices with KNOX installed, provision the Exchange account through the Samsung KNOX Email Account configuration policy. For devices using NitroDesk TouchDown, use the NitroDesk Account configuration policy; for other devices, use the appropriate LG or Samsung KNOX Standard Exchange account configuration policy.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click *Access Policy* > *Android*.
4. Perform one of the following tasks:
   a. To allow synchronization requests, select *Always allow*.
   b. To block synchronization requests, select *Always block*.
   c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.
5. If you select *Allow when*, perform at least one of the following tasks:
   a. To allow synchronization requests from devices that have the SAP Afaria client installed and granted administrator privileges, select *Afaria setting enabled*.

b. To allow synchronization requests from devices with a password policy, select *Password Policy Enabled*.
c. To allow synchronization requests from devices that are not rooted, select *Device uncompromised*.
d. To allow synchronization requests from devices that have connected within a period of time, select *Device connected within* and set the period of time.

6. Click *Save*.

3.1.2 Creating Access Control Policies for iOS Devices

You can create an access control policy in the Afaria Administration console to regulate synchronization requests from iOS devices.

Context

Access control policies are prioritized in this order: group-level policy, device-level policy, server-level policy.

> **i Note**
>
> The iOS access control policy is not applied to a newly enrolled iOS device until 60 minutes after the first connection. This grace period allows time for the device to complete enrollment and for the server to synch all settings. After 60 minutes, the server processes incoming synchronization requests from the device according to your access control settings.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click *Access Policy* > *iOS*.
4. Perform one of the following tasks:
   a. To allow synchronization requests, select *Always allow*.
   b. To block synchronization requests, select *Always block*.
   c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.
5. If you select *Allow when*, perform at least one of the following tasks:
   a. To allow synchronization requests from devices that are under SAP Afaria MDM management, select *Administered by mobile device management*.
   b. To allow synchronization requests from devices that have the SAP Afaria client installed and have connected within a period of time, select *Afaria installed and device connected within* and set the period of time.
   c. To allow synchronization requests from devices that have received policies within a period of time, select *Assigned policy delivered within* and set the period of time.

d. To allow synchronization requests from devices that use hardware encryption, select *Device hardware encrypted*.
e. To allow synchronization requests from devices that are not jailbroken, select *Device uncompromised*.

6. Click *Save*.

3.1.3 Creating Access Control Policies for Windows Mobile Devices

You can create an access control policy in the Afaria Administration console to regulate synchronization requests from Windows Mobile devices.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click *Access Policy* > *Windows Mobile*.
4. Perform one of the following tasks:
   a. To allow synchronization requests, select *Always allow*.
   b. To block synchronization requests, select *Always block*.
   c. To allow synchronization requests from devices that have connected within a period of time, select *Allow when connected within time frame* and set the period of time.
5. Click *Save*.

3.1.4 Creating Access Control Policies for Windows Phone Devices

You can create an access control policy in the Afaria Administration console to regulate synchronization requests from Windows Phone devices.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click *Access Policy* > *Windows Phone*.
4. Perform one of the following tasks:

a. To allow synchronization requests, select *Always allow*.
b. To block synchronization requests, select *Always block*.
c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.

5. If you select *Allow when*, perform at least one of the following tasks:
   a. To allow synchronization requests when devices are under SAP Afaria MDM management, select *Administered by mobile device management*.
   b. To allow synchronization requests when devices have connected within a period of time, select *Device connected within* and set the period of time.
6. Click *Save*.

3.1.5 Creating Access Control Policies for Unknown Devices

Define a default access control policy for a local email to manage e-mail synchronization for devices that do not enroll in SAP Afaria management.

Context

You are advised to define an unknown device policy for each domain managed by your e-mail server.

> **i** Note
>
> For cloud implementation on the unknown devices the connection is rejected.

Procedure

1. On the Home page Server tile, click *Configuration* to open the Server Configuration page.
2. Navigate to the *Component* > *Access Control Option* page.
3. Click the *Domains* tab.
4. Click *Add* to define unknown device properties.
5. Enter the e-mail server's domain.
6. Select the default policy for that domain.
7. Define the interval at which the SAP Afaria ISAPI filter's polling agent queries the SAP Afaria server for a list of known devices and policies.
8. In the inline editor row, click the *Check* icon to save.

3.1.6 Creating Access Control Policies for Domains

You can create an access control policy in the Afaria Administration console to regulate synchronization requests to specific domains.

Context

Access control policies for domains can regulate synchronization requests from devices that are unknown to SAP Afaria.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option* .
3. Click *Domains*.
4. Click *Add*.
5. In the *Primary Domain* tab, type the domain.
6. In the *Access Control Policy* list, select how SAP Afaria responds to synchronization requests to the domain.
7. In the *Retry Rate* field, select the interval that SAP Afaria enforces between synchronization requests.
8. In the *Accepted Domains*, specify the subdomains that the primary domain includes.
9. Click *Save*.

3.1.6.1 Primary and Accepted Domains

This section discusses couple of primary domain and accepted domains scenarios.

Scenario 1: CAS 1 on one network domain and CAS 2 and CAS 3 are on a different network domain

CAS A runs on domain domainA.com, services domains A.com, AA.com, and AAA.com.

CAS B runs on domain domainB.com, services domains B.com, BB.com, and BBB.com.

CAS C runs on domain domainB.com, services domains C.com, CC.com, and CCC.com.

A primary domain maps to the network domain on which the server resides. The accepted domain list includes all supported e-mail domains. Therefore, this scenario has two primary domains on the *Server* > *Configuration* > *Access Control Option* page:

- One primary domain for domainA.com with accepted domains A.com, AA.com, and AAA.com.
- One primary domain for domainB.com with accepted domains B.com, BB.com, BBB.com, C.com, CC.com, and CCC.com.

Scenario 2: CAS 1, CAS 2, and CAS 3 on different network domains

CAS A runs on domain domainA.com, services domains A.com, AA.com, and AAA.com.

CAS B runs on domain domainB.com, services domains B.com, BB.com, and BBB.com.

CAS C runs on domain domainC.com, services domains C.com, CC.com, and CCC.com.

A primary domain maps to the network domain on which the server resides. The accepted domain list includes all supported e-mail domains. Therefore, this scenario has three primary domains on the *Server* > *Configuration* > *Access Control Option* page:

- One primary domain for domainA.com with accepted domains A.com, AA.com, and AAA.com.
- One primary domain for domainB.com with accepted domains B.com, BB.com, and BBB.com.
- One primary domain for domainC.com with accepted domains C.com, CC.com, and CCC.com.

3.1.7 Creating Access Control Policies for Groups

You can create an access control policy in the Afaria Administration console to regulate synchronization requests from groups.

Context

Blocking and allowing by groups can let you block devices that do not meet some criteria, or allow devices that meet some criteria. You define dynamic group with your criteria to use with this feature.

The frequency of the Dynamic Group Refresh schedule, access control polling interval, and device inventory reporting all affect when a group policy goes into effect on a device.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.

3. Click *Groups*.
4. To block synchronization requests from groups, perform the following tasks in the *Block selected groups* section:
   a. In the *Available Groups* list, select a group.
   b. Click the arrow to add the group to the *Selected Groups* list.
5. To only allow synchronization requests from selected groups, perform the following tasks in the *Only allow selected Groups* section:
   a. Select *Enable*.
   b. In the *Available groups* list, select a group.
   c. Click the arrow to add the group to the *Selected Groups* list.
6. Click *Save*.

3.1.8 Access Control Device List

SAP Afaria displays access control devices and policy assignments in different locations of the Afaria Administration console, depending upon the device type.

Assignment locations include:

- Android, Windows Mobile, and Windows Phone – *Access Control Option* > *Devices* page tab.
  On the Devices tab, the device list shows devices and white list devices that are access control devices. The SAP Afaria server populates this list with devices after it assigns a synchronization policy to a connecting device. White list devices populate the list as you add them. Therefore, the list starts empty and grows as each device connects and receives its synchronization policy assignment, and as you manually add devices.

  > **i Note**
  >
  > When an Android device does not contain a known ActiveSync ID or an Exchange User ID, Access Control ID displays the value NOT_EXCHANGE followed by the client GUID.

- iOS – Device List page

3.1.9 Viewing Access Control Information for Devices

You can view access control information for devices in the Afaria Administration console.

Procedure

1. On the *Devices* page, select a device.
2. Click the *Show/Hide Inspector* icon.

The Device Inspector displays the following information about access control:

- Access control policy that is applicable to the device
- Current access policy state for the device: allowed or blocked
- Device compliance state: Whether the device is compliant or not
- Last remediation timestamp for the device

3.2 Custom Access Control Policies

Adding Android Devices to Access Control [page 257]
You can add Android devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Adding Windows Mobile Devices to Access Control [page 258]
You can add Windows Mobile devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Adding Windows Phone Devices to Access Control [page 259]
You can add Windows Phone devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Adding iOS Devices to Access Control [page 260]
You can edit the access control policies for iOS devices in the Afaria Administration console.

Editing Custom Access Control Policies [page 261]
You can edit access control policies .

Exchange Environment Unique Device ID Value [page 261]
For access control in a Microsoft Exchange environment, the unique device ID value is the DeviceID value stored in the device registry.

3.2.1 Adding Android Devices to Access Control

You can add Android devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Context

You should add devices when:

- Devices synchronize with your email server but are not managed by SAP Afaria.
- Devices will connect to the email server in the future and you want to make sure that the default access control policy does not prevent synchronization requests.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Devices* tab.
4. Click *Add*.
5. In the *Device* field, type the Exchange environment unique device identifier of the device.
6. In the *User Name* field, type the Exchange user name.
7. In the *Domain*, type the Exchange domain.
8. In the *OS* list, select *Android*.
9. In the *Access control policy* list, perform one of the following tasks:
    a. To allow synchronization requests, select *Always allow*.
    b. To block synchronization requests, select *Always block*.
    c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.
10. If you select *Allow when*, perform at least one of following tasks:
    a. To allow synchronization requests from devices that have the SAP Afaria client installed and granted administrator privileges, select *Afaria setting enabled*.
    b. To allow synchronization requests from devices with a password policy, select *Password Policy Enabled*.
    c. To allow synchronization requests from devices that are not rooted, select *Device uncompromised*.
    d. To allow synchronization requests from devices that have connected within a period of time, select *Device connected within* and set the period of time.
11. Click *Save*.

3.2.2 Adding Windows Mobile Devices to Access Control

You can add Windows Mobile devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Context

You should add devices when:

- Devices synchronize with your email server but are not managed by SAP Afaria.
- Devices will connect to the email server in the future and you want to make sure that the default access control policy does not prevent synchronization requests.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Devices* tab.
4. Click *Add*.
5. In the *Device* field, type the Exchange environment unique device identifier of the device.
6. In the *User Name* field, type the Exchange user name.
7. In the *Domain*, type the Exchange domain.
8. In the *OS* list, select *Windows Mobile*.
9. In the *Access control policy* list, perform one of the following task:
    a. To allow synchronization requests, select *Always allow*.
    b. To block synchronization requests, select *Always block*.
    c. To allow synchronization requests from devices that have connected within a period of time, select *Allow when connected within time frame*.
10. Click *Save*.

3.2.3 Adding Windows Phone Devices to Access Control

You can add Windows Phone devices that are not enrolled in SAP Afaria to access control in the Afaria Administration console.

Context

You should add devices when:

- Devices synchronize with your email server but are not managed by SAP Afaria.
- Devices will connect to the email server in the future and you want to make sure that the default access control policy does not prevent synchronization requests.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Devices* tab.
4. Click *Add*.
5. In the *Device* field, type the Exchange environment unique device identifier of the device.
6. In the *User Name* field, type the Exchange user name.

7. In the *Domain*, type the Exchange domain.
8. In the *OS* list, select *Android*.
9. In the *Access control policy* list, perform one of the following task:
    a. To allow synchronization requests, select *Always allow*.
    b. To block synchronization requests, select *Always block*.
    c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.
10. If you select *Allow when*, perform at least one of the following task:
    a. To allow synchronization requests from devices that have connected within a period of time, select *Device connected within time frame*.
    b. To allow synchronization requests from devices with a password policy, select *Password policy enabled*.
11. Click *Save*.

3.2.4 Adding iOS Devices to Access Control

You can edit the access control policies for iOS devices in the Afaria Administration console.

Context

> **i** Note
>
> The iOS access control policy is not applied to a newly enrolled iOS device until 60 minutes after the first connection. This grace period allows time for the device to complete enrollment and for the server to synch all settings. After 60 minutes, the server processes incoming synchronization requests from the device according to your access control settings.

Procedure

1. On the *Device* page, select a device.
2. Click *Edit*.
3. In the *Access Control Policy* field, click *Setup*.
4. Perform one of the following tasks:
    a. To apply the default access control policy to the device, select *Use default policy*.
    b. To create a custom access control policy for the device, select *Use explicit policy* .
5. In you select *Use explicit policy*, perform one of the following tasks:
    a. To allow synchronization requests, select *Always allow*.
    b. To block synchronization requests, select *Always block*.
    c. To allow synchronization requests when devices meet specific criteria, select *Allow when*.
6. If you select *Allow when*, perform at least one of following tasks:

a. To allow synchronization requests from devices that are under SAP Afaria MDM management, select *Administered by mobile device management*.
b. To allow synchronization requests from devices that have the SAP Afaria client installed, select *Afaria installed*.
c. To allow synchronization requests from devices that have received policies, select *Assigned policy delivered*.
d. To allow synchronization requests from devices that use hardware encryption, select *Device hardware encrypted*.
e. To allow synchronization requests from devices that are not jailbroken, select *Device uncompromised*.

7. Click *Ok*.
8. Click *Save*.

3.2.5 Editing Custom Access Control Policies

You can edit access control policies .

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option* >.
3. Click *Devices*.
4. Select one or more devices on the managed device list.
5. Click *Edit*.
6. Select new policy and click the *Save* icon.

3.2.6 Exchange Environment Unique Device ID Value

For access control in a Microsoft Exchange environment, the unique device ID value is the DeviceID value stored in the device registry.

You can obtain the value from a device if it has already connected to the Exchange server. SAP Afaria cannot retrieve the value if the SAP Afaria client is not installed on the device. You can use your own method to retrieve the value or:

- Use a device utility to read the value.
- Use your Exchange Server ActiveSync Web Administration tool to run a query that retrieves the value. Choose the *Remote Device Wipe* menu option and query for the user of interest. The query returns information about the devices associated with the user. Copy the value from the Device ID column and exit the page without initiating any further action.

3.3 Access Control Policy Conflict Resolution

When a device is subject to more than one access control policy, the most restrictive policy takes precedence.

> **Example**
>
> For example, if an Android device is subject to a default policy for Android that allows access, and a group policy that blocks access, then the device is blocked from synchronizing with the e-mail server.

3.4 Troubleshooting

Troubleshoot issues related to access control.

- If a device is not receiving e-mail, track down the relevant entries in the log file and in the Devices.xml file, and:
  1. Make sure that the ActiveSync IDs (ASIDs) in the files `C:\Windows\System32\config\systemprofile\AppData\Roaming\Devices.xml` and `C:\Windows\System32\config\systemprofile\AppData\Roaming\NewDevices.xml` match.
  2. Verify that the Exchange account information in both the files agree.
  3. Ensure the device is not being blocked because SAP Afaria believes it to be out of compliance with policy.

  To manage access control for an Android device, proper ASID must appear in the *Server* > *Configuration* > *Component* > *Access Control Option* > *Device* tab.

  > **Note**
  >
  > NOT_EXCHANGE is not treated as an ASID of the device. If the device reports NOT_EXCHANGE, unknown policy will be applied on the Android device.

  If an Android device reports NOT_EXCHANGE, perform the following steps:

  1. Delete the device record from the *Server* > *Configuration* > *Component* > *Access Control Option* > *Device* tab.
  2. Wait for the polling time set on the *Server* > *Configuration* > *Component* > *Access Control Option* > *Domain* page.
  3. Follow the steps mentioned in the topic *Manually Configuring an E-mail Application for Android Devices While Using an Access Control Policy*.
- The Messages log entry that access control generates when it does not find a matching device in the Microsoft Exchange email server for a given Afaria device, with code "BPOS0032" and text "... cannot find mailbox... " is retyped from error to informational. Therefore, instance of not matching a device during processing will not add to the error count on the Home page, but are still available in the log for investigation.

4 Remediation Policies

Remediation policies define the conditions of compliance and the actions that SAP Afaria takes when devices go out of compliance.

You create remediation policies in the Afaria Administration console to apply to tenants in SAP Afaria.

4.1 Defining Remediation Policies for Android Devices

Define the remediation policy and remediation actions for Android devices that go out of compliance.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Remediation Policy* tab.
4. Click the *Android* tab.
5. To define the conditions of compliance, perform the following tasks in the *Remediation Policy* pane:
   a. To make devices non-compliant if users remove administrator privileges for SAP Afaria on devices, select the *Administrator setting disabled* check box.
   b. To make devices non-compliant if users ignore the password prompt when connecting devices to SAP Afaria, select the *Password policy disabled* check box.
   c. To make devices non-compliant if users root devices, select the *Device compromised* check box.
   d. To make devices non-compliant if users are in a blocked group, select the *Device in blocked group* check box.

e. To make device non-compliant if users are not in an allowed group, select the *Device not in selected group* check box.
f. To make devices non-compliant if devices have not connected to SAP Afaria within a specific time, select the *Device not connected within* check box and define the time period in the *days* and *hours* boxes.

6. To define the actions that SAP Afaria takes when devices are not compliant, perform the following tasks in the *Remediation Action* pane:
   a. To wipe email from NitroDesk on devices, select *Remote Wipe Email*.
   b. To remove the KNOX container on Samsung devices, select *Remove KNOX Container*.
   c. To send a message to users, select *Send message to client when device remediated*. Select the type of message and type a subject and the text for the message.
7. To send a message to users when devices become compliant again, select *Send message to client when device becomes compliant* in the *Re-compliant Message Settings* pane. Select the type of message, and type a subject and text for the message.
8. Click *Save*.

4.2 Defining Remediation Policies for iOS devices

Define the remediation policy and remediation actions for iOS devices that go out of compliance.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option* >.
3. Click the *Remediation Policy* tab.
4. Click the *iOS* tab.
5. To define the conditions of compliance, perform the following tasks in the *Remediation Policy* pane:
   a. To make devices non-compliant if users remove the MDM payload from device, select the *Mobile device management payload removed* check box.
   b. To make devices non-compliant if devices have not connected to SAP Afaria within a specific time, select the *Device not connected within* check box and define the time period in the *days* and *hours* boxes.
   c. To make devices non-compliant if SAP Afaria cannot deliver assigned policies to devices, select the *Assigned policy not delivered* check box.
   d. To make devices non-compliant if encryption is not active on devices, select the *Device hardware not encrypted* check box.
   e. To make devices non-compliant if users jailbreak devices, select the *Device compromised* check box.
   f. To make devices non-compliant if users are in a blocked group, select the *Device in blocked group* check box.
   g. To make device non-compliant if users are not in an allowed group, select the *Device not in selected group* check box.

6. To define the actions that SAP Afaria takes when devices are not compliant, perform the following tasks in the *Remediation Action* pane:
    a. To remove the SAP Mobile Docs application from devices, select the *Remove SAP Mobile Docs* check box.
    b. To remove the SAP Afaria MDM management from devices, select the *Remove control* check box.
    c. To send a message to users, select *Send message to client when device remediated*. Select the type of message and type a subject and the text for the message.
7. To send a message to users when devices become compliant again, select *Send message to client when device becomes compliant* in the *Re-compliant Message Settings* pane. Select the type of message, and type a subject and text for the message.
8. Click *Save*.

4.3 Defining Remediation Policies for Windows Phone Devices

Define the remediation policy and remediation actions for Windows Phone devices that go out of compliance.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Remediation Policy* tab.
4. Click the *Windows Phone* tab.
5. To define the conditions of compliance, perform the following tasks in the *Remediation Policy* pane:
    a. To make devices non-compliant if devices are not under SAP Afaria MDM management, select the *Device not administered by mobile device management* check box.
    b. To make devices non-compliant if devices have not connected to SAP Afaria within a specific time, select the *Device not connected within* check box and define the time period in the *days* and *hours* boxes.
    c. To make devices non-compliant if users are in a blocked group, select the *Device in blocked group* check box.
    d. To make device non-compliant if users are not in an allowed group, select the *Device not in selected group* check box.
6. To define the actions that SAP Afaria takes when devices are not compliant, perform the following tasks in the *Remediation Action* pane:
    a. To remove the SAP Afaria MDM management from devices, select the *Remove control* check box.
    b. To send a message to users, select *Send message to client when device remediated*. Select the type of message and type a subject and the text for the message.
7. To send a message to users when devices become compliant again, select *Send message to client when device becomes compliant* in the *Re-compliant Message Settings* pane. Select the type of message, and type a subject and text for the message.

8. Click *Save*.

4.4 Defining Remediation Policies for Windows DM Devices

Define the remediation policy and remediation actions for Windows DM devices that go out of compliance.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Access Control Option*.
3. Click the *Remediation Policy* tab.
4. Click the *Windows DM* tab.
5. To define the conditions of compliance, perform the following tasks in the *Remediation Policy* pane:
   a. To make devices non-compliant if an anti-virus solution is not active on devices, select the *Anti Virus Status is off* check box.
   b. To make devices non-compliant if a firewall solution is not active on devices, select the *Firewall Status is off* check box.
   c. To make devices non-compliant if encryption is not active on devices, select the *Device hardware not encrypted* check box.
   d. To make devices non-compliant if devices have not connected to SAP Afaria within a specific time, select the *Device not connected within* check box and define the time period in the *days* and *hours* boxes.
   e. To make devices non-compliant if users are in a blocked group, select the *Device in blocked group* check box.
   f. To make device non-compliant if users are not in an allowed group, select the *Device not in selected group* check box.
6. To define the actions that SAP Afaria takes when devices are not compliant, perform the following tasks in the *Remediation Action* pane:
   a. To remove the SAP Afaria MDM management from devices, select the *Remove control* check box.
   b. To send a message to users, select *Send message to client when device remediated*. Select the type of message and type a subject and the text for the message.
7. To send a message to users when devices become compliant again, select *Send message to client when device becomes compliant* in the *Re-compliant Message Settings* pane. Select the type of message, and type a subject and text for the message.
8. Click *Save*.

4.5 Viewing Device Compliance

View device compliance using the Device inspector in the Afaria Administration console

Procedure

1. On the *Devices* page, select a device.
2. Click *Device Inspector*.

5 Unmatched Email Devices

Unmatched devices are devices that connect to an organization's Microsoft Exchange servers but SAP Afaria either does not manage the devices or does not have enough information to match the devices with devices that are managed by SAP Afaria.

SAP Afaria examines device data from the Microsoft Exchange servers and compares the Microsoft Exchange device records to the devices that are SAP Afaria. SAP Afaria uses either directory variables (for integrated AD or LDAP security) or system variables added to enrollment policies to collect device data. Based on the comparison, SAP Afaria classifies the devices into three categories.

- Matched devices are devices where there is a complete match between the Microsoft Exchange device record and the device record in SAP Afaria. For a match, SAP Afaria needs to know the email identity (the email user and the ActiveSync ID) of the device. Matched devices are enrolled with and managed by SAP Afaria, so they do not appear in the unmanaged devices list.
- Indeterminate devices are devices where there is a partial match between the data in Microsoft Exchange servers and the data in SAP Afaria.
- Unmatched devices are devices where there is no match between the data in Microsoft Exchange and SAP Afaria.

Device Matches [page 269]
SAP Afaria can identify two types of matches with devices associated with a Microsoft Exchange Server: deterministic and ambiguous.

Adding Microsoft Exchange Client Access Servers [page 269]
You can add Microsoft Exchange Client Access Server (CAS) connections in the Afaria Administration console. SAP Afaria retrieves device records from CAS servers and compares those records to the devices under SAP Afaria management.

Allowing Ambiguous Matches [page 270]
You can use the Afaria Administration console to allow SAP Afaria to make ambiguous matches automatically between device records in Microsoft Exchange and device records in SAP Afaria.

Matching Email Devices [page 271]
You can manually match a device record in Microsoft Exchange with a device record in SAP Afaria using the Afaria Administration console.

Resetting Email Identities [page 271]
You can remove the match between a device record in Microsoft Exchange and a device record in SAP Afaria using the Afaria Administration console. Resetting the email identity clears the device distinguished name.

5.1 Device Matches

SAP Afaria can identify two types of matches with devices associated with a Microsoft Exchange Server: deterministic and ambiguous.

Match	Description
Deterministic	• Match between a Microsoft Exchange device record and an SAP Afaria device record • SAP Afaria knows both the email user and ActiveSync ID data of the device • SAP Afaria makes deterministic matches automatically
Ambiguous	• Partial match between a Microsoft Exchange device record and an SAP Afaria device record • SAP Afaria does not know the ActiveSync ID of the device • SAP Afaria knows the email user data (the device has connected to Microsoft Exchange) • SAP Afaria can make some ambiguous matches automatically • SAP Afaria attempts to match device IMEI first and device OS second

5.2 Adding Microsoft Exchange Client Access Servers

You can add Microsoft Exchange Client Access Server (CAS) connections in the Afaria Administration console. SAP Afaria retrieves device records from CAS servers and compares those records to the devices under SAP Afaria management.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Server* > *MS Exchange* .
3. Click *Add*.
4. In the *List View* field, select whether the CAS server appears in the list view.
5. In the *Remote* field, select whether the CAS server is available for access control remote.
6. In the *MS Exchange CAS URL* field, type the URL of the CAS server.
7. In the *Domain* field, select one of the following options:
   - *Local* includes only the domain on which the CAS is located.
   - *Global* includes the subdomains of the domain on which the CAS is located.

8. In the *Account User* field, type the user name for the Microsoft Exchange administration account.
9. In the *Password* field, type the password for the Microsoft Exchange administration account.
10. To test the connection to the Microsoft Exchange Server, click *Test connection*.
11. To save the CAS server settings, click the green check mark.
12. To allow SAP Afaria to make ambiguous matches with unmatched email devices automatically, select *Allow Afaria to make matches on ambiguous devices*.
13. Click *Save*.

5.3 Allowing Ambiguous Matches

You can use the Afaria Administration console to allow SAP Afaria to make ambiguous matches automatically between device records in Microsoft Exchange and device records in SAP Afaria.

Context

When you allow automatic ambiguous matching, SAP Afaria begins making ambiguous matches when all deterministic matches are complete. SAP Afaria cycles through the list of unmatched email devices, automatically matches devices, removes the Microsoft Exchange device record from the unmatched devices list, and retains the device distinguished name. SAP Afaria continues to cycle through the updated list until it makes all of the ambiguous matches.

Allowing ambiguous matching can increase the time it takes SAP Afaria to process connections to CAS servers.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Server* > *MS Exchange*.
3. Select *Allow Afaria to make matches on ambiguous devices*.
4. Click *Save*.

5.4 Matching Email Devices

You can manually match a device record in Microsoft Exchange with a device record in SAP Afaria using the Afaria Administration console.

Context

You need to manually match an email device if there is an incorrect or missing value for the email user in SAP Afaria (for example, if the enrollment policy did not include the ExchangeUser variable), or if you reset the email identity to remove an incorrect match. After you match a device, SAP Afaria removes the Microsoft Exchange device record from the unmatched devices list and retains the device distinguished name.

You can reverse a match by resetting the email identity of the device.

Procedure

1. On the *Devices* page, click *Unmatched Email Device*.
2. (Optional) You can use the *State* column to filter for indeterminate or unmatched devices.
3. Select a Microsoft Exchange device record.
4. Click *Resolve*.
5. In the *Resolve Email Identity* window, select the SAP Afaria record to match with the Microsoft Exchange device record.
6. Click *OK, Resolve*.

5.5 Resetting Email Identities

You can remove the match between a device record in Microsoft Exchange and a device record in SAP Afaria using the Afaria Administration console. Resetting the email identity clears the device distinguished name.

Context

You need to reset the email identity of a device if you or SAP Afaria matched a device incorrectly. If you reset an email identity from an ambiguous match that SAP Afaria, you might need to match the device manually to prevent the same incorrect match.

Procedure

1. On the *Devices* page, select a device.
2. Click *Reset Email Identity*.
3. In the *Reset Email Identity* window, click *Reset*.

6 Device Enrollment

Enrollment is adding devices to Afaria device management. Enrollment is complete when a device has connected to its Afaria and received policies.

Use enrollment policies, enrollment codes, enrollment code URLs, Afaria applications, and the Self-Service Portal to enroll devices. The availability and use of the enrollment options varies by device type.

Enrollment codes simplify connecting a device to Afaria for enrollment. The codes are short codes that are easy for users to enter on the Afaria client on their device. You can communicate enrollment codes to users directly or they can get an enrollment code from the Self-Service Portal.

Windows Devices [page 287]
: Windows devices have an installed application for SAP Afaria management, as deployed by your organization.

Windows Device Enrollment [page 291]
: Windows (Windows DM) devices provide a built-in device management client that communicates with the SAP Afaria server. These devices can be enrolled in management either from the Self-Service Portal by activating the enrollment code, or directly from the device using domains.

Windows Mobile Devices [page 293]
: Windows Mobile devices have an installed application for SAP Afaria management, as deployed by your organization. “Windows Mobile” is a general reference to Windows Mobile Professional, Windows Mobile Standard, and Windows CE device types.

Windows Phone Device Enrollment [page 296]
: Windows Phone devices include a built-in device management client that communicates with the Afaria server. Enroll devices using the enrollment URL that you obtain from the Self-Service Portal or that the administrator distributes.

Approving Devices [page 300]
: Approve devices that are in an unapproved state so they can be managed with policies on future connections. Unapprove devices to discontinue management.

6.1 Device Enrollment Options

SAP Afaria supports the following enrollment options for devices.

Option	Android	iOS	Windows	Windows CE	Windows Mobile	Windows Phone	Windows DM
Enrollment codes	•	•			•	•	
Self-Service Portal	•	•			•	•	•
Custom installations			•	•	•		

6.2 SAP Afaria Client Sources

The SAP Afaria client is available from the following sources.

Source	Android	iOS	Windows	Windows CE	Windows Mobile	Windows Phone
Application market	•	•				
Enrollment Policy			•	•	•	
Enterprise Application		•				•

6.3 Enrollment Codes

Enrollment codes simplify connecting a device to SAP Afaria for enrollment. Enrollment codes are available for Android, iOS, Windows Phone, and Windows Mobile devices.

The codes are short codes that are easy for users to enter on the SAP Afaria client on their device. You can communicate enrollment codes to users directly or they can get an enrollment code from the Self-Service Portal. The user interface and the provisioning details you defined in the enrollment policy drives the rest of the interaction.

Create one or more enrollment codes when creating enrollment policies. Each code has its own attributes for an optional expiration date, use with Self-Service Portal, and its enabled or disabled state.

The enrollment code for Windows Phone consists of a URL, automatically generated when you create an enrollment policy for Windows Phone. The users can get the URL directly from the administrator or they can get it from the Self-Service Portal.

6.4 Device Enrollment with the SAP Afaria Client

Users install the Afaria application directly on the device. The device can be configured to connect to the Afaria server via an enrollment code created as part of an Afaria server enrollment policy. If you did not use an enrollment policy to provision the device, you need to configure the device settings directly after installation.

Afaria is supported on these device types:

- Android
- iOS
- Windows Mobile Professional

- Windows Mobile Standard

The following is a general overview of how users enroll their devices using the SAP Afaria client:

- Users access the Afaria Self-Service Portal using the browser on the enrolling device, from a personal computer, or by administrators sending enrollment codes to devices.
- Within the portal, the device owner downloads the SAP Afaria client for the device type they are enrolling, and obtain the device's enrollment code for entry on the device. The portal is tied to an SAP Afaria server enrollment policy for each device type, the policy configuration allows you to download the SAP Afaria client from within the portal (based on device type).
- The portal also provides an enrollment code for use by the end user to enter into the SAP Afaria client once installed on the device in order to complete the device enrollment process.
- After a user enters an enrollment code in the SAP Afaria client on the device, the client contacts a public URL shortening service to get an expanded address, then connects to that address. The expanded address is for connecting a device to an Afaria enrollment server, or its relay server proxy, to enroll in device management with the Afaria server.

> **i** Note
>
> Windows Phone uses the enrollment code URL, obtained from the Self-Service Portal, to enroll the device. During enrollment, the Afaria client is silently installed on the device.

iOS device end users have the ability to download the Afaria from:

- Apple App Store
- Custom-signed Afaria application portal

6.5 Device Enrollment with Enrollment Codes

For device types that support enrollment codes, and when you are not using an Afaria Self-Service Portal, the end users can open the Afaria application on their device and enter an enrollment code to connect to Afaria and enroll in management.

Enrollment codes are supported on these device types:

- Android
- iOS (versions 4.3.x – 6.x)
- Windows Mobile Professional
- Windows Mobile Standard

After a user enters an enrollment code, Afaria contacts a public URL shortening service to get an expanded address, then connects to that address. The expanded address is for a device to connect to an enrollment server, or its relay server proxy, or to enroll in management.

6.6 Device Enrollment with the SAP Afaria Self-Service Portal

For device types that support using the Self-Service Portal, users visit the portal to enroll in Afaria management.

Device enrollment using the portal is supported for these device types :

- Android
- iOS
- Windows Phone
- Windows Mobile Professional
- Windows Mobile Standard

The portal experience varies for end-users based on the device type:

- Android, iOS (versions 4.3.x – 6.x) – access the portal from the enrolling device or from a personal computer. Portal includes a link to the appropriate commercial market for installing Afaria and provides an enrollment code to enroll in management.
- iOS (version 7 or higher) – access the portal from the enrolling device and click the enroll button. Access the portal from a personal computer to activate the enrollment code URL in the portal, then enter the URL in the native Web browser (Safari) on the device.
- Windows Phone – access the portal from the enrolling device or from a personal computer. Activate the enrollment code URL on the portal, access company apps on the device and provide the enrollment URL and other details. The enrollment URL connects to the discovery service, which in turn contacts the enrollment service for enrollment and authentication.
- Windows Mobile Professional and Standard – access the portal from a personal computer. Portal includes a link to download the Afaria application from the enrollment policy, and provides an enrollment code to enroll in management.

For device types that use an enrollment code, the application contacts a public URL shortening service to get an expanded address, and then connects to that address. The expanded address is for connecting a device to an enrollment server, or its relay server proxy, to enroll in management.

6.7 Device Enrollment with Custom Installations

You can create custom installations for the Self-Service Portal application that end-users can install directly on end-user devices. You can configure it to connect to the Afaria server to enroll the device. If you did not define a server address in the enrollment policy, you need to configure it on the device after installation.

Custom installations are supported on these device types:

- Windows CE
- Windows Mobile Professional
- Windows Mobile Standard
- Windows

For Windows Mobile devices, the user opens the application and cancels the enrollment code prompt, defines configuration if not already defined, and then initiates a connection to the enrollment server, or its relay server proxy, to enroll in management.

For Windows CE and Windows, the user opens the application, defines configuration if not already defined, and then initiates a connection to the SAP Afaria server, or its relay server proxy, to enroll in management.

6.8 Device Reenrollment

Restart management for a device with the same server without hard resetting the device.

Reenrollment helps you resolve scenarios, which may vary by device type:

- Need for user to reenter user prompts.
- Device has been hard reset.
- User removed, then reinstalled, the Afaria application.
- To let user have access to Afaria Self-Service Portal management, user can reenroll over the portal.
- Device state was enrolled but not yet approved for management; but now device is approved for management.
- Need to change a device's tenant.
- Changes to server address, such as the Afaria server, enrollment server, or relay server.

If a device that was already enrolled reenrolls with the server, the device is enrolled under the system tenant, and is unapproved.

6.9 Android Device Enrollment

Android devices install the Afaria application from the Google Play market.

Enrolling Android Devices [page 279]
Enroll Android devices with enrollment codes that you distribute or that users get from the Self-Service Portal. Afaria applications are installed from the Google Play market.

Enrollment Actions for Android Devices [page 279]
Enrolling Android devices in management completes several actions for your devices.

Required E-Mail Formats for Android Devices [page 280]
For Android devices, the e-mail user name requirement for Access Control for Email varies according to your enterprise environment.

Removing the SAP Afaria Client [page 280]
You can remove an Android device from management by removing the Afaria client from the device. To remove the client from the device, you must first remove the device administrator privileges for the client.

6.9.1 Enrolling Android Devices

Enroll Android devices with enrollment codes that you distribute or that users get from the Self-Service Portal. Afaria applications are installed from the Google Play market.

Procedure

1. On the Afaria server, create an enrollment policy.
2. If users are going to enroll using the portal, install it using an enrollment code from the policy.
3. On the device, install an Afaria application from the Google Play market.
4. Give users the enrollment code from the enrollment policy or instruct them to enroll and get an enrollment code from the portal.
5. On the device, open the application and enter the enrollment code.

   The device connects to Afaria through its proxy or directly, according to your environment configuration.

   If either server security or the enrollment policy is set to automatically approve devices, enrollment is completed.

   If neither server security nor the enrollment policy is set to automatically approve devices, the device is in an unapproved state. If reenrolling for a new tenant, the device may be in an unapproved state.

   > **i** Note
   >
   > If the device enrollment fails, the device re-prompts for entering an enrollment code.
6. If the device is unapproved on the Afaria Administration console, approve the device for management according to your organizational processes.
7. (Optional) If you approved a device, take any appropriate additional steps to effect management actions, such as sending an outbound notification to apply policies or have the user re-enroll.

6.9.2 Enrollment Actions for Android Devices

Enrolling Android devices in management completes several actions for your devices.

Enrollment actions for devices include:

- Configuring the application if the device is unapproved.
- (Optional) Generating the Afaria client name.
- (Optional) Applying Access Control for Email policy.
- (Optional) Enrolling in groups.
- If automatically approving devices, applying policies.

6.9.3 Required E-Mail Formats for Android Devices

For Android devices, the e-mail user name requirement for Access Control for Email varies according to your enterprise environment.

Ensure that users enter the information correctly. On the device's configuration page (*Afaria* > *Configuration* >), the e-mail user name must comply with your e-mail server's requirement for user name. The format, as observed in table `A_ANDROID_DEVICES`, is:

- domain\user
- user@domain

6.9.4 Removing the SAP Afaria Client

You can remove an Android device from management by removing the Afaria client from the device. To remove the client from the device, you must first remove the device administrator privileges for the client.

Procedure

1. To remove Afariadevice administrator privileges, perform these tasks:
   a. On the device, tap *Settings*.
   b. Tap *Security*.
   c. Tap *Device administrators*.
   d. From the Device aedministrators screen, clear the check box for the Afaria client.

      You'll be prompted to deactivate the Afaria client.
   e. To remove the administrative privileges, tap *Deactivate*.
   f. Tap *OK* to confirm the removal of the administrative privileges.
2. To remove the Afariaclient from the device, perform these tasks:
   a. On the device, tap *Settings*.
   b. Tap *Apps*.
   c. Tap the Afaria client icon.
   d. From the App info screen, tap *Uninstall*.
   e. Tap *OK* to confirm the removal of the client.

6.10 iOS Device Enrollment

iOS devices have native support for device management using Apple Mobile Device Management (MDM) and can install the SAP Afaria client from the custom-signed enterprise application portal on the SAP Afaria customer support site or the Apple App Store.

6.10.1 Enrolling iOS Devices

Enroll devices using enrollment codes that you distribute, or that users obtain from the Self-Service Portal.

Procedure

1. On the SAP Afaria server, create an enrollment policy.
2. If enrolling users with Self-Service Portal, install the portal using an enrollment code from the policy.
3. On the device, install an SAP Afaria Client from the custom-signed enterprise application portal or from the Apple App Store.

   Users can download the SAP Afaria client from the Apple App Store or install a custom-signed SAP Afaria client.

4. Give users the enrollment code from the enrollment policy, or instruct users visit the self-service portal to enroll and get an enrollment code.
5. On the device, open the application and enter the enrollment code.

   The device connects to Afaria through its proxy or directly, according to your environment configuration.

   If either server security or the enrollment policy is set to automatically approve clients, or you have taken action to approve a device, SAP Afaria completes enrollment. The user must accept and install the Mobile Device Management (MDM) policy to complete MDM enrollment.

   If neither server security nor the enrollment policy is set to automatically approve devices, the device is in an unapproved state. If reenrolling for a new tenant, the device may be in an unapproved state.
6. If the device is unapproved on the Afaria Administration console, approve the device for management according to your organizational processes.
7. (Optional) If you approved a device, take any appropriate additional steps to effect management actions, such as sending an outbound notification to apply policies or have the user re-enroll.

6.10.2 Enrolling iOS Devices in Management Using MDM-First Enrollment

Enroll iOS devices using an MDM enrollment link that you distribute to users. The enrollment policy generates the MDM enrollment link.

Context

When the enrollment is complete, the device is subject to the policies in SAP Afaria. These policies might require you to perform additional actions on your device. For example, you might need to set a passcode for the device.

Procedure

1. On the SAP Afaria server, create an enrollment policy.
2. Send the MDM enrollment link from the enrollment policy to the user.
3. On the device, browse to the MDM enrollment link and enter your credentials.
4. If prompted, enter values for the user-defined variables.
5. To start the installation of the MDM Device Enrollment Profile Service, click *Install* and then *Install now*.
6. If a password is set on the device, enter the password to authorize the installation.
7. If prompted to install a profile, click *Install*.
8. Click *Done*.
9. To install the SAP Afaria Client, click *Install*.

6.10.3 Enrolling iOS Devices in Management Using The Self Service Portal

Enroll iOS devices using the Self-Service Portal.

Context

When the enrollment is complete, the device is subject to the policies in SAP Afaria. These policies might require you to perform additional actions on your device. For example, you might need to set a passcode for the device.

Procedure

1. On the SAP Afaria server, create an enrollment policy.
2. Send the Self-Service Portal link from the enrollment policy to the user.
3. On the device, browse to the Self-Service Portal and enter your credentials.
4. Click *Enroll New Device*.
5. Click *Enroll*.
6. If prompted, enter your credentials.
7. If prompted, enter values for the user-defined variables.
8. To start the installation of the MDM Device Enrollment Profile Service, click *Install* and then *Install now*.
9. If a password is set on the device, enter the password to authorize the installation.
10. If prompted to install a profile, click *Install*.
11. Click *Done*.
12. To install the SAP Afaria Client, click *Install*.

6.10.4 Enrolling Jailbroken iOS Devices in Management

Afaria allows iOS devices that have been jailbroken or compromised to complete the enrollment process, including MDM relationship enrollment.

Procedure

1. From the *Policy* > *Edit* > *iOS Enrollment* > *General* page, select *Enable jailbroken devices*.

> **i Note**
>
> A jailbroken iOS device can proceed with the MDM enrollment process only if this option is selected.

2. Click *Save*.

6.10.5 Processing Jailbroken iOS Devices

When you enable the jailbroken devices option while creating or editing an iOS enrollment policy, SAP Afaria performs some steps for successful enrollment.

1. The SAP Afaria client on the jailbroken iOS device receives the enrollment policy and proceeds with the initial enrollment process by accepting or entering the enrollment code into the SAP Afaria client.
2. SAP Afaria verifies the enrollment code and authenticates it back to the enrollment server.
3. The enrollment server delivers the enrollment payload to the SAP Afaria client to install on the device. The SAP Afaria client prompts the user to install the enrollment payload on the device.
4. The SAP Afaria client enrollment server that the enrollment payload has been successfully installed on the device, as a result enrollment server creates a device record.
5. The enrollment server sends request to the SAP Afaria client to verify device details, and the SAP Afaria client sends jailbreak status to the enrollment server.
6. The enrollment server determines the MDM status and sends the MDM enrollment command to the SAP Afaria client.

6.10.6 Enrollment Actions for iOS Devices

Enrolling in management completes several actions for your devices.

Enrollment actions for devices include:

- Configuring the SAP Afaria client.
- (Optional) Generating the SAP Afaria client name.
- (Optional) Applying Access Control for Email policy.
- (Optional) Enrolling in groups.
- If automatically approving devices, provisioning SAP Afaria Mobile Device Management (MDM).
- If automatically approving devices, applying policies.
- If automatically approving devices, collecting inventory.

6.10.7 Resetting User Credentials on iOS Devices

Change the domain, user name, or password that the SAP Afaria client uses for authentication.

Procedure

1. On the device, close the SAP Afaria client.

2. Navigate to *Settings* > *General* > *Afaria* > *Reset Credentials* and set to On.

Results

The user is prompted to enter credentials the next time the application requires authentication.

6.10.8 Apple Device Enrollment Program

The Apple Device Enrollment Program (DEP) simplifies the enrollment of devices that organizations purchase from Apple.

SAP Afaria uses a DEP token and profile to connect to Apple and retrieve enrollment and configuration information about devices. The DEP automates device enrollment in SAP Afaria, can require devices to automatically enroll in MDM management, and can skip screens (for example, the Passcode or Restore from backup screens) and the associated user prompts in the enrollment process. When the MDM profile is on devices, the DEP allows you to prevent users from removing devices from MDM control by preventing them from removing the MDM profile.

The DEP allows wireless supervision of devices and provides addition control of devices. The DEP can wirelessly enable supervision mode on devices without requiring devices to connect to a computer with the Apple Configurator.

To use the DEP, organizations must register with Apple. For more information about the DEP, visit the Apple web site.

Obtaining a Server Token [page 285]
You can install an Apple Device Enrollment Program (DEP) token to allow SAP Afaria to connect securely to the DEP Web services to enroll and manage devices.

Configuring the Apple Device Enrollment Program [page 286]
You can use the Afaria Administration console to upload an Apple Device Enrollment Program (DEP) token and configure SAP Afaria to use the DEP when enrolling iOS devices.

6.10.8.1 Obtaining a Server Token

You can install an Apple Device Enrollment Program (DEP) token to allow SAP Afaria to connect securely to the DEP Web services to enroll and manage devices.

Prerequisites

To use the DEP, organizations must register with Apple. For more information about the DEP, visit the Apple web site.

Context

When you request the DEP token from the Apple Deployment Programs web site, you will be required to upload a public key that Apple uses to encrypt the DEP token to be downloaded. Once downloaded, the private key can then be used to decrypt the DEP token before it is installed on the SAP Afaria server. You can use an MDM push certificate for the public and private keys.

Procedure

1. Obtain the MDM push certificate in `.pfx` format from the certificate store on the SAP Afaria server.
2. To use OpenSSL to extract the public and private key from the MDM push certificate, perform the following tasks:
   a. To extract the public key, type the following into a command prompt:

      ```
      openssl pkcs12 -in yourP12File.pfx -clcerts -nokeys -out publicCert.pem
      ```

   b. To extract the private key, type the following into a command prompt:

      ```
      openssl pkcs12 -in yourP12File.pfx -nocerts -out privateKey.pem
      ```

3. To obtain an S/MIME encrypted token file from the Apple Deployment Programs web site, perform the following tasks:
   a. Sign in to the Apple Deployment Programs web site.
   b. Add a virtual MDM server.
   c. Upload the extracted public key.
   d. Download the S/MIME encrypted token file.
   e. Enter a device serial number and assign the serial number to the SAP Afaria server.
4. To use the private key to decrypt the S/MIME encrypted token file, type the following into a command prompt:

   ```
   openssl smime -decrypt -in <path-to-file>\yourServer_Token_smime.p7m -inkey
   <path-to-file>\privateKey.pem > Server_Token.stoken
   ```

6.10.8.2 Configuring the Apple Device Enrollment Program

You can use the Afaria Administration console to upload an Apple Device Enrollment Program (DEP) token and configure SAP Afaria to use the DEP when enrolling iOS devices.

Context

DEP tokens are specific to tenants. An error occurs if you try to upload an DEP token that is already associated with a tenant.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Enrollment* > *Apple Device Enrollment*.
3. In the *Token file* field, browse to and select the decrypted token file from Apple Deployment Programs Web site.
4. In the *Department name* field, type the department name.
5. In the *Support phone number* field, type the number that device users contact for support.
6. (Optional) In the *iOS Enrollment Policy* field, select the enrollment policy that SAP Afaria applies to iOS devices in the DEP. By default, SAP Afaria uses the default iOS enrollment policy.
7. In the *Anchor Certificate* table, add the certificates that devices use to validate SSL connections to the SAP Afaria server.
8. In the *Supervising Host Certificate* table, add the certificates that devices use to determine which hosts to connect to.
9. In the *Policy settings* list, perform the following tasks:
   a. To allow devices to tether to computers, select *Pairing*.
   b. To wirelessly activate supervised mode on devices, select *Supervised*.
   c. To require installation of the MDM profile, select *Profile installation required*.
   d. To allow users to remove the MDM profile from devices, select *Profile removable*.
10. In the *Skip Device Setup Panels* list, select the pages and prompts that devices skip during enrollment.
11. Click *Save*.

6.11 Windows Devices

Windows devices have an installed application for SAP Afaria management, as deployed by your organization.

The Windows OS versions that SAP Afaria supports use different native APIs, .NET Framework technologies, and have differences in user and application security and management. These differences affect some SAP Afaria operations.

Windows Browser Sessions [page 291]

SAP Afaria supports HTML-based channels that Windows devices can run in a browser. Windows devices that run a channel this way are referred to as browser sessions. Browser sessions can also run non-HTML channels.

6.11.1 Windows Device Management Life Cycle

Manage devices using applications created in enrollment policies and distributed to devices.

Procedure

1. Create an enrollment policy. The policy defines configuration settings and creates an SAP Afaria client.
2. Download the application from the enrollment policy.
3. Deploy and install the application on the device.
4. Connect the device to the SAP Afaria server.
5. When updates are available on the SAP Afaria server, update the application by connecting to SAP Afaria or reinstalling the application.
6. To terminate management, the user removes the application.

6.11.2 Enrolling Windows Devices

Enroll devices using applications from enrollment policies that you distribute to users.

Procedure

1. On the SAP Afaria server, create an enrollment policy and download the SAP Afaria application.
2. Deploy the application using network, local, or portable media.
3. On the device, install the application.
4. Connect to the SAP Afaria server.

   The device connects to Afaria through its proxy or directly, according to your environment configuration.

   If either server security or the enrollment policy is set to automatically approve devices, enrollment is completed.

   If neither server security nor the enrollment policy is set to automatically approve devices, the device is in an unapproved state. If reenrolling for a new tenant, the device may be in an unapproved state.

6.11.3 Installing Afaria on Windows Computers

Windows application users run the setup executable file on their PCs to install the product.

6.11.4 Updating the Afaria Windows Application

Connect the computer to the SAP Afaria server to update or upgrade the application. SAP Afaria automatically delivers file updates, and the application automatically applies the updates without any user interaction.

6.11.5 Update Considerations for Windows Devices

The beginning of each device session checks whether the server has file updates for the device to apply. SAP Afaria automatically delivers file updates.

How the device retrieves and applies the updates depends on the value of the following server registry key that is installed during product installation:

```
hklm\software\afaria\afaria\server\silentupgrade
```

The key is defined according to the following values:

- 0 – Not silent.
- 1 – Silent, attended reboot. Prompts device user for reboot.
- 2 – Silent, unattended reboot. No prompting.
- 3 – Obsolete key. Defaults to behavior of value 5.
- 4 – Silent, no reboot. If upgrade requires reboot, the process is aborted. This key is included only for backwards compatibility and should be used with caution.
- 5 – Silent, delayed reboot. If reboot is necessary, waits until the device user performs a reboot to continue the upgrade process.

Update to Upgrade Windows Device

When SAP Afaria applies an upgrade for the Windows device, a system restart may be required to fully complete the upgrade.

If a reboot is required and your device user connects to the server before rebooting, the upgrade process is incomplete and the SAP Afaria client does not run a session but the server does create a log entry.

If the user defers the system restart until a later time, and then attempts to run a session, SAP Afaria will display a brief message to the device user that the system must be restarted before running any sessions. After the user restarts the device system, and the upgrade is completed, all sessions run normally.

When a device in need of a restart attempts to run a session, a message is added to the server log to record the event. Administrators can read the Messages log to identify devices in need of a reboot.

6.11.6 Windows OS Variations

The Windows OS versions that SAP Afaria supports use different native APIs, .NET Framework technologies, and have differences in user and application security and management. These differences affect some SAP Afaria operations.

SAP Afaria is designed to install and operate in different contexts: as logged on user, as a service without associated user credentials, and as a service with associated user credentials. This flexibility lets you manage Windows computers in ways that best suit your enterprise.

While it is your responsibility to understand the behavior of each Windows OS version that you use in your organization, the variations in Windows OS versions warrant advisement about some of the SAP Afaria behavior impacted by the differences. Consider the following subjects as you plan and manage SAP Afaria operations for different Windows OS versions.

Installation and Data Storage

- Installation and data directory – Windows OS versions vary with respect to the security restrictions enforced when writing application data to the Program Files folder. Therefore, Windows devices use different implementations for storing install files and data files based on Windows OS version.
  - Windows Vista client default install folder – %PROGRAMFILES%\Aclient\Bin
  - Windows Vista client default data folder – %ALLUSERSPROFILE%\AClient\Data
  - Before Windows Vista clients install and data folder – %PROGRAMFILES%\Aclient
- Session variables – You may want to use session variables <ClientDataDir> and <ClientOS> during operations to help you decide upon and execute behavior that is appropriate for different OS versions.
- Install package and application installation
  - Windows Vista – Within the User Access Control (UAC) security framework, the application is installed with the LOCALSYSTEM account and does not require a set of credentials to run an application as a service.
  - Before Windows Vista – The security framework for running an application as a service optionally permits associating user credentials with the service operations.

Session Channel Operations

Channels often need to perform tasks that require elevated privileges in order to be successful. You need to understand the interrelationship between the SAP Afaria client context, the operating system security restrictions on specific channel tasks, and the channel's features you choose. It is the interrelationship of these items that impacts a channel's ability to successfully execute.

- SAP Afaria context – the SAP Afaria service or user context for performing channel tasks:
  - SAP Afaria installed as a service without associated administrator credentials
  - SAP Afaria installed as a service with associated administrator credentials
  - SAP Afaria installed as the logged on user
- Operating system security restrictions – the operating system may restrict or limit channel tasks at the client. These restrictions may vary by Windows OS version.

- Write to the root folder
- Write to the Windows folder
- Write to the Windows system folder
- Write to the registry
- Interact with the user interface

Session channels include features and options that enable you to work successfully within the operating system security framework.

- Read, write, and delete files and folders
- Get, set and delete registry values
- Impersonate user events
- Execute programs and scripts
- Expose message to user interface event
- Use and set session variables
- Use and read environmental variables

6.11.7 Windows Browser Sessions

SAP Afaria supports HTML-based channels that Windows devices can run in a browser. Windows devices that run a channel this way are referred to as browser sessions. Browser sessions can also run non-HTML channels.

Browser sessions may warrant special consideration in an SAP Afaria server farm environment. By default, browser sessions connect only to the main SAP Afaria server. If you feel it is necessary that you distribute browser session connections across your farm environment, then you can force the distribution by using a round-robin load balancer.

6.12 Windows Device Enrollment

Windows (Windows DM) devices provide a built-in device management client that communicates with the SAP Afaria server. These devices can be enrolled in management either from the Self-Service Portal by activating the enrollment code, or directly from the device using domains.

The enrollment of Windows DM devices supports auto-discovery. Auto-discovery service, if enabled, attempts to automatically detect the enrollment server address and enroll the device in management. Otherwise, if the administrator has provided the enrollment server URL, the user can paste it in the server address field on the Workplace account creation page.

To enable auto-discovery in Afaria for enrollment server, the Afaria administrator must configure a public Domain Name System (DNS) entry in the format `enterpriseenrollment.domain.x` for the device-reachable enrollment server module.

For more details about enabling auto-discovery service, see *Enabling Auto-Discovery for Windows and Windows Phone Devices*.

Using Self-Service Portal

1. On the Afaria Administration console, create a Windows DM enrollment policy.
   The enrollment code to enroll the device is auto-generated, based on the enrollment server settings.
2. Access Self-Service Portal on the device and activate the enrollment code.
3. Navigate to Workplace on the device, provide your user ID and the server address URL (if provided) to create a workplace account, and turn on device management for the device.
4. On the login page, provide the user credentials for authentication, and log in to management.
5. Accept the agreement regarding apps and services from IT admin, and the device gets enrolled in SAP Afaria management.

Using Domains

1. On the Afaria Administration console, create a new domain for enrolling the Windows DM device.
2. Choose one of the following:
   - For Windows 8.1 OS version, navigate to Workplace
   - For Windows 10 OS version, navigate to *Settings* > *Accounts* > *Work Access*
3. Provide your user ID to create a workplace account, and turn on device management for the device.
   Based on the domain name in the user ID and the default enrollment settings for Windows device, the auto-discovery service retrieves the server details for enrolling the device, and a login page shows up for user authentication.
4. On the login page, provide the user credentials for authentication, and log in to management.
5. Accept the agreement regarding apps and services from IT admin, and the device gets enrolled in SAP Afaria management.

Afaria application silently installs on the device, after the device is enrolled in management.

For more details on configuring domains, see *Configuring Domains for Enrolling Windows Phone and Windows DM Devices* in *Configuring Afaria*.

Enabling Auto-Discovery for Windows and Windows Phone Devices [page 292]
Enabling auto-discovery capabilities for the Afaria enrollment server provides a simplified enrollment process for Windows (Windows DM) and Windows Phone users. Auto-discovery is not a pre-requisite for enrolling Windows DM and Windows Phone devices.

6.12.1 Enabling Auto-Discovery for Windows and Windows Phone Devices

Enabling auto-discovery capabilities for the Afaria enrollment server provides a simplified enrollment process for Windows (Windows DM) and Windows Phone users. Auto-discovery is not a pre-requisite for enrolling Windows DM and Windows Phone devices.

To enable auto-discovery in Afaria for enrollment server, the Afaria administrator has to make sure that there is a public Domain Name System (DNS) entry in the format `enterpriseenrollment.domain.x` for the device-reachable enrollment server module. This means that if the enrollment server is placed in the DMZ then its IP

address should be mapped. If enrollment server is behind the firewall and exposed through relay server, then the administrator can use reverse proxy to re-route the traffic to relay server and have DNS entry mapped to reverse proxy.

If there are multiple domains or subdomains used, then there should be Fully Qualified Domain Names (FQDN) with all the possible domain and subdomain name combinations. For example, if you want users from the domain `sampledomain.com` to enroll, the FQDN should be `enterpriseenrollment.sampledomain.com`. To the same enrollment server if the administrator wants to allow users from `subdomain.sampledomain.com`, then there should be another FQDN `enterpriseenrollment.subdomain.sampledomain.com` as well. The HTTPS port where device communicates should have multiple bindings with the respective FQDNs.

> **i Note**
>
> Wild card certificates are not supported for auto-discovery.

6.13 Windows Mobile Devices

Windows Mobile devices have an installed application for SAP Afaria management, as deployed by your organization. “Windows Mobile” is a general reference to Windows Mobile Professional, Windows Mobile Standard, and Windows CE device types.

Windows Mobile Device Management Life Cycle [page 294]
: Manage devices using applications created in enrollment policies and distributed to devices.

Enrolling Windows Mobile Devices [page 294]
: Enroll devices using applications and enrollment codes from enrollment policies that you distribute, or users get from the Self-Service Portal.

Enrolling Windows CE Devices [page 295]
: Enroll devices using applications from enrollment policies that you distribute to users.

Download File Requirements for Windows Mobile [page 295]
: If you are deploying the SAP Afaria client directly to devices from a Web server, you may encounter errors if the download file requirements are not met.

Updating the Afaria Client for Windows Mobile Devices [page 296]
: Connect the device to the SAP Afaria server to update or upgrade the application. SAP Afaria automatically delivers file updates, and the application automatically applies the updates without any user interaction.

6.13.1 Windows Mobile Device Management Life Cycle

Manage devices using applications created in enrollment policies and distributed to devices.

Procedure

1. Create an enrollment policy. The policy defines configuration settings and creates an SAP Afaria client.
2. Deploy the application using either of these methods:
   - Download the application from the enrollment policy and distribute to users with an enrollment code.
   - Install an Self-Service Portal instance that uses the enrollment policy and let users connect with their desktop computers and download the application and get an enrollment code.
3. Users install the SAP Afaria client on their devices. You can configure the SAP Afaria client for connections to the SAP Afaria server prior to deployment to devices.
4. Users enter their enrollment code and connect to SAP Afaria.
5. Connect the device to SAP Afaria.
6. When updates are available on the SAP Afaria server, update the application by connecting to SAP Afaria or reinstalling the application.
7. To terminate management, the administrator wipes the device or the user removes the application.

6.13.2 Enrolling Windows Mobile Devices

Enroll devices using applications and enrollment codes from enrollment policies that you distribute, or users get from the Self-Service Portal.

Procedure

1. On the SAP Afaria server, create an enrollment policy.
2. If enrolling users with Self-Service Portal, install the portal using an enrollment code from the policy.
3. Deploy the application using either of these methods:
   - Download the application from the enrollment policy and distribute to users with an enrollment code.
   - Install an Self-Service Portal instance that uses the enrollment policy and let users connect with their desktop computers and download the application and get an enrollment code.
4. On the device, install the application.
5. On the device, open the application and enter the enrollment code.
6. Connect the device to SAP Afaria.

   The device connects to Afaria through its proxy or directly, according to your environment configuration.

   If either server security or the enrollment policy is set to automatically approve devices, enrollment is completed.

If neither server security nor the enrollment policy is set to automatically approve devices, the device is in an unapproved state. If reenrolling for a new tenant, the device may be in an unapproved state.

7. If the device is unapproved on the Afaria Administration console, approve the device for management according to your organizational processes.
8. (Optional) If you approved a device, take any appropriate additional steps to effect management actions, such as sending an outbound notification to apply policies or have the user re-enroll.

6.13.3 Enrolling Windows CE Devices

Enroll devices using applications from enrollment policies that you distribute to users.

Procedure

1. On the SAP Afaria server, create an enrollment policy and download the SAP Afaria client.
2. Deploy the application using any appropriate method.
3. On the device, install the application.
4. Connect to the SAP Afaria server.

   The device connects to Afaria through its proxy or directly, according to your environment configuration.

   If either server security or the enrollment policy is set to automatically approve devices, enrollment is completed.

   If neither server security nor the enrollment policy is set to automatically approve devices, the device is in an unapproved state. If reenrolling for a new tenant, the device may be in an unapproved state.

6.13.4 Download File Requirements for Windows Mobile

If you are deploying the SAP Afaria client directly to devices from a Web server, you may encounter errors if the download file requirements are not met.

Some devices do not preserve a file's extension when downloading it. These devices may have errors installing the application.

Successful installation at the device requires that the application is downloaded and saved with the .CAB file extension.

User can use the “save as” command to manually define the file name and correct extension, rather than allowing the devices default behavior to save it incorrectly.

6.13.5 Updating the Afaria Client for Windows Mobile Devices

Connect the device to the SAP Afaria server to update or upgrade the application. SAP Afaria automatically delivers file updates, and the application automatically applies the updates without any user interaction.

6.14 Windows Phone Device Enrollment

Windows Phone devices include a built-in device management client that communicates with the Afaria server. Enroll devices using the enrollment URL that you obtain from the Self-Service Portal or that the administrator distributes.

Windows Phone also supports simplified device enrollment using the auto-discovery service. For more details about enabling auto-discovery service, refer the section *Enabling Auto-Discovery for Windows 8.1 and Windows Phone Devices*.

After enrollment, during the first connection to the server, the Afaria application silently installs on the device. The Windows Phone device management client has two components:

- Enrollment client – enrolls and configures the device to communicate with the Afaria server.
- Device management client – periodically synchronizes and checks for updates on the Afaria server, and applies the latest policies to the device.

The following sequence of events provisions and configures the client to connect to the Afaria server:

1. Discovery service provides the configuration information necessary for a user to enroll the device with Afaria management.
2. Certificate installation handles user authentication, certificate generation, and installs certificates for SSL authentication.
3. Client provisioning provisions the device management client to connect to the Afaria server after enrollment.
4. Administrator configures an inbound connection schedule with predefined values, as Windows Phone does not support outbound connections.

The life cycle of a Windows Phone device in Afaria management can be summarized as:

1. From the Afaria Administration console, create a Windows Phone enrollment policy.
   The enrollment code URL used to enroll the device is autogenerated based on the enrollment server settings.
2. Access the Self-Service Portal on the device and activate the enrollment code URL.
   In the auto-discovery scenario, if the user does not use the Self-Service Portal for enrollment, ensure that the user's domain is configured in the *Server* > *Configuration* > *Enrollment* > *Domains* page on the Afaria Administration console. For more details about configuring domains for auto-discovery, refer the section *Configuring Domains for Enrolling Windows Phone and Windows DM Devices* in the *Configuring Afaria* module.
3. Enter values for user variables prompted on the portal, if variables have been configured in the associated enrollment policy.
4. To enroll a device, provide valid credentials to create a company apps/workplace user account.
5. If prompted for a server address on the device, enter the enrollment code URL, and provide the user credentials when prompted.

If auto-discovery service is configured on the SAP Afaria server, the enrollment server details are automatically retrieved, and a password prompt appears. Enter the password and tap *sign in*.
The device is enrolled in management. After enrollment, during the first connection to the Afaria server, the Afaria application is silently installed on the device.

6. Apply configuration, access control, or remediation policies on the device, as required.
7. To remove the device from management, the administrator wipes the device remotely, or the user deletes the company apps/workplace account on the device.

Device management activities for a Windows Phone device include:

- Editing device details
- Collecting inventory details
- Security actions on the device
- Checking the diagnostic dashboard details

> **i Note**
>
> - There may be variations in the time taken to perform actions such as removal of the account on the device, or the application of a passcode. The actions may not happen instantly.
> - When a device is removed from management, any applications and ActiveSync accounts that have been applied by the MDM server also get deleted.
> - Removal of a password policy does not mean that the password is removed from the device. It only means that the password is not enforced.

Enrolling Windows Phone Devices [page 298]
: Enroll Windows Phone 8.1 and Windows Phone 10 devices in Afaria management, using the MDM enrollment URL that you distribute, or that the users obtain from the Self-Service Portal. Windows Phone also supports auto-discovery service for enrollment, where the enrollment server details are automatically retrieved based on the domain details of the enrolling user's e-mail address.

Removing Windows Phone Devices from Management [page 299]
: Windows Phone devices can be removed from Afaria management either by the user from the device or remotely by the administrator. The administrator uses the remote wipe action to disconnect the device from management. To initiate the disconnection process from the device, the user must delete the company apps account created during the enrollment.

Related Information

Creating an Enrollment Policy for Windows Phone [page 238]
Creating a Configuration Policy for Windows Phone [page 225]
Creating Access Control Policies for Windows Phone Devices [page 252]
Defining Remediation Policies for Windows Phone Devices [page 265]
Editing a Windows Phone Device [page 313]
Hardware Inventory for Windows Phone Devices [page 357]
Security Actions for Windows Phone Devices [page 318]

6.14.1 Enrolling Windows Phone Devices

Enroll Windows Phone 8.1 and Windows Phone 10 devices in Afaria management, using the MDM enrollment URL that you distribute, or that the users obtain from the Self-Service Portal. Windows Phone also supports auto-discovery service for enrollment, where the enrollment server details are automatically retrieved based on the domain details of the enrolling user's e-mail address.

Prerequisites

In the auto-discovery scenario:

- If the user does not use Self-Service Portal for enrollment, ensure that the user's domain is configured on the *Server* > *Configuration* > *Enrollment* > *Domains* page in the Afaria Administration console.

Context

Windows Phone device enrollment works only with HTTPS, when communicating with the discovery service and the enrollment server. For Windows Phone devices, if you use non-default port and HTTPS in a self-signed environment, you must specify the port in the enrollment server address, for the enrollment to work. If you use default port in a self-signed environment, the enrollment settings configured for HTTP will automatically switch to HTTPS on the device.

See topic *Configuring SSL Connections for Enrollment Server* in *Configuring Afaria*.

Procedure

1. In the Afaria Administration console, create a Windows Phone enrollment policy.
   The MDM Enrollment URL used to enroll the device is auto-generated based on the enrollment server settings in *Server* > *Component* > *Enrollment Server* page.
2. If you are enrolling devices using the Self-Service Portal, install the portal using an enrollment code from the policy.
3. Activate the enrollment code URL on the Self-Service Portal.
4. Enter values for user variables prompted on the Self-Service Portal, if variables have been configured in the associated enrollment policy.
5. Choose one of the following based on your Windows Phone OS version:
   - On a Windows Phone 8.1 device, tap *Settings*> *WorkPlace*.
   - On a Windows Phone 10 device, tap *Settings* > *Accounts* > *Work Access*.
6. Create a new company account, by providing a valid e-mail address.
7. Enter the server URL and tap *sign in*.

> **Note**
>
> In case your administrator has enabled Auto-discovery, you will be directed to the authentication page directly.

8. On the authentication page, enter username and account password.
9. Tap *Connect*.
10. Approve the device for Afaria management according to your organization's processes.

6.14.2 Removing Windows Phone Devices from Management

Windows Phone devices can be removed from Afaria management either by the user from the device or remotely by the administrator. The administrator uses the remote wipe action to disconnect the device from management. To initiate the disconnection process from the device, the user must delete the company apps account created during the enrollment.

When disconnecting from Afaria management, the client on the device:

- Removes from the device the client and root certificates configured by the Afaria Server.
- Stops enforcing policies applied by the administrator.
- Removes client configuration details from the device. The client remains dormant until the user reconnects.
- If the administrator initiates the disconnection process, notifies the user that the device has been removed from management.

> **Note**
>
> The remote wipe and remove control actions will not occur until the device initiates the connection, as Windows Phone devices do not support outbound connections.

Related Information

Security Actions for Windows Phone Devices [page 318]

6.15 Approving Devices

Approve devices that are in an unapproved state so they can be managed with policies on future connections. Unapprove devices to discontinue management.

Context

Your server may be configured to automatically approve devices, as per the *Server* > *Configuration* > *Security* page.

Procedure

1. On the Device page, select one or more devices.
2. On the top toolbar:
   - Click *Approve* to approve all selected devices for management.
   - Click *Unapprove* to unapprove all selected devices for management.
3. (Optional) For devices that you approve, take additional action to affect management actions, such as:
   - iOS example – reenroll a device using the same enrollment code. Reenrolling provisions mobile device management (MDM) and applies policies.
   - Non-iOS example – send a command to run a channel.

7 Device Administration

Devices are phone and computing devices, such as smartphones, tablets, and desktop or laptop computers that you manage with groups and policies. In the Afaria Administration console, the Device page is the landing page for device-focused tasks.

You can move a device to a different tenant in the Afaria Administration console.

Sending Messages to Devices [page 325]
You can use the Afaria Administration console to send email or push notification messages to devices.

Connecting a Device to Apply Policies [page 326]
Send a notification to a device to make it connect immediately to an SAP Afaria server and apply its policies.

Connecting a Device to Run a Channel [page 327]
Send a notification to a device to make it connect immediately to an SAP Afaria server to request a specific, published channel. For the device to be able to run the channel, the channel must be included in one of its session policies.

Deleting a Device or its Data from the Server [page 327]
Delete a device's record and all of its data from the server, or keep the device record but delete some of its data from the server.

Getting Log Files from Devices [page 328]
You can get the log files from an Android device or an iOS device using the Afaria Administration console.

Windows Phone Custom Branding [page 328]
You can customize the SAP Afaria client (xap) for Windows Phone devices, with your own corporate brand images and text.

Configuring Password Reset and Expiry Details for Windows Phone [page 329]
Configure the expiry time interval for the new password that is generated when the administrator initiates the Lock Device and Reset Password action for a device. Compose the password reset e-mail message for the user.

7.1 Viewing the Device Dashboard

View a graphical representation of device metrics, such as the number of devices in approved or unapproved states, and days since last connection.

Procedure

1. On the Device page, on the left toolbar, click *Device Dashboard*.
2. Review the dashboard.

   The Top Carriers list is limited to 10 carriers.

7.2 Viewing Devices in the Device List

View information on managed devices in the device list. This list displays details for each device, such as the state of approval, operating system, client ID, and corporate or personal ownership of the device.

Context

You can filter and sort the list as well as select and perform actions on a device in the list. For example, you can edit device information, delete a device, or perform security actions such as locking a device or remotely wiping it.

Procedure

1. On the Home page banner, click *Device*.
2. Review the device list.

   The system default view lists all devices and may span multiple pages. To select another view, see Selecting a System or Custom View for the Device List [page 306]. To create a custom view, see Creating Custom Device Views [page 307].
3. (Optional) Click the title of any column to sort by that column.

7.3 Viewing the Policies Linked to Devices

View the policies linked to a device. Devices are implicitly linked to policies through their common relationship with groups.

Procedure

1. On the Device page, select one or more devices.
2. On the left toolbar, click *Show/Hide Link*.

   The filters for the policy panel behave differently depending upon how many devices you have selected.
   - If you have one device selected:
     - All – displays all available policies, regardless of link state.
     - Linked – displays policies linked to the device.
     - Unlinked – displays policies that are not linked to the device.
     - Mixed linked – is not applicable when only one device is selected.

- If you have multiple devices selected:
  - All – displays all available policies, regardless of link state.
  - Linked – displays policies that are linked to all selected devices.
  - Unlinked – displays policies that are not linked to any of the selected devices.
  - Mixed linked – displays policies that are linked to some of the selected devices, but not all.

7.4 Viewing Groups Linked to Devices

View the groups linked to a device.

Procedure

1. On the Device page, select one or more devices.
2. On the left toolbar, click *Show/Hide Link*.

   The filters for the group panel behave differently depending upon how many devices you have selected.
   - If you have one device selected:
     - All – displays all available groups, regardless of link state.
     - Linked – displays groups linked to the device.
     - Unlinked – displays groups that are not linked to the device.
     - Mixed linked – is not applicable when only one device is selected.
   - If you have multiple devices selected:
     - All – displays all available groups, regardless of link state.
     - Linked – displays groups that are linked to all selected devices.
     - Unlinked – displays groups that are not linked to any of the selected devices.
     - Mixed linked – displays groups that are linked to some of the selected devices, but not all.

7.5 Custom Buttons on the Device Page

You can add custom buttons to the top toolbar on the device page. Custom buttons allow you to send information about devices that you select in the Afaria Administration console to Web pages.

To create custom buttons, add the following code to the `Afaria.Admin\web.config` file. The `configSections` code must be the first section in the `configurations` section.

```
<configuration>
  <configSections>
    <section name="DevicePageButtons"
type="Afaria.Admin.Utilities.CustomButtonsConfig"/>
  </configSections>
  <DevicePageButtons>
    <buttons>
```

```
      <add iconURL="<URL>" pageURL="<URL>" uniqueID="<string>"
toolTipText="<string>" typeFilterList="<list>" tenantNameFilterList="<list>"/>
    <buttons>
  </DevicePageButtons>
```

Each `add` line creates a button; this table describes the attributes that you can use to define the custom buttons:

Attribute	Description
iconURL	(Required) The URL of the image file for the button. If the URL starts with `<~/>`, it is relative to the root of the Afaria Administration console Web page. The image must be 16 by 16 pixels.
pageURL	(Required) The address of the Web page and the information that is sent to the Web page. Include the attributes for the selected device in this format: `<URL>?<attribute name>=%<device attribute>%&amp;<attribute name>=%<device attribute>%$amp;...` The URL can include: • `Uid` • `Name` • `Type` • `Approved` • `TenantID` • `Tenant` The device attributes are case-insensitive. If a value for the device attribute is unavailable, the URL includes the localized string of `unknown` for the device attribute.
uniqueID	(Required) The unique string that identifies the button. Keep the string short to minimize page load time.
toolTipText	(Optional) The string that appears as hover text for the button.
typeFilterList	(Optional) A comma- or semicolon-delimited list of device type IDs that determines the device types for which the button appears. Exclude this attribute to make the button visible for all device types.
tenantNameFilterList	(Optional) A semicolon-delimited list of tenant names that determines for which tenants the buttons appear. Exclude this attribute to make the button visible for all tenants. This attribute is case-insensitive and, before a match, the strings are trimmed to remove additional spaces.

7.6 Searching for Devices

Search across tenants for devices. Search criteria includes multiple, user-selected data, such as operating system, device ID, client name, and telephone number.

Procedure

1. On the Device page, on the left toolbar, click *Search*.
2. (Optional) In the Search dialog, type a search string for searching the client name field.

   You can use literal, or literal plus wildcard, characters to define the string. The search supports wildcard characters “*” and “?” for multiple characters and single characters, respectively.

   For example, type `br*n` to search for devices with names that have a "br" string and then an "n," such as "J Brown" and "LBromein."

   Leave the search string empty to include all client names.
3. For the tenant, OS, and field columns, select or unselect your criteria.

   The tenant list includes only the tenants in your user role.
4. Click *Search*.
   Results appear in the last column, grouped by tenant.
5. To view a tenant's results list, double-click the tenant in the list.
   A search result page opens with the tenant's list of devices that meet your criteria.
6. Review the results list and continue with operations.
7. (Optional) To restore the list to show all devices, on the left toolbar, click *Device List*.

7.7 Selecting a System or Custom View for the Device List

Select a system or custom view for the device list to display only those devices you are interested in.

Context

You can also set a device view as the default view for all users. The default view is set on a per-tenant basis. If you set a default for the system tenant, this view is propagated down to all tenants unless there is a default set at the tenant level. You can also override the system-wide default at the tenant level by setting a different view for an individual tenant.

Procedure

1. On the *Device* page, on the left toolbar, click *Select View*.
2. Navigate to the *System Views* and *Custom Views* folders, then click the view you want to use.
   - *System Views* folder – contains views with predefined popular filters applied, such as all devices, device type iOS, or devices with an unapproved status.
   - *Custom View*s folder – populated custom views that you create.
3. On the *View* toolbar, click *Select* to open the view in the *Device* page.
4. To set a device view as the default, select a view from the list and click *Pin as default view* on the *View* toolbar.

   To unset a view as the default, use the *Unpin as default view* button. When you unset a view, the default view reverts to the *All Devices* view.

7.8 Creating Custom Device Views

Create a view for the Device page that includes your columns of choice and meets your filter criteria. For example, you can define a view that returns only Android devices that have Bluetooth turned off and displays only columns for client name, user name, and phone number, all sorted by user name.

Context

Fields that are common to most or all device types, such as device model or directory variables, are listed under the "Server" group in the Data Fields list. Server subgroups for variables and user-defined fields display only when definitions exist.

Procedure

1. On the Device page, on the left toolbar, click *Select View*.
2. On the view list, select the Custom Views folder or one of its child folders.
3. (Optional) To define a new folder for the view, on the View toolbar, click *Add new folder within currently opened folder*, enter a folder name and note, and then click *Save*.
4. With a custom view folder selected, on the View toolbar, click *Add new view within currently opened folder* to open the Custom View dialog.
5. Enter a view name and note.
6. To select the columns to include in your view, select fields in the Data Field list and click the *Add column* icon.

   You can further define the columns in the list by selecting a row and using the icons on the right side to move a row's order and edit a row's alias, show/hide property, and sort properties. Row order in this list indicates the resulting custom view's column order from left to right.

> **Note**
>
> If you set a column's show option to "hide", you must also select a sort option ("sort ascending" or "sort descending") or SAP Afaria deletes the column on save.

7. To define criteria for which devices are returned in your view, select fields in the Data Field list, click the *Add criteria* icon, select the row in the list, and click the *Edit* icon that is available on the right side to edit a row's criteria definition.

> **Note**
>
> If you add fields of type Boolean, certain operators that are not valid with Boolean field comparison will not be used in the filter SQL construction. Invalid filter statements will not be constructed or executed.

8. You can group the Criteria fields to meet your specific needs. To enable the grouping feature:
    1. Hold down the SHIFT key and select at least two criteria fields using the left mouse button.
    2. While continuing to hold the SHIFT key, click the last row you intend to group a second time.
       The Group criteria items icon appears on the right side of the grid.
    3. Click on the *Group criteria items* icon to group the fields.
       You will now see open and close parentheses around the selected fields.
    4. To remove the grouping, perform the same steps to select the fields, click the last field a second time while holding the SHIFT key, and click on the *Ungroup criteria items* icon on the right side of the grid.
9. (Optional) When the view is defined, click the *Show as SQL statement* link to see the select statement that will be executed to display your custom data view.
10. Click *Save*.

Results

The view is added to your custom views list. Select the view to show devices that meet the view's criteria.

7.9 Editing a Device

Edit device information, such as its Self-Service Portal registered user name, device name, and access control policies.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Edit*.
3. Edit data as appropriate.
4. On the top of the page, click *Save*.

7.9.1 Editing an Android Device

Edit device information, such as device name, device ownership type, Self-Service Portal registered user name, and SMS address.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Edit*.
3. Edit data as appropriate.
   - Device – click *Setup* to open the ID Setup dialog and select naming options:
     - Optional Prefix – enter a prefix to use for the name. For example "Sales_".

       > **i Note**
       >
       > The optional prefix is temporary for Android devices. This prefix is removed from the device ID during the next device connection.

     - Data Column – select a data item to concatenate with the prefix. The list includes predefined columns, the user name variable, and any additional user-defined substitution variables you defined. Select something meaningful to your organization to facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
       If you select a data item that is based on a user's response to a user prompt that you add to the enrollment policy, the user's response forms the name, even if it is inaccurate. For example, if you

prompt for an e-mail address and the user incorrectly types the address, the name contains the incorrect address, even if the correct address is later stored in inventory.

- Device owner – set a corporate or personally owned device, or reset to the default value.
- (SSP) Registered User – device user name, as a user would provide for Windows NT or LDAP authentication in your SAP Afaria environment, such as `<Domain>\<UserName>`. If users have enrolled in management, this is the user name they provided for authentication on the Self-Service Portal or in response to a user name prompt.
- SMS address – address to which the server sends outbound notifications to connect and run a channel or apply a policy.

4. On the top of the page, click *Save*.

Related Information

Substitution Variables [page 29]

7.9.2 Editing an iOS Device

Edit device information, such as device name, device ownership type, values for user variables, Self-Service Portal registered user name, and access control policies.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Edit*.
3. Edit data as appropriate.
   - Device – click *Setup* to open the ID Setup dialog and select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. Selecting something meaningful to your organization can help facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
   - Device owner – set a corporate or personally owned device or reset to default value.
   - (SSP) Registered User – device user name, as a user would provide for Windows NT or LDAP authentication in your SAP Afaria environment, such as `<Domain>\<UserName>`. If users have enrolled in management, this is the user name they provided for authentication on the Self-Service Portal or in response to a user name prompt.
   - Notification Address – if a phone number is unavailable for SMS messaging, address for the server to send outbound notifications to configure the Self-Service Portal client.
   - Email Address and password – e-mail address and password for access control policy.
   - Access Control Policy – click *Setup* to open the Device > Access Control Policy Setup dialog. Accept (use default policy) or override (use explicit policy) the enterprise default policy for iOS, as defined on

the iOS tab on the *Server* > *Configuration* > *Access Control Option* page. Select one of the following options to use an explicit policy:

- Always allow – allow synchronization requests at all times.
- Always block – block synchronization requests at all times.
- Allow when:
  - Administered by mobile device management – the device is under mobile device management (MDM) control.
  - Afaria installed – the Afaria App Store application is installed.
  - Assigned policy delivered – assigned policies are reported to the Self-Service Portal server as delivered and installed on the device, as verified in the Policy Delivery log.
  - Device hardware encrypted – the device has the hardware encryption feature enabled.
  - Device uncompromised – the device's most recent connection did not report the device's status as jailbroken.

4. (Optional) Substitution – if you include user-defined substitution variables in policies that are planned for this device, define values for the appropriate variables. If the variable is not yet on the list, click *Add* to enter the variable name and value for the current device, as appropriate for your requirements.

   The variables on the list are global for the current tenant. The values you define for the variables are for only the current device.
5. On the top of the page, click *Save*.

Related Information

Substitution Variables [page 29]

7.9.3 Editing a Windows Mobile Device

Edit device information, such as device name, device ownership type, Self-Service Portal registered user name, and SMS address.

Procedure

1. On the Device page, select a device.
2. On the top toolbar, click *Edit*.
3. Edit data as appropriate.
   - Device – click *Setup* to open the ID Setup dialog and select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. Selecting something meaningful to your organization can help facilitate effective searching, create a value for building custom views, or differentiate like-named devices.

- Device owner – set a corporate or personally owned device or reset to default value.
- (SSP) Registered User – device user name, as a user would provide for Windows NT or LDAP authentication in your SAP Afaria environment, such as `<Domain>\<UserName>`. If users have enrolled in management, this is the user name they provided for authentication on the Self-Service Portal or in response to a user name prompt.
- SMS address – address to which the server sends outbound notifications to connect and run a channel or apply a policy.
- User IP address – if an SMS address is unavailable, address to which the server sends outbound notifications to connect and run a channel or apply a policy.

4. On the top of the page, click *Save*.

7.9.4 Editing a Windows Device

Edit device information, such as device name, device ownership type, Self-Service Portal registered user name, and IP address.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Edit*.
3. Edit data as appropriate.
   - Device – click *Setup* to open the ID Setup dialog and select naming options:
     - (Optional) Optional Prefix – enter a prefix to use for the name. For example "Sales_".
     - (Optional) Data Column – select a data item to concatenate with the prefix. Selecting something meaningful to your organization can help facilitate effective searching, create a value for building custom views, or differentiate like-named devices.
   - Device owner – set a corporate or personally owned device or reset to default value.
   - (SSP) Registered User – device user name, as a user would provide for Windows NT or LDAP authentication in your SAP Afaria environment, such as `<Domain>\<UserName>`. If users have enrolled in management, this is the user name they provided for authentication on the Self-Service Portal or in response to a user name prompt.
   - User IP address – address to which the server sends outbound notifications to connect and run a channel or apply a policy.
4. On the top of the page, click *Save*.

7.9.5 Editing a Windows Phone Device

Edit specific Windows phone information, such as Device Owner, (SSP) Registered User, and Email Address.

Procedure

1. On the Device page, select a Windows phone device.
2. On the top toolbar, click *Edit*.
   - Device owner – set a corporate or personally owned device or reset to default value.
   - (SSP) Registered User – device user name, as a user would provide for Windows NT or LDAP authentication in your Afaria environment, such as `<Domain>\<UserName>`. If users have enrolled in management, this is the user name they provided for authentication on the Self-Service Portal or in response to a user name prompt.
   - Email Address – e-mail address for access control policy.
3. On the top of the page, click *Save*.

7.9.6 Device Names Using Database Specified Values

When using the database specified values to name devices, SAP Afaria uses the data in a specific database table and column to name devices.

Database Specific Value is a data column option for device naming when you are:

- Creating an enrollment policy for Windows CE, Windows Mobile Professional, Windows Mobile Standard, or any Windows variation.
- Editing any device type.

Syntax: `tableName.columnName`

Consider these items:

- It is your responsibility to ensure that the table, column, and row exist in the Afaria database.
- The value is retrieved during each device's initial connection, but always returns the first row of the table.
- It is your responsibility to populate the table at connection time. Consider using techniques such as stored procedures and triggers to detect a connection and the device's identity, and to populate the table accordingly.

7.10 Performing Security Actions on Devices

You can send security commands to devices from the Afaria Administration console.

Context

The security commands vary by device type and state. Using security commands requires appropriate role permissions.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click a security command.

   Security Actions for Android Devices [page 314]
   The following security commands are available for Android devices.

   Security Actions for iOS Devices [page 316]
   The following security commands are available for iOS devices.

   Security Actions for Windows Mobile Devices [page 317]
   The following security command is available for Windows Mobile devices.

   Security Actions for Windows Phone Devices [page 318]
   The following security commands are available for Windows Phone devices.

   Security Actions for Windows 8.1 and Higher Devices [page 319]
   The following security commands are available for Windows DM (Windows 8.1 or higher) devices.

   Security Actions for Windows DM 10 [page 320]
   The following security commands are available for Windows DM 10.

7.10.1 Security Actions for Android Devices

The following security commands are available for Android devices.

The SAP Afaria server attempts to send commands using Firebase Cloud Messaging (FCM), formerly Google Cloud Messaging (GCM), first and then Short Message Service (SMS). The device receives and executes the command without user interaction.

Action	Description
Lock Device	This command locks the device. The device remains locked until the user enters the correct passcode. While locked, the device still allows emergency calls. The device lock is not removed if the user resets the device or removes the battery.
Delete Device Data	Resets your device to factory condition, including removing the SAP Afaria client
Unlock - Clear Passcode	Removes an Administrator Lock and clears the passcode
Remote Wipe Email	Deletes all SAP Afaria provisioned Exchange accounts on the device including those configured in NitroDesk TouchDown. When you use this button, you are prompted to include a secure wipe of the TouchDown SD card. When you choose to perform a secure wipe, NitroDesk TouchDown deletes only the data it has stored on the card. **i Note** This button is only displayed if an SAP Afaria provisioned Exchange account is configured on the device.
Lock KNOX Container	Locks the KNOX container. When a KNOX container is locked, users are prevented from logging in. The container can only be unlocked using the *Unlock KNOX Container* button on the Device toolbar. You can use this button to secure data in the KNOX container if, for example, the device is lost or stolen. **i Note** This button is only displayed if a Samsung KNOX container is installed on the device.
Unlock KNOX Container	Unlocks a locked KNOX container. For example, you can use this button to unlock a locked KNOX container after a lost or stolen device has been recovered. **i Note** This button is only displayed if a Samsung KNOX container is installed on the device.

Action	Description
Remove KNOX Container	Deletes all applications and data in the KNOX container and removes the container from the device. Use this button when, for example, a user leaves your company. **i Note** This button is only displayed if a Samsung KNOX container is installed on the device.
Reset KNOX Container Password	Resets the user's password on the KNOX container. Use this button when a user forgets their password. When a password is reset, the user is prompted to enter a new password the next time they try to access the KNOX container. **i Note** This button is only displayed if a Samsung KNOX container is installed on the device.

7.10.2 Security Actions for iOS Devices

The following security commands are available for iOS devices.

The SAP Afaria server attempts to send the command using the APNS. The device receives and executes the command without user interaction.

Action	Description
Lock Device	This command locks the device. The device remains locked until the user enters the correct passcode. While locked, the device still allows emergency calls. The device lock is not removed if the user resets the device. You can add a message and phone number when sending the lock command. The device displays the message and phone number on the lock screen.
Remote Wipe	This command resets the device and removes it from SAP Afaria management. If you choose this option, the user must connect the device to iTunes to restore data.
Unlock - Clear Passcode	This command unlocks the device and removes the passcode. If the device has a policy that requires a passcode, the device prompts the user to create a new passcode. An outbound notification through SMS or FCM/GCM is provided.

Action	Description
Remove Control	This command removes the device and all device content from SAP Afaria MDM control. The device remains enrolled in SAP Afaria management with limited management capabilities.
Modify Access Control Policy	This command opens the access control policy for the device.
Change Device Name	This command changes the current name of device in the Afaria Administration console.
Clear Restriction Password	This command changes the current name of the device. Once the new name is provided, the device user is notified with this change and the new name appears on the device. However, in the administration console, the new name is reflected on completion of the subsequent device inventory collection.
Clear Activation Lock	This command clears the activation lock on a supervised device so that it can be wiped and reactivated for another user. Activation lock prevents unauthorized people from erasing and reactivating a lost or stolen device. It is enabled when a user sets up Find My iPhone on the device. To reactivate a device after you have cleared the activation lock, you must enter the device bypass code in the *Password* field. The bypass code is generated by the device, retrieved by SAP Afaria, and stored in device inventory. This button is only available if the device is supervised, *Allow activation lock* is enabled in the enrollment policy, and Find My iPhone has been set up on the device.

7.10.3 Security Actions for Windows Mobile Devices

The following security command is available for Windows Mobile devices.

The SAP Afaria server attempts to send the command using Short Message Service (SMS) first and then TCP/IP. The device receives and executes the command without user interaction.

Action	Description
Reset Password	Reset the password on Windows Mobile devices.

> **i Note**
>
> If you disabled the device's external card using configuration policy's port control properties, a remote wipe command that includes wiping the external data card leaves the card intact because the device cannot mount the card. For Windows Mobile 6.1 and later, if you disabled the device's SMS messaging using configuration policy's port control properties, Microsoft messaging applications on the device do not receive the remote wipe command.

7.10.4 Security Actions for Windows Phone Devices

The following security commands are available for Windows Phone devices.

Action	Description
Remote Wipe	This command removes the device from Afaria management and resets it to factory settings as a brand new device.
Remove Control	This command removes the device and all device content from Afaria MDM control. The device remains enrolled in Afaria management with limited management capabilities.
Lock Device	This command locks the device; the device remains locked until the correct passcode is entered. The device lock is not removed even if the battery is replaced. **i Note** The lock action applies only to Windows Phone 8.1 devices, though it appears on both Windows Phone 8 and Windows Phone 8.1 devices. For the lock action to work, a passcode should have been applied on the device. Lock action is applied only in the next DM session initiated from the device.
Remote Ring	This command produces an audible ring on the device regardless of the volume set on the device. When the administrator initiates this action, a push notification is triggered and the device connects back to Afaria server. An MDM session is established and the remote ring action is completed.

Action	Description
Lock Device and Reset Password	This command locks the device and resets the password on the device. A new password is generated on successful completion of this action, and the password appears in the Device Inspector tab. The administrator can select the option to share the password via e-mail or Self-Service Portal, either while initiating the command or afterwards from the Device Inspector panel. The administrator can use this command to revoke the password, if the device goes out of compliance. This command works irrespective of whether a password is set on the device or not. The password value conforms to the minimum password complexity requirements of the merged policies that are set on the device. If no password policy has been set on the device, the device generates an 8-digit numeric password and sets it for the device. **i Note** This action works only for Windows Phone 8.1 Update 1 devices and onwards.

i Note

The remote wipe and remove control actions will not occur until the device initiates the connection, as Windows Phone devices do not support outbound connections. While disconnecting from Afaria management, the Microsoft Exchange e-mail account configured by Afaria on the device will also be removed, although the message that appears on the device may indicate otherwise.

7.10.5 Security Actions for Windows 8.1 and Higher Devices

The following security commands are available for Windows DM (Windows 8.1 or higher) devices.

Action	Description
Unregister Device	This command removes the device from the 'My Devices' list and from the Self-Service Portal. The device remains enrolled in Afaria management.
Remove Control	This command removes the device and all device content from Afaria MDM control.
Lock Device	This command locks the device; the device remains locked until the correct passcode is entered. The device lock is not removed even if the battery is replaced.

7.10.6 Security Actions for Windows DM 10

The following security commands are available for Windows DM 10.

Action	Description
Remote Wipe	This command removes the device from Afaria management and resets it to factory settings as a brand new device.
Remove Control	This command removes the device and all device content from Afaria MDM control. The device remains enrolled in Afaria management with limited management capabilities.

7.11 Viewing Certificate Information

This task describes how to view information about certificates issued by your certificate authority.

Context

SAP Afaria includes device system views for active, expired, expiring soon, issued, and revoked certificates.

> **i** Note
>
> Revoked certificates are marked as either "Revoked" or "Locally Revoked" in the *Revocation State* column of the certificate view. "Revoked" indicates certificates that have been revoked at the Certificate Authority (CA) and added to the Certificate Revocation List (CRL). "Locally Revoked" indicates certificates that are revoked locally. These certificates are expiring or expired certificates that are no longer active and cannot be used. To improve performance, these certificates are not revoked at the CA nor added to the CRL.

Procedure

1. On the Device page, on the left toolbar, click *Select View*.
2. Expand *System Views* and then *Device Certificates*.
3. Select an appropriate view and click *Select*.

   SAP Afaria lists all matching certificates and includes information such as the device ID, effective date, expiration date, and revocation state.

7.12 Renewing and Revoking Certificates

This task describes how to renew expired or expiring certificates and revoke active certificates.

Context

You may want to revoke a certificate on a lost or stolen device.

Procedure

1. On the Device page, on the left toolbar, click *Select View*.
2. Expand *System Views* and then *Device Certificates*.
3. Select an appropriate view and click *Select*.

   SAP Afaria lists all matching certificates and includes information such as the device ID, effective date, expiration date, and revocation state.
4. Select the certificate you want to renew or revoke and click the Renew Certificate or Revoke Certificate button as appropriate.

7.13 Device Ownership

Device ownership can be either personal or corporate.

Default Device Ownership [page 322]
SAP Afaria assigns default ownership based on device type.

Changing Device Ownership [page 322]
You can set the owner of the device to corporate, personal, or the default setting.

Importing a Corporate Device List [page 322]
You can import a corporate device list to override the default personal device ownership settings for Android and iOS devices with your corporate device ownership settings.

7.13.1 Default Device Ownership

SAP Afaria assigns default ownership based on device type.

Device	Default Ownership
Android	Personal
iOS	Personal
Windows	Corporate
Windows CE	Corporate
Windows Mobile Professional	Corporate
Windows Mobile Standard	Corporate
Windows Phone	Personal

7.13.2 Changing Device Ownership

You can set the owner of the device to corporate, personal, or the default setting.

Procedure

1. On the Device page, select a device.
2. On the top toolbar, click *Modify Device Owner*.
3. Select Corporate, Personal, or Reset to Default.
4. Click *Yes, Continue*.

7.13.3 Importing a Corporate Device List

You can import a corporate device list to override the default personal device ownership settings for Android and iOS devices with your corporate device ownership settings.

Context

A corporate device list is a CSV file that provides a unique device identifier such as user name, phone number, or IMEI number for your corporate devices. When you import the device list, the A_Corporate table is populated

with device identifying values. As devices identified on the list connect with new hardware inventory reports, the corporate device override is applied to the device record.

The corporate device list import process ignores values that are redundant of any value it already processed in the current list.

For more information on creating a corporate device list, see *Corporate Device List Requirements*.

Procedure

1. On the *Device* page, on the left toolbar, click *Import Corporate Device List*.
2. Click *Browse*, navigate to the import file (`.CSV`), and click *Open*.
3. On the File Upload dialog, navigate to an import file (`.CSV`) with required syntax, then click on the file to select it.
4. On the File Upload dialog, click *Open* to start the import.
   The import file is processed. Processing populates the A_Corporate_Device table with the values. You return to the Import Corporate Device List dialog with a results message.
5. Click the *Close* icon to return to the *Device* page.

Corporate Device Import List Requirements [page 323]
You can create and import a corporate device list for corporate device ownership settings. The import file must be of type `.CSV` and use appropriate syntax.

7.13.3.1 Corporate Device Import List Requirements

You can create and import a corporate device list for corporate device ownership settings. The import file must be of type `.CSV` and use appropriate syntax.

Corporate Device List File Requirements

- Import file type – comma-separated values (`.CSV`, also known as comma delimited).
  You can use editors such as Notepad and Microsoft Excel to edit the device list file.
- File structure:
  - First row, first field – **`CorporateDeviceID`**
  - Additional rows, one per device to update, first field – `<DeviceIdentifyingField>`

Corporate Device List Device-Identifying Fields

Android and iOS use different device-identifying fields.

For Android, valid fields are:

- From the Device Inspector Summary page:
  - User, but only when populated by enrollment policy user prompts
  - Phone number
  - IMEI (IMSI, MEID)
  - ClientFriendlyName
- From the Device Inspector Hardware pages:
  - Android > Phone SIM serial number
  - Android > WIFI MAC address
  - Android > PhoneSIMSubscriberID
  - Bluetooth > Device address

> **Note**
>
> Hardware inventory item Device > Serial number is not guaranteed to be unique across all Android devices.

For iOS, valid fields are:

- From the Device Inspector Summary page:
  - User, but only when populated by enrollment policy user prompts
  - Phone number
  - IMEI
  - UDID
  - Serial number
- From the Device Inspector Hardware pages:
  - WIFI > WIFI MAC address
  - Bluetooth > Bluetooth MAC address

> **Example**
>
> ```
> CorporateDeviceID
> A0000225CAC89
> mycompany.com/lbrowne
> 6db9a85857f6845
> 5555428305
> ```
>
> > **Note**
> >
> > You can use different device identifiers in a single corporate device list file.

7.14 Moving Devices to Another Tenant

You can move a device to a different tenant in the Afaria Administration console.

Context

When you move a device to a different tenant, SAP Afaria moves the device data to the new tenant and sends the policies for the tenant to the device when it connects next. All future sessions for the device are associated with the tenant.

If you move a Windows Phone device to another tenant that has a different AET uploaded, you must re-enroll the device to enable features such as application management, push notification, and location collection.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Move to Tenant* to open the Tenant Browser dialog.
3. Select a tenant.
4. On the dialog toolbar, click *Select*.

7.15 Sending Messages to Devices

You can use the Afaria Administration console to send email or push notification messages to devices.

Prerequisites

For Windows DM, ensure you have enabled Exchange ActiveSync. For more information on this, see *Exchange ActiveSync* section for Windows DM in this document.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Send Message*.
3. To send the message as an email message, select *Email* and type a subject for the email message in the *Subject* field.

> **Note**
>
> For Windows DM user, Step 4 is not applicable as the Push Notification feature is not available. Proceed to Step 5.

4. To send the message using a platform-specific notification service, select *Push Notification*.
   - Apple Push Notification Service (APNS) for iOS devices
   - Microsoft Push Notification Service (MPNS) for Windows Phone devices
   - Firebase Cloud Messaging (FCM), formerly Google Cloud Messaging (GCM), for Android devices
5. Enter a message (with a maximum length of 1024 characters) in the text box.

   For Windows Phone, the length of the notification message received on the device, when the Afaria application is closed, is restricted as per the limitations of the device operating system.
6. Click *Yes, Continue* to send the message.

   Select *Server* > *Server Log* to verify that the message has been sent.

Related Information

Exchange ActiveSync [page 244]

7.16 Connecting a Device to Apply Policies

Send a notification to a device to make it connect immediately to an SAP Afaria server and apply its policies.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Apply Policies*

Results

The server attempts to notify the device to connect and apply its policies. If notification is successful, the device attempts to connect to the server. The Messages log captures the success or failure of sending the notification. If the notification fails due to an unknown or invalid address, you can edit the device to update the SMS, IP, or SMTP address.

7.17 Connecting a Device to Run a Channel

Send a notification to a device to make it connect immediately to an SAP Afaria server to request a specific, published channel. For the device to be able to run the channel, the channel must be included in one of its session policies.

Procedure

1. On the *Device* page, select a device.
2. On the top toolbar, click *Run Channel*.
3. Select one published channel that is appropriate for the selected device, and include it one of the device's session policies.
4. On the Run Channel toolbar, click *Select*.

Results

The server attempts to notify the device to connect and request the channel. If notification is successful, the device attempts to connect to the server and request the selected channel. The Messages log captures the success or failure of sending the notification. If the notification fails due to an unknown or invalid address, you can edit the device to update the SMS, IP, or SMTP address.

7.18 Deleting a Device or its Data from the Server

Delete a device's record and all of its data from the server, or keep the device record but delete some of its data from the server.

Procedure

1. On the Device page, select one or more devices.
2. On the top toolbar click, *Delete*.
3. Select *All Device Data Below* to delete the device and all its data from the server, or select the data of interest from the list to keep the device but delete the selected data from the server.

7.19 Getting Log Files from Devices

You can get the log files from an Android device or an iOS device using the Afaria Administration console.

Procedure

1. On the *Device* page, select an Android device or an iOS device.
2. On the top toolbar, click *Get Log File*.
   A message "Notification sent to device" is displayed. To download the log file, see the topic *Downloading the Client Log*.

7.20 Windows Phone Custom Branding

You can customize the SAP Afaria client (xap) for Windows Phone devices, with your own corporate brand images and text.

Branding details must be uploaded first, before uploading the signed client. After saving the branding details, the SAP Afaria client (the xap file) must be downloaded, signed and uploaded so that the branding information gets picked up in the application. The custom branding appears on the device directly, once the client is downloaded and installed on the device.

Branding details are inherited from the system tenant to the non-system tenants. To change the branding in the non-system tenant, the branding details have to be updated in the non-system tenant, and the SAP Afaria client must be downloaded, re-signed and uploaded.

Adding Custom Branding to Afaria Windows Phone Applications [page 328]
Customize the SAP Afaria client for Windows Phone devices, with your corporate brand using custom background images, icons, and text.

7.20.1 Adding Custom Branding to Afaria Windows Phone Applications

Customize the SAP Afaria client for Windows Phone devices, with your corporate brand using custom background images, icons, and text.

Procedure

1. On the Home page Server tile, click Configuration.

2. Navigate to *Component* > *Windows Phone* page.
3. On the *Branding* tab, select default or specify custom values for App Name and Tile Name.
4. Select default or specify custom About Text for the application.

   This text will appear on the device.
5. Click *Language Option* to define the text in additional languages, as required, for devices in supported regions.

   Language Option is available only if you specify custom about text. The about text is localized in all languages supported by the Windows Phone application. If no localized text exists for the language on the device, the custom text, as specified in the branding page appears on the device. Please note that this text can be empty, in which case the about text on the device will be blank.

   Scenario1: When default is selected: We get the default about text for all the languages (unbranded).

   Scenario2: When custom about text is selected: When the about text for different languages are inserted (administrator must provide the text in these languages as the Windows Phone device will not take care of localization), the about text displayed on device is as set by the administrator for the respective languages. However, for those languages which are not set by the administrator, the custom default about text takes precedence. Custom default about text can be empty, in which case the about text on the device will be blank.
6. Select default or custom option for splash screen, background image, app icon, and tile icon (.JPG or .PNG).
7. Click *Browse* and select the required custom branding images.
8. Click *Save*.
9. On the *General* tab, download the unsigned SAP Afaria client (xap).

   After you sign and upload the custom branded xap, the new or the updated branding appears when the SAP Afaria client (xap) is opened on the device.

7.21 Configuring Password Reset and Expiry Details for Windows Phone

Configure the expiry time interval for the new password that is generated when the administrator initiates the Lock Device and Reset Password action for a device. Compose the password reset e-mail message for the user.

Prerequisites

For the e-mail message to function properly, the user's exchange account must be configured using Afaria; the inventory collection should be able to retrieve the account information.

Procedure

1. On the Home page Server tile, click *Configuration*.
2. Navigate to *Component* > *Windows Phone*.
3. On the Password Expiry tab, specify the time period after which the newly generated password expires.

   The default is one hour.
4. In the Reset Password Email section, compose the e-mail message, or use the default template to send the new password to the user.
5. Click *Save*.

8 Device Activity Collection

SAP Afaria can monitor and report on device activities for enrolled devices.

Depending on the device type, monitored activities include:

- Cellular data
- Wi-Fi data
- Outgoing and incoming phone calls
- Outgoing and incoming Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages
- International roaming status and usage

No additional server components are required, but you must configure the SAP Afaria Server and devices for device activity collection. Use the Afaria Administration console to configure device activity settings on a tenant-by-tenant basis.

Definitions of data connection details collected by device type, for example, Bearer Type and MNC.

Device Activity Messages by Device Type [page 340]
Definitions of message details collected by each device type, for example, cell ID and Type. Device Activity messages are not supported on iOS devices.

Configuring General Device Activity Settings [page 340]
Enable and configure device activity data collection by configuring the Afaria Administration console.

Configuring Device Activity Settings for Roaming [page 341]
Configure Afaria Device Activity International Roaming settings to notify users that their devices are in an international roaming state and additional charges may apply.

Configuring Device Activity Settings for Data Views [page 342]
Customize how SAP Afaria Device Activity data appears in Data Views.

Enabling Device Activity Cleanup [page 343]
You can use the Afaria Administration console to configure how the SAP Afaria Server removes old device activity data.

Customizing Device Activity Cleanup Schedule [page 343]
Customize the date and time at which the SAP Afaria Server deletes old device activity data.

Creating Custom Device Activity Views [page 344]
Select columns for a custom device activity view, and define criteria for selecting which subscribers populate your view.

Viewing the Device Activity List in the Default View [page 345]
Display the device activity list in the default system-defined data view.

Viewing the Device Activity List in the Non-default View [page 345]
Display the system-defined data views that allow you to review device activity data.

Viewing the Device Location [page 345]
You can view the last location that a device reports to SAP Afaria on a map.

Client Logging [page 346]
Retrieve and export client logs for iOS and Android devices at the request of SAP Afaria support teams to help validate and resolve issues.

8.1 Preparing Devices for Activity Collection

Prepare the device for activity collection by installing the SAP Afaria client and enabling Location Services.

Procedure

1. Install the SAP Afaria client on the device and enroll in SAP Afaria device management.
2. During the application installation, authorize and enable Location Services.

   On iOS devices, the SAP Afaria client must continuously run for device activity to be able to monitor activities. Enabling Location Services for SAP Afaria keeps the SAP Afaria client continuously running in the background.

8.2 Device Activity Collection Considerations

Afaria Device Activity data collection allows you to collect various types of data from enrolled devices and use it for monitoring and report purposes.

> **i** Note
>
> Device activity data collection is disabled by default.

Starting data collection:

- If user authorization is required, device activity data collection begins after the user accepts device activity enrollment. The user response (accept or decline) is sent back to the Afaria server and appears in the Opt-in column of the Subscribers view.
- If user authorization is not required, device activity data collection begins after you enable device activity collection; restart the Afaria server service; and the device connects to the server.
- A device retains its device activity collection preference (accept or decline) when it changes tenant. However, if the user has previously declined and you move the device to a tenant where user acceptance of device activity is not required, device activity collection begins without further user notification.

Ongoing data collection:

- Device activity data is associated with a subscriber. If a device has an SIM, the subscriber is identified by the SIM IMSI or ICCID. Device activity data moves with the SIM from device to device.
- On iOS devices, device activity data collection stops automatically if the user turns off location services for more than 10 minutes.

8.3 Device Activity Collection Frequency

Data collection frequency settings indicate when Afaria collects device activity data from enrolled devices.

The frequency of data collection varies by device type.

- For iOS devices, Afaria collects device activity data once a day between 2:00 a.m. and 3:00 a.m. (client local time).
- For Android devices, Afaria collects device activity data at the frequency based on the schedule settings defined in the configuration policy.
- For Windows Phone devices, a background service enabled for the Afaria application, runs along with other scheduled operating system tasks and collects device activity data. This background task runs approximately every 20 minutes and sends the device coordinates to the Afaria server.

8.4 Collecting Device Activity Data

Use the Afaria Administration console to configure SAP Afaria to collect device activity data.

Procedure

1. On the *Server* page, click *Configuration*.
2. Click *Component* > *Device Activity*.
3. On the *General Settings* tab, perform the following tasks:
   a. Select *Enable Activity Collection*.
   b. To collect phone numbers that make calls to devices, select *Collect Remote Party Phone Numbers*.
   c. To collect location data from devices, select *Collect Subscriber Location Information*.
   d. To prompt users to allow SAP Afaria to collect device activity data, select *Prompt Subscriber for Activity Enrollment*.
   e. Type the message that devices display when prompting users to allow the collection of device activity data.

   If you select *Prompt Subscriber for Activity Enrollment*, data collection begins when the user accepts the device activity collection prompt on the device.
4. To prompt users to accept device activity collection, select *Prompt Subscriber for Activity Enrollment*.

   For Windows Phone devices, this option applies only if you select Collect Subscriber Location Information.
5. In the *Enrollment Notification* field, type the message that devices display when prompting users to accept device activity collection.
6. Click *Save*.
7. Click *Restart Server*.

8.5 Stopping Device Activity Collection

Stop the SAP Afaria Server from collecting device activity data.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.
2. On the *General Settings* tab, unselect *Enable Activity Collection*.
3. Save changes.
4. Click *Restart Server* to restart the SAP Afaria Server service.

After you restart the server, device activity data collection stops for each device connecting to the server.

8.6 Reprompting for Device Activity Enrollment

Reprompt users and resend the Device Activity enrollment notifications to those who have previously accepted or declined enrollment.

Prerequisites

Before you set up the reprompt, verify that *Prompt Subscriber for Activity Enrollment* is selected on the Device Activity General Settings tab on the *Server* > *Configuration* > *Component* > *Device Activity* page.

Procedure

1. On the Device page, select *Activity List*.
2. Navigate the Activity views, select *Subscribers view*, and click *Select*.
3. Select a subscriber and click *Reprompt* to resend the notification.

   The Opt In column in the Subscribers view indicates which users have accepted or declined enrollment.

   The user receives either the default enrollment notification or the custom notification you set up on the Device Activity General Settings page.

8.7 Subscriber Data Collected by Device Type

Definitions of subscriber data, such as IMSI, ICCID, and MSISDN, collected by each device type.

Subscriber Data	iOS	Android	Windows Phone	Definitions
IMSI		X		International Mobile Subscriber Identity, conforming to International Telecommunication Union (ITU) standard.
ICCID	X			Integrated Circuit Card Identifier, conforming to International Telecommunication Union (ITU) standard.
Cell ID		X		Last reported cell ID. On CDMA networks, the Base Station ID (BID).

Subscriber Data	iOS	Android	Windows Phone	Definitions
Current Afaria Client ID	X	X	X	SAP Afaria client global unique identifier (GUID).
Current Device ID	X	X		iOS – Unique Device Identifier (UDID), Wi-Fi MAC Address. Android - International Mobile Equipment Identity (IMEI).
MSISDN		X		Mobile Subscriber Integrated Services Digital Network Number which is the literal phone number as reported by the device. Not all SIM cards, specifically in Europe, are preprogrammed with an MSISDN.
Home MCC	X	X	X	Home network Mobile Country Code.
Home MNC	X	X	X	Home network Mobile Network Code.
Activity Last Collected	X	X	X	Date on which Device Activity data was last posted on the server by the device.
Last MCC	X	X		Last reported Mobile Country Code (MCC).
Last MNC	X	X		Last reported Mobile Network Code (MNC). On CDMA networks, the network System Identifier (SID).
Latitude	X	X	X	Last reported approximate latitude, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location.
Longitude	X	X	X	Last reported approximate longitude, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location.
Location Last Determined	X	X	X	Date and time of the last location change.
Opt In	X	X	X	User answer to request for Device Activity Enrollment (accepted/declined).
Roaming Change Date	X	X		Date and time of the last roaming state change.
Status of Location Services	X	X	X	Status of Location Services on the device (enabled or disabled).

8.8 Removing Device Activity Data for a Subscriber

Remove all device activity data related to a subscriber.

Procedure

1. On the Device page, on the left toolbar, click *Device List*.
2. Select a subscriber.
3. On the top toolbar, click *Delete*.
4. Select *Device Activity*.
   All device activity data collected for the subscriber is deleted, regardless of when it was collected.

8.9 Hardware Inventory Data Collection

Due to several factors, SAP Afaria cannot collect all inventory information from all devices types, nor can it collect all the same inventory items from all of the same device types. Understanding these variations can help you better understand your Afaria inventory data and custom views.

Several device and environmental variables can impact the ability to collect phone, network, identifier, and other data from your device. For example:

- Device type
- Device manufacturer and model exposed APIs
- Mobile/cellular service provider
- Carrier network type
- Operating system implementation
- Device's power state
- Device's settings for Wi-Fi radio state

Inventory Data Elements with Greatest Variability

For smartphones and other handheld devices, the greatest variability for data collection is often observed on these data elements:

- Serial number and similar identifiers, such as International Mobile Equipment Identity (IMEI) and Mobile Equipment Identifier (MEID)
  - For Android devices, Afaria cannot always retrieve a serial number. Therefore, it may reuse IMEI and MEID values as the serial number and client name values.
  - Some devices return a manufacturer-specific serial number or some other number that may not match the number that is visible on the outside of the device.

- Phone – some devices on GSM or CDMA do not expose their phone number.
- Wi-Fi
  - Most non-Wi-Fi devices do not return a value for Wi-Fi Supported and Wi-Fi status.
  - Many Windows Mobile Standard devices do not expose their MAC address.
- Bluetooth – some device manufacturers protect their Bluetooth data with driver licensing.

Implications for Inspector Hardware Data and Device Views

Device inventory records are not created for class data groups that are not supported on a device. This has implications for understanding Inspector hardware data and creating device views:

- Device Inspector hardware data list – the list always includes all of a device type's possible inventory data classes. However, individual device results for specific data classes appear only when there are corresponding device inventory records for the associated data class.
- Custom device views – Device inventory records for a data class are not created, such as Phone or Wi-Fi, if the feature is unsupported on a device when you build custom views. Plan your queries to account for the possible absence of a record type, rather than the record type containing a null or blank value.

8.10 Device Activity Calls by Device Type

Definitions of voice call details collected by each device type, for example, Cell ID and MCC.

Voice Call Details	iOS	Android	Definitions
Remote Party		X	Remote party phone number.
Start Time	X	X	Start time of the call event.
End Time	X	X	End time of the call event. End Time does not appear in data views and reports.
Duration	X	X	Duration of call event.
Call Direction	X	X	Outbound or inbound call.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the start of the connection.
Roaming State	X	X	Roaming status.
Latitude	X	X	Latitude generated at the start of a call.
Longitude	X	X	Longitude generated at the start of a call.

Voice Call Details	iOS	Android	Definitions
MCC	X	X	Mobile Country Code of the network on which the call event occurred.
MNC	X	X	Mobile Network Code of the network on which the call event occurred.

8.11 Device Activity Data Connections Details by Device Type

Definitions of data connection details collected by device type, for example, Bearer Type and MNC.

Data Connection Details	iOS	Android	Definitions
Start Time	X	X	Start time of the call event
End Time	X	X	End time of the call event. End Time does not appear in data views and reports.
Duration	X	X	Duration of call event.
Bearer Type	X	X	Network type, such as CMDA, GSM and Wi-Fi, at the start of the connection.
Connection Name		X	Network name.
Access Point Name		X	Access Point Name.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the start of the connection.
Roaming State	X	X	Roaming status.
Latitude	X	X	Latitude generated at the start of the connection.
Longitude	X	X	Longitude generated at the start of the connection.
MCC	X	X	Mobile Country Code of the network on which the connection occurred.
MNC	X	X	Mobile Network Code of the network on which the connection occurred.
Sent	X	X	Number of bytes transmitted.
Received	X	X	Number of bytes received.

8.12 Device Activity Messages by Device Type

Definitions of message details collected by each device type, for example, cell ID and Type. Device Activity messages are not supported on iOS devices.

Message Details	iOS	Android	Definitions
Remote Party		X	Remote party phone number.
Start Time		X	Start time of the call event.
Message Direction		X	Outbound or inbound message.
Type		X	SMS or MMS.
Cell ID		X	Mobile cell ID at the start of connection. On CDMA networks, the Base Station ID (BID) at the time the message is sent.
Roaming State		X	Roaming status.
Latitude		X	Latitude generated when message is initiated/received.
Longitude		X	Longitude generated when message is initiated or received.
MCC		X	Mobile Country Code of the network on which the message occurred.
MNC		X	Mobile Network Code of the network on which the message occurred.

8.13 Configuring General Device Activity Settings

Enable and configure device activity data collection by configuring the Afaria Administration console.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.
2. On the General Settings tab, select *Enable Activity Collection*.
   If you do not want to start data collection at the next service restart, unselect *Enable Activity Collection*.
3. (Optional) To collect the phone numbers of remote devices, select *Collect Remote Party Phone Numbers*.
   This option is not applicable for Windows Phone devices.
4. (Optional) Select *Collect Subscriber Location Information*.
5. (Optional) Select *Prompt Subscriber for Activity Enrollment* and compose the enrollment notification for users to view on their devices.

When device activity collection is enabled the first time, actual data collection begins after you restart the SAP Afaria Server service and the device successfully connects to the server.

8.14 Configuring Device Activity Settings for Roaming

Configure Afaria Device Activity International Roaming settings to notify users that their devices are in an international roaming state and additional charges may apply.

Context

You do not need to configure device activity settings to restart the Afaria server service unless you want to initiate device activity data collection.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Component* > *Device Activity*.
2. On the General Settings tab, select *Enable Activity Collection*.
   If device activity is enabled, a notification appears on the device every time the device enters international roaming.
3. On the Roaming Settings tab:
   a. Select *Enable Roaming Notification*.
      This option is not applicable for Windows Phone devices.
   b. (Optional) Customize notification content.
   c. (Optional) To reduce the number of notifications when close to a roaming boundary, set the length of time a device must be in roaming status before a user receives a notification.
   d. Save changes.
   e. If you do not want to begin or resume device activity data collection at the next service restart, return to the General Settings tab and unselect *Enable Activity Collection*.

8.15 Configuring Device Activity Settings for Data Views

Customize how SAP Afaria Device Activity data appears in Data Views.

Procedure

1. In the Afaria Administration console, on the *Server* page, select *Configuration* > *Component* > *Device Activity*.
2. On the Data Views tab:
   a. In the Accounting Period area, set the start day in the month of the current and previous accounting periods.
   b. In the Threshold area, set the threshold fields for each type of activity in the local network while in a roaming state.
   c. In the Roaming Network area, set the percentage threshold value for each type of activity occurring in the local network while in a roaming state.
3. Save changes.

Example

Example: Enterprise mobile plan with prepaid activities for each subscriber each accounting period

Your enterprise mobile plan includes these prepaid activities, for each accounting period and for each subscriber:

- Local network:
  - 1000MB for data
  - 700 outgoing messages
  - Unlimited outgoing local calls
  - Unlimited incoming calls and messages
- Roaming:
  - 400MB for data
  - 500 messages (both outgoing and incoming)
  - 300 minutes for calls (both outgoing and incoming)

Set the threshold field for each activity accordingly. For example, enter 700 in the Number of Outgoing Messages field in the Local Network area; and “0” in the Total Outgoing Calls field in the Local Network. Incoming calls and messages in the local network are usually unlimited prepaid activities. As a result, you do not need to set thresholds for those activities. The Roaming Network views show the percentage of the prepaid activities for each subscriber during the current or previous accounting period.

For example, if a subscriber has sent 350 messages while in the local network, the Msg Out % column of the Message Threshold Summary view shows 50%.

To flag subscribers who are about to exceed the prepaid activities allowed by your enterprise mobile plan, set the percentage value for each activity to 95%.

The Exceed Threshold Summary view lists all subscribers who have exceeded 95% for any of the prepaid activities. A subscriber who has exceeded the percentage threshold for one kind activity but not for all

others, continues to appear in the Exceed Threshold Summary view. The Activity threshold views show the percentage of the prepaid activities that each subscriber has carried on during either the current or previous accounting period. For example, if a subscriber has sent 350 messages while in the local network, the Msg Out % column of the Message Threshold Summary view shows 50%.

8.16 Enabling Device Activity Cleanup

You can use the Afaria Administration console to configure how the SAP Afaria Server removes old device activity data.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Component* > *Device Activity*.
2. On the Cleanup Settings tab:
   a. Select *Enable Activity Cleanup*.
   b. (Optional) Set the number of days to keep device activity data before it is removed from your system.

   When device activity cleanup is enabled, the SAP Afaria Server automatically removes old device activity data at the time of the default schedule (12:00 a.m. every day) or at the time specified in your custom device activity cleanup schedule.

8.17 Customizing Device Activity Cleanup Schedule

Customize the date and time at which the SAP Afaria Server deletes old device activity data.

Context

The device activity cleanup schedule applies to all tenants with device activity cleanup enabled.

Procedure

1. In the Afaria Administration console, on the Server page, select *Configuration* > *Server* > *Schedule*.
2. Click *Edit connection rule* to open the Schedule Editor.

3. Specify your schedule settings.
4. (Optional) On the *Range* tab, specify a date range for the schedule.
5. (Optional) On the *Rate* and *Repeat* tabs, set the schedule to run on a recurring basis.
6. Click *Save*.
   When Activity Cleanup is enabled, SAP Afaria removes old device activity data at the time and frequency you have set in your schedule.

8.18 Creating Custom Device Activity Views

Select columns for a custom device activity view, and define criteria for selecting which subscribers populate your view.

Procedure

1. On the Device page, on the left toolbar, click *Activity List*.
2. On the left toolbar, click *Select View*.
3. (Optional) To define a new folder for the view, select a target folder, and then on the View toolbar, click *Add new view within currently opened folder* to open the Custom View dialog.
4. Enter a view name and note.
5. To select the columns to include in your view, populate the column list by selecting fields in the Data Fields list and clicking the *Add column* icon.

   You can further define the columns in the list by selecting a row and using the right-side icons to move a row's order and edit a row's alias, show/hide property, and sort properties. Row order in this list indicates the resulting custom view's column order from left to right.

   > **i Note**
   >
   > If you set a column's show option to "hide", you must also select a sort option ("sort ascending" or "sort descending") or SAP Afaria deletes the column on save.

6. To edit a row's criteria definition, select fields in the Data Fields list, click the *Add criteria* icon, select the row in the list, and click the right-side *Edit criteria*.

   You can further define criteria by selecting multiple criteria rows and using the right-side icons to group or ungroup the selection.
7. (Optional) When the view is defined, click the *Show as SQL statement* link to open the resulting SQL statement and review it or copy it to the Windows clipboard for subsequent pasting.
8. Click *Save*.

Results

The view is added to your custom views list. Select the view to show subscribers that meet the view's criteria.

8.19 Viewing the Device Activity List in the Default View

Display the device activity list in the default system-defined data view.

Procedure

1. On the Device page, on the left toolbar, click *Activity List*.
   The Subscribers view is the default view.
2. (Optional) Click the title of any column to sort by that column.

8.20 Viewing the Device Activity List in the Non-default View

Display the system-defined data views that allow you to review device activity data.

Procedure

1. On the *Device* > *Activity* page, on the left toolbar, click *Select View*.
2. Navigate the Activity views folders, then click on a view of interest.
3. On the View toolbar, click *Select* to open the view in the *Device* > *Activity* page.
4. (Optional) Click the title of any column to sort by that column.

8.21 Viewing the Device Location

You can view the last location that a device reports to SAP Afaria on a map.

Context

The location view also shows the date and time when the device location was last determined, based on the local time zone of the browser session of the Afaria Administration console.

Procedure

1. On the *Device* page, on the left toolbar, click *Activity List*.
2. On the left toolbar, click *Select View*, select *Location view*, and click *Select* to display the view.
3. Select a subscriber.
4. On the top toolbar, click *Map*.

Latitude and Longitude Definitions [page 346]
Definitions for longitude and latitude data collection values.

8.21.1 Latitude and Longitude Definitions

Definitions for longitude and latitude data collection values.

Latitude and Longitude columns appear in the Location view in the device activity data view.

Value	Definition
<longitude > <latitude>	Last retrieved approximate longitude and latitude of the device, based on crowd-sourced Wi-Fi hotspot and mobile cell tower location. Level of accuracy varies by device type. For iOS and Android, accuracy requested is 1km (0.62 miles).
Unknown	The location of the device is temporarily unknown.
Disabled	Location services are disabled on the device.
Not Collected	Collection of subscriber location information is disabled on the Device Activity General Settings tab of the Afaria Administration console.
Unsupported	The device does not support location services.

8.22 Client Logging

Retrieve and export client logs for iOS and Android devices at the request of SAP Afaria support teams to help validate and resolve issues.

After you send the request for log files from the Afaria Administration console, the SAP Afaria client sends the log file as compressed binary data to SAP Afaria. The SAP Afaria Enrollment server processes the log data and saves it in the SAP Afaria database. The database keeps a maximum of 10 log data sets and keeps each log data set for a maximum period of 30 days.

When you select a log file (identified by a time stamp) in the Device Inspector, the Afaria Administration console retrieves the compressed binary data from the database and packages it into an HTTP response with a file name that includes the device identifier and a time stamp. The log file is then available as a file download in the browser.

The SAP Afaria server sends requests to Android devices using Firebase Cloud Messaging (FCM), formerly Google Cloud Messaging (GCM). To use client logging on Android devices:

- Configure FCM/GCM on the SAP Afaria server.
- Enable FCM/GCM in the enrollment policy.
- Enable logging in the SAP Afaria client on devices.

The SAP Afaria server sends requests to iOS devices using the Apple Push Notification service (APNs). To use client logging on iOS devices:

- Configure iOS Notifications on the SAP Afaria server.
- The iOS device must be under MDM management with a certificate for MDM.
- The SAP Afaria client must be a custom-signed application with a certificate for the custom-signed application.
- Enable logging in the SAP Afaria client on devices.
- The SAP Afaria client must be able to receive notifications and be in the foreground.

Retrieving Client Logs [page 347]
You can use the Afaria Administration console to retrieve client logs remotely from the SAP Afaria client on iOS and Android devices.

8.22.1 Retrieving Client Logs

You can use the Afaria Administration console to retrieve client logs remotely from the SAP Afaria client on iOS and Android devices.

Procedure

1. On the device, configure client logging in the SAP Afaria client. You can enable logging, set the log file size (1 MB by default), and define the logging level (error, informational, warning, and debug; informational by default).
2. On the device, recreate the issue.
3. On the *Device* page in the Afaria Administration console, select the device.
4. To send the request for log files to the device, click *Get Log File*.
5. On the device, open the SAP Afaria client application to connect to SAP Afaria and deliver the log to the server.
6. On the *Device* page in the Afaria Administration console, select the device and click *Show/Hide Inspector* to open the Device Inspector.
7. In the Device Inspector, click *Client Log*.
8. In the *Client Logs* table, select the client log and click *Download selected client log* to save the file.
9. On the device, disable client logging.

9 Device Inspector

The Device Inspector displays information about the devices under SAP Afaria management.

The information that the Device Inspector displays varies by device OS.

9.1 Information in the Device Inspector

The information that the Device Inspector displays varies by device OS.

Information	Description
Summary	The Summary page displays general information about devices.
Hardware	The Hardware page displays information about device hardware.
Software Inventory	The Software Inventory page displays the applications on devices.
Connection Log	The Connection Log page displays the log files that describe connections between devices and SAP Afaria. You can select and view the details of each log file.

Information	Description
File Transfer Log	The File Transfer Log page displays log files that describe the transfer of files between devices and SAP Afaria. You can select and view the details of each log file.
Package Tracking Log	The Package Tracking Log page displays log files that describe the transfer of application packages from SAP Afaria to devices.
Policy Log	The Policy Log page displays log files that describe the transfer of polices from SAP Afaria to devices.
Client Logs	The Client Logs page displays log files that SAP Afaria collects from the SAP Afaria client on devices. This page is available for Android and iOS devices.

9.2 Hardware Inventory for Android Devices

View the hardware inventory information for Android devices from the Device Inspector page.

The Android client uses a series of Android APIs to gather hardware inventory information, packages them into an XML file, sends them to the SAP Afaria server where the files are parsed, and saves the information in the SAP Afaria database. Users can view the following hardware inventory information:

- Android – hardware information, such as device model, platform version, phone type, roaming status (allow data roaming, auto sync when roaming, allow push while roaming) and more.
- App black list
- App white list
- Bluetooth – information about Bluetooth support on the Android device, including device name and address, bonded devices, and more.
- Certificate – information about certificates that are installed, such as CA Cert Name, User Cert Name, Issued To, Issued By, Validity, Type and Hash Code.
- Device – device information, such as device OS, IMEI, OS version, serial number, and more.
- Firewall – information about firewall, such as proxy address, port, IP tables proxy rules, and IP tables proxy option (true if "proxy rule" is enabled, else false).
- Managed software – information about managed software is populated only for Samsung AES capable devices (with the proper SAP Afaria AES application installed on the device), such as:
    - Package name
    - Install count – number of times the application has been installed. This value persists irrespective of application installation and uninstallation.
    - Uninstall count – number of times the application has been uninstalled, will persist irrespective of application installation and uninstallation.
    - Disabled – current status of application.
    - Installation disabled – installation status of application.
    - App installed – true if application package is successfully installed on the device, else false.

- Memory – available memory, total memory, and name of the memory of both the device and SD card.
- Phone – current network, current mobile operator, and phone number.
- Restrictions – as defined by SAP Afaria configuration policy restriction payloads. Restrictions defined by the device holder are not reported.
- Security – password attributes, MDM version, CA certificate details, and more.

9.3 Hardware Inventory for iOS Devices

The majority of hardware inventory is collected and defined by the Apple MDM protocol. Some data is collected by the SAP Afaria client on the device.

Afaria Hardware Inventory [page 350]

Bluetooth Hardware Inventory [page 351]

Certificates Hardware Inventory [page 351]

Device Hardware Inventory [page 352]

General Hardware Inventory [page 352]

Managed Certs Hardware Inventory [page 353]

Memory Hardware Inventory [page 354]

MS Exchange Hardware Inventory [page 354]

Organization Info Hardware Inventory [page 354]

Payloads Hardware Inventory [page 355]

Phone Hardware Inventory [page 355]

Provisioning Profiles Hardware Inventory [page 356]

Restrictions Hardware Inventory [page 356]

The Restrictions hardware inventory displays settings from the Restriction payload in configuration policies that apply to the device.

Security Hardware Inventory [page 356]

Wi-Fi Hardware Inventory [page 357]

9.3.1 Afaria Hardware Inventory

Inventory Item	Description
Afaria detected jailbreak	This inventory item indicates whether a device is in a security-compromised state.

Inventory Item	Description
Afaria installed	This inventory item indicates whether the SAP Afaria client is installed on the device.
Last policy connect	This inventory item indicates when the device last connected to the SAP Afaria server to allow the application of a policy.
Last notification sent	This inventory item indicates when the SAP Afaria send a notification to the device to initiate a connection.
Sync policy	This inventory item indicates the name of the synchronization policy.
Afaria version	This inventory item indicates the version of the SAP Afaria client on the device.
Under MDM Control	This inventory item indicates whether the device is under MDM control.
Is supervised	This inventory item whether the device is supervised.

9.3.2 Bluetooth Hardware Inventory

Inventory Item	Description
Bluetooth MAC	This inventory item indicates the media access control (MAC) address of the Bluetooth hardware of the device.

9.3.3 Certificates Hardware Inventory

Inventory Item	Description
Common name	This inventory item indicates the common name of the certificate.
Is identity	This inventory item indicates whether the certificate is an identity certificate.

9.3.4 Device Hardware Inventory

Inventory Item	Description
Compromised	This inventory item indicates whether the device is compromised.
Device name	This inventory item indicates the name of the device.
iOS version	This inventory item indicates the version of iOS on the device.
ROM	This inventory item indicates the ROM version.
iOS user name	This inventory item indicates the name of the device user.
OS	This inventory item indicates the operating system of the device.
UDID	This inventory item indicates the UDID of the device.
Is do not disturb on	This inventory item indicates whether the Do Not Disturb feature is active on the device.
Is device locator on	This inventory item indicates whether the device is reporting its location to the iCloud.
Is iCloud backup enabled	This inventory item indicates whether the device backs up data (device settings, photos, application data, etc.) to the iCloud.
Last iCloud backup date	This inventory item indicates the last date that the device backed up data to the iCloud.
Product Name	This inventory item indicates the product name of the device. This value is from Apple and might not reflect device branding.

9.3.5 General Hardware Inventory

Inventory Item	Description
Serial number	This inventory item indicates the serial number of the device.
IMSI	This inventory item indicates the International Mobile Subscriber Identity (IMSI) of the device.
IMEI	This inventory item indicates the International Mobile Station Equipment Identity (IMEI) of the device.
Device Model Number	This inventory item indicates the model number of the device.

Inventory Item	Description
Device Model	This inventory item indicates the product name of the device. This value is from Apple and might not reflect device branding.
MEID	This inventory item indicates the Mobile Equipment Identifier (MEID).
Last Connection	This inventory item indicates the last time that the device connected to SAP Afaria.
Phone number	This inventory item indicates the phone number of the device.

9.3.6 Managed Certs Hardware Inventory

Inventory Item	Description
Serial Number	This inventory item indicates the serial number of the certificate.
Thumbprint	This inventory item indicates the hash, or thumbprint, of the certificate.
Subject	This inventory item indicates the entity identified by the certificate.
Issuer	This inventory item indicates the entity that verified and issued the certificate.
Effective Date	This inventory item indicates the date on which the certificate is first valid.
Expiration Date	This inventory item indicates the date on which the certificate ceases to be valid.
CA Name	This inventory item indicates the name of the certificate authority.
CA Type	This inventory item indicates the type of the certificate authority.
Purpose	This inventory item indicates the purpose for which the device uses the certificate.
Subject Alternative Name	This inventory item indicates alternate entities identified by the certificate.
Revocation State	This inventory item indicates the revocation state, if any, of the certificate.

9.3.7 Memory Hardware Inventory

Inventory Item	Description
Available device capacity	This inventory item indicates the amount of available memory on the device.
Device capacity	This inventory item indicates the total amount of memory, both allocated and available, on the device.

9.3.8 MS Exchange Hardware Inventory

Inventory Item	Description
Device ID	This inventory item indicates the device identity on the Microsoft Exchange server.
User ID	This inventory item indicates the user identity on the Microsoft Exchange server.

9.3.9 Organization Info Hardware Inventory

Inventory Item	Description
Name	This inventory item indicates the name of the organization.
Address	This inventory item indicates the address of the organization.
Phone	This inventory item indicates the phone number of the organization.
Email	This inventory item indicates the email address of the organization.
Other	This inventory item indicates additional information about the organization.

9.3.10 Payloads Hardware Inventory

Inventory Item	Description
Description	This inventory item indicates the name of the payload in the Device Inspector. The name distinguishes the different payloads on the device.
Display name	This inventory item indicates the display name of the certificate.
Has removal passcode	This inventory item indicates whether a passcode is required to remove the certificate from the device.
ID	This inventory item indicates the ID of the certificate.
Identifier	This inventory item indicates the identifier of the certificate.
Is encrypted	This inventory item indicates whether the certificate is encrypted.
Organization	This inventory item indicates the organization.
Removal disallowed	This inventory item indicates whether users can remove the certificate from the device.
Type	This inventory item indicates the type of the certificate.
Version	This inventory item indicates the version of the certificate.
Is managed	This inventory item indicates whether the certificate is managed by SAP Afaria.

9.3.11 Phone Hardware Inventory

Inventory Item	Description
Carrier settings version	This inventory item indicates the version of carrier settings on the device. Carrier settings include settings for network, calling, cellular data, etc. Apple or the carrier might update the carrier settings and users might receive notifications to install new settings.
Data roaming enabled	This inventory item indicates whether the device can use the cellular network for data communication when the device is away from its home network.
Modem firmware version	This inventory item indicates the firmware installed on the device for the data modem.

Inventory Item	Description
SIM serial number	This inventory item indicates the unique serial number of the SIM card in the device.
SIM carrier network	This inventory item indicates the wireless provider for the device.
Voice Roaming Enabled	This inventory item indicates whether the device can use the cellular network for phone communications when the device is away from its home network.
Cellular Technology	This inventory item indicates the cellular technology that the device uses.

9.3.12 Provisioning Profiles Hardware Inventory

Inventory Item	Description
Expiration date	This inventory item indicates the date on which the provisioning profile expires.
ID	This inventory item indicates the identifier of the provisioning profile on the device.
Name	This inventory item indicates the name of the provisioning profile.

9.3.13 Restrictions Hardware Inventory

The Restrictions hardware inventory displays settings from the Restriction payload in configuration policies that apply to the device.

9.3.14 Security Hardware Inventory

Inventory Item	Description
Hardware encryption capability	This inventory item indicates the hardware encryption that is available on the device.
Passcode compliant	This inventory item indicates if the passcode on the device is compliant.
Profile passcode compliant	This inventory item indicates if the profile passcode is compliant.

Inventory Item	Description
Passcode present	This inventory item indicates whether the passcode is present on the device.

9.3.15 Wi-Fi Hardware Inventory

Inventory Item	Description
WIFI MAC	This inventory item indicates the media access control (MAC) address of the Wi-Fi hardware of the device.
Personal hotspot on	This inventory item indicates whether the device is acting as a Wi-Fi hotspot.

9.4 Hardware Inventory for Windows Phone Devices

View the hardware inventory information for Windows Phone devices from the Device Inspector page.

- Afaria – indicates whether the device is under MDM control.

  > **i Note**
  >
  > This status is updated even when the user initiates the unenrollment by deleting the MDM account on the device.

- Certificate – provides information such as Common Name and Is identity for all certifcates on the device.
- Client Configuration – device identification and certificate renewal information, including device name, enterprise ID, certificate renewal, signed certificate renewal.
- Device – hardware information, such as device model, platform version, phone type.
- MS Exchange – values related to Access Control for Email including domain, account type, server name, and SSL connection.
- Managed Certificates – information on certificates which are deployed/managed by Afaria such as: Serial number, Thumbprint, Subject, Issuer, Effective Date, Expiration Date, CA Name, CA Type, Purpose, Subject Alternative Name, Revocation State.
- Provisioning Profiles – information related to provisioning the device, including address, use hardware device ID, port number.
- Security – password configuration details, such as: whether the device password enabled, length, expiration date, history.

9.5 Hardware Inventory for Windows DM Devices

View the hardware inventory information for Windows DM devices from the Device Inspector page.

The hardware inventory details are:

- Device – device details such as device model, manufacturer, identifying number, system name, type etc.
- Certificate – provides information such as Common Name and Is identity for all certifcates on the device.
- Disk Space – device ID, name, total disk space, and the available free space.
- Network Adapter – adapter details such as ID, type, GUID, MAC address, manufacturer details etc.
- Operating System – name, manufacturer name, architecture, and version of the operating system.
- Printer – printer name, ID, driver details, network and sharing details, print capabilities etc.
- Managed Certificates – information on certificates which are deployed/managed by Afaria such as: Serial number, Thumbprint, Subject, Issuer, Effective Date, Expiration Date, CA Name, CA Type, Purpose, Subject Alternative Name, Revocation State.
- Security Settings – antivirus and antivirus signature status, auto update status, firewall status etc.

9.6 Viewing the Device Inspector

You can use the Device Inspector to view information about the devices under SAP Afaria management.

Procedure

1. On the *Devices* page, click *Show/Hide Inspector* .
2. Select a device to view information about the device.
3. Click the icons across the top of the Device Inspector to view additional information.

9.7 Viewing the Device Package Tracking Log

Identify all apps made available to devices and view package status.

Context

View the application package status details for a device. The information on this page filters to show Android, iOS, or Windows Phone details depending on the device selected. If you select an Android or a Windows Phone device, the *Status by MDM* column does not display.

You can access the *Package Tracking Log* from either the *Policy* > *List* page or the *Device* > *List* page. Different columns are displayed depending on the context. Package tracking logs are collected only if the software inventory option is enabled in the associated configuration policy.

Procedure

1. Select the applicable device from the *Device List* page.
2. On the left toolbar, click the *Show/Hide Inspector* icon to display device inspector options.
   A right pane displays allowing you to a select toolbar option and view details about a device.
3. Click the *Package Tracking* icon in the *Inspect* toolbar.
   The *Package Tracking Log* page shows the list of device package status details. You can also filter the log using the following criteria:
   - Package – the identifier, as defined by the developing entity.
   - Status by Afaria – status when you push an application policy via package server. For example, Failed, Installed, Installed by User.
   - Status by MDM – status when you push an application policy via MDM. For example, Managed, User Rejected. This is relevant only for iOS.
     There are two statuses specific to taking over apps on managed devices:

     Prompting For Management The user is being prompted to change an unmanaged installed app to managed.

     Management Rejected The user has declined management of an unmanaged installed app.
   - Last Update – date the device was updated last.
   - Type – application policy type: Android Enterprise, Android Market, iOS Enterprise, iOS App Store, or Windows Phone Enterprise.

9.8 Downloading the Client Log

You can use the Device Inspector to view client logs with timestamp, and to download the client log to your computer.

Procedure

1. Select an Android device or iOS device from the Devices page.
2. On the Devices page, click *Show/Hide Inspector*.
3. Click *Client Log*.
   The date and timestamp when the log file is last fetched from the device is displayed.
4. Select the timestamp and click *Download selected client log*.
   The client log is downloaded to your computer.

10 Application Onboarding

For commercial or enterprise applications for iOS and Android devices, Afaria can provision data and certificates to facilitate onboarding.

- Data provisioning – delivers application configuration data as needed, such as for connectivity or operations.
- Certificate provisioning – delivers a certificate to a device as needed, such as for user authentication.

10.1 Data Provisioning for iOS and for Android

For iOS and for Android commercial or enterprise applications, Afaria can deliver application configuration data to devices as needed, such as for connectivity or operations.

10.1.1 Compiling Applications for iOS and Android Data Provisioning

Compile applications with the Afaria Static Link Library (SLL) with calls that retrieve data defined in an portal application package.

Procedure

1. Refer to the Static Link Library documentation, as available on the product image in folder `\Documents\English\Developers`.

   Documentation is available for iOS and Android development.
2. Follow documented procedures for using the library to make a `retrieveSeedData` call.
3. As required for your application, develop response for retrieving, using, and deleting the data.

10.1.2 Output Requirements for iOS and Android Data Provisioning

Provisioning requires an application call and configuration data.

- For the device, an application compiled with the SAP Afaria SLL `retrieveSeedData` call.
- For the administrator, configuration data, as either:
  - A file of any type with any extension.
  - Data that an administrator enters in to the Afaria Administration console.

10.1.3 Provisioning Data for iOS and Android Applications

Create an iOS or Android enterprise or commercial application package that includes configuration data for application onboarding.

Procedure

1. On the Home page banner, click *Policy*, or click one of the links on the Policy tile.
2. Review the policy list.

   The default view is unfiltered; it includes all policies and may span multiple pages.
3. On the top toolbar, click *New* > *Application* and click an application type.
4. On the Summary page, enter a policy name and note and click to indicate published or unpublished.

   Connecting devices receive only published policies.

5. On the Configuration page, type or import your application seeding configuration data.

   Import source location is relative to the browsing computer. Importing a file overwrites the content in the data box. If you edit the file in the Afaria Administration console it is stored in UTF-8 format. If you do not edit the file, it is stored in its original format.

   If you import an empty text file here, the file will not be saved with the policy.
6. Click *Edit* to open the *Application Policy* > *Configuration* dialog and click the *Substitution link*. The substitution variables dialog opens. The list combines predefined and user-defined substitution variables.
7. Select a substitution variable and click *Select* to add it to the application.

   If the substitution variable is not on the list, click *Add* to define it, as is appropriate for your requirements.

   To delete a substitution variable from the list, select it and click *Delete*. This action deletes the user-defined variable and any associated value from all iOS and Android definitions.
8. Click *Save*.

10.2 About Certificate Provisioning for Android

For commercial or enterprise applications, Afariacan deliver certificates to devices as needed, such as for user authentication, from your certificate authority (CA).

This feature requires a configured provisioning server and CA, as defined on *Server Configuration* > *Properties* > *Component Configuration* > *Portal Package Server* page, including any certificate request information.

Compiling Applications for Android Certificate Provisioning [page 362]
Compile applications with the AfariaStatic Link Library (SLL) with calls that retrieve a certificate from your enterprise certificate authority (CA) server.

Output Requirements for Android Certificate Provisioning [page 363]
For the device, an application compiled with the Afaria Static Link Library retrieveCertificate call.

10.2.1 Compiling Applications for Android Certificate Provisioning

Compile applications with the AfariaStatic Link Library (SLL) with calls that retrieve a certificate from your enterprise certificate authority (CA) server.

Procedure

1. Refer to the Afaria Static Link Library documentation.

   For Android, the library documentation is available on the product image in folder `\Documents\English\Developers`.

2. Follow documented procedures for using the library to make the `retrieveCertificate` call.

   Defining values for call parameters is the responsibility of the developing party:
   - Cert public key
   - Cert private key
   - Cert common name
   - CA challenge response
   - If using authentication the portal package server, user credentials as <domain>\<username> and password or <username> and password.
3. As required for your application, develop a response for using the certificate.

10.2.2 Output Requirements for Android Certificate Provisioning

For the device, an application compiled with the Afaria Static Link Library retrieveCertificate call.

10.3 Certificate Provisioning for iOS

For iOS commercial or enterprise applications, Afaria can deliver application configuration certificates as needed for authentication, connectivity, or operations.

This feature requires a configured provisioning server and CA, as defined on *Server Configuration* > *Properties* > *Component Configuration* > *Portal Package Server* page, including any certificate request information.

Compiling Applications for iOS Certificate Provisioning [page 364]
Compile applications with the Afaria Static Link Library (SLL) with calls that retrieve a certificate from your enterprise certificate authority (CA) server.

Output Requirements for iOS Certificate Provisioning [page 364]
For the device, an application compiled with the AfariaStatic Link Library retrieveCertificateWithPrivateKey and retrieveCertificateWithUrl calls.

10.3.1 Compiling Applications for iOS Certificate Provisioning

Compile applications with the Afaria Static Link Library (SLL) with calls that retrieve a certificate from your enterprise certificate authority (CA) server.

Procedure

1. Refer to the Afaria Static Link Library documentation, as available on the product image in folder `\Documents\English\Developers`.
2. Follow documented procedures for using the library to make the `retrieveCertificateWithPrivateKey` and `retrieveCertificateWithUrl` calls.

   Defining values for call parameters is the responsibility of the developing party:
   - Cert public key
   - Cert private key
   - Cert common name
   - CA challenge response
   - If using authentication the portal package server, user credentials as <domain>\<username> and password or <username> and password.
3. As required for your application, develop a response for using the certificate.

10.3.2 Output Requirements for iOS Certificate Provisioning

For the device, an application compiled with the AfariaStatic Link Library retrieveCertificateWithPrivateKey and retrieveCertificateWithUrl calls.

11 Integration with SAP Mobile Documents Application

Meet the highest security standards including document level security and compliance management with SAP Mobile Documents application that is installed using SAP Afaria.

SAP Mobile Documents application is designed for enterprise deployments where collaboration, security, and control of business content is critical.

Use SAP Afaria to:

- Install SAP Mobile Documents application on an iOS device (iPad and iPhone devices having iOS version 6 or higher) by creating an application policy for iOS App Store application and pushing it on the device.
- Remove the SAP Mobile Documents application from an iOS device (iPad and iPhone devices having iOS version 6 or higher) by deleting the application policy or unlinking the application policy from the group.
- Remove the SAP Mobile Documents application from an iOS device (iPad and iPhone devices having iOS version 6 or higher) when it is not compliant, by defining a remediation policy.
- Automatically reinstall the SAP Mobile Documents application on an iOS device (iPad and iPhone devices having iOS version 6 or higher) when the device comes back to compliance.

Installing SAP Mobile Documents iOS Client Application [page 366]
Install SAP Mobile Documents iOS client application on the iOS device from the Apple App Store.

Removing SAP Mobile Documents iOS Client Application [page 366]
Remove SAP Mobile Documents iOS client application by deleting the application policy.

Removing SAP Mobile Documents Application through a Remediation Policy [page 367]
Remove SAP Mobile Documents client application from an iOS device (iPad and iPhone devices having iOS version 6 or higher) when the device is out of compliance by creating a remediation policy.

Related Information

Creating an Application Policy for iOS Enterprise Applications [page 122]
Defining Remediation Policies for iOS devices [page 264]

11.1 Installing SAP Mobile Documents iOS Client Application

Install SAP Mobile Documents iOS client application on the iOS device from the Apple App Store.

Prerequisites

Complete the procedure to prepare for an App Store application, which includes recording the App Store number and country code for SAP Mobile Documents application.

Procedure

1. On the Policy list page in the top toolbar, click *New* > *Application* > *iOS App Store* to create an application policy. For more information, see Creating an Application Policy for iOS App Store Apps.
2. (Optional) To include managed app configuration to the managed SAP Mobile Documents iOS app, navigate to the Configuration page and add name value pair settings in the managed app configuration grid. For example, add server URL by setting the Name to "server.URL" and Value to the server URL for SAP Mobile Documents application backend. The SAP Mobile Documents iOS app (version 1.2.x) for iOS devices supports only managed app configuration.

   This configuration data gets seeded when using the iOS Afaria application from the App Store, and not if using the iOS Afaria custom application.

11.2 Removing SAP Mobile Documents iOS Client Application

Remove SAP Mobile Documents iOS client application by deleting the application policy.

Procedure

1. On the Policy list page, select the application policy created for SAP Mobile Docs.
2. Click Delete to delete the application policy.

   SAP Mobile Documents application is removed from the device once the application policy is deleted.

11.3 Removing SAP Mobile Documents Application through a Remediation Policy

Remove SAP Mobile Documents client application from an iOS device (iPad and iPhone devices having iOS version 6 or higher) when the device is out of compliance by creating a remediation policy.

Prerequisites

SAP Mobile Documents application is installed on the iOS device via Afaria and it is under MDM control.

Procedure

1. On the Home page Server tile, click *Configuration*.
2. Navigate to the *Component* > *Access Control Option* page, then select the *Remediation Policy* tab.
3. Select the *iOS* tab and indicate the remediation policy and remediation action parameters.
   - Remediation Policy – select any or all of the remediation policy options:
     - Mobile device management payload removed – server takes action if the mobile device management payload on the device is removed.
     - Afaria not installed or not connected within xx days and xx hours – server takes action if the Afaria application on the device is deleted or not connected within the number of days and hours specified.
     - Assigned policy not delivered – server takes action if the policies assigned by the Afaria server are not delivered and installed on the device within the time frame specified in the server configuration.
     - Device hardware not encrypted – server takes action if the device does not have hardware encryption capability.
     - Device compromised – server takes action if the device status changes to jailbroken.
     - Device in blocked group – server takes action if the device is present in the blocked groups list.
     - Device not in selected group – server takes action if the device is not present in the allowed groups list.
   - Remediation Action – select any or all of the remediation actions:
     - Remove SAP Mobile Docs – removes the SAP Mobile Documents application from the device.
     - Remove control – removes the device from the MDM control of the server.
     - Send message to client – informs via APNs or e-mail why the device has gone out of compliance, and the remediation actions.
       The maximum size of an APNs notification is 256 bytes. If the message exceeds this size limit, it may get truncated on the device.

       > **i Note**
       >
       > For remediations based on blocked groups, the remediation reason appears on the device only if you provided information in the Note field when you created the group.

4. Click *Save* to save the remediation policy.

   If you have selected the Remove SAP Mobile Docs remediation action and an iOS device is compromised, Afaria application detects that the device has been jailbroken and notifies the Afaria server. Afaria server verifies the device has been jailbroken and proceeds with the corresponding remediation actions by removing SAP Mobile Documents application from the device.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP