Knox Service Plugin for Matrix42 MDM

These instructions provide an overview of how to install KSP with the following MDM. Always check your MDM's specific documentation for the most up to date instructions.

Step 1: Matrix42 MDM - Add to UEM console

https://www.matrix42.com is a secure, mobile device management portal that works with KSP.

This section provides instructions on how to set up the KSP plugin in Matrix MDM.

Before you begin

Before you begin, however, ensure that you have:

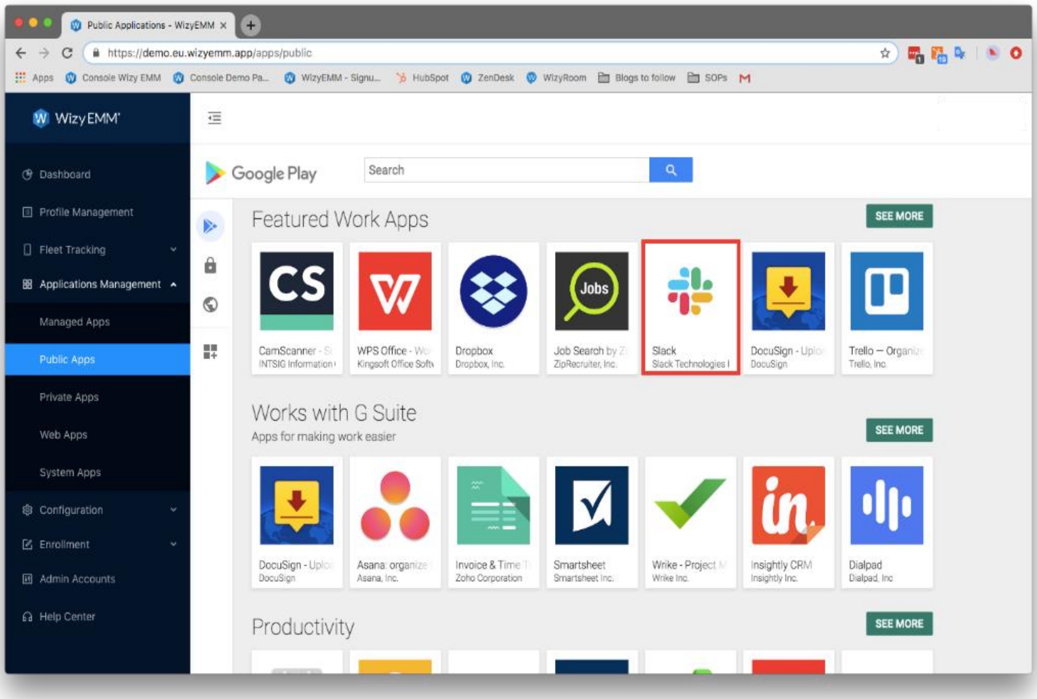
1. Access to the UEM console.
2. Linked your Matrix MDM console with a Managed Google Account. This allows you to deploy Android Enterprise devices.
3. Enrolled eligible devices and applied any necessary enterprise policies.

For more information on logging in to and setting up your Matrix MDM console, see Matrix42 MDM Guide

How to add Knox Service Plugin to Matrix42 MDM

The Knox Service Plugin (KSP) is Samsung's OEMConfig based solution that enables you as an IT administrator to use a wide range of Knox management features with Matrix as soon as they are commercially available in the market.
Samsung devices running Android 8.0 or above with Knox 3.0 or later, if enrolled as Device Owner or devices running Android 9.0 or later with Knox 3.2.1 or above when enrolled as Profile Owner.

Full instructions on the configuration of MGP can be found here.



For more information on adding apps to the Managed App Catalog, see Adding apps to Manage Apps Catalog

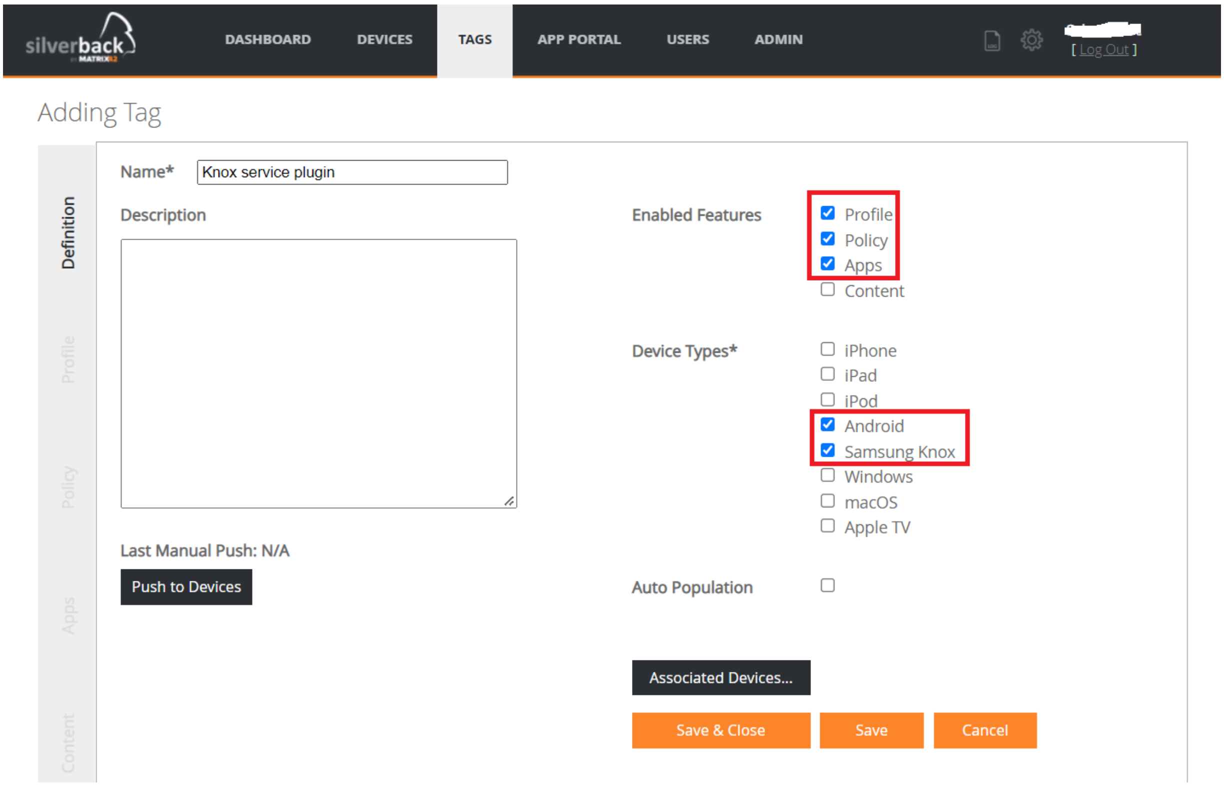
Next steps - Configure KSP

Step 2: Matrix42 MDM – Configure

This section provides instructions on how to configure KSP policies in Matrix MDM.

To configure your Samsung devices, please follow these guidelines:

Navigate to Tags



Adding Tag

Name* Knox service plugin

Description

Enabled Features
☑ Profile
☑ Policy
☑ Apps
□ Content

Device Types*
□ iPhone
□ iPad
□ iPod
☑ Android
☑ Samsung Knox
□ Windows
□ macOS
□ Apple TV

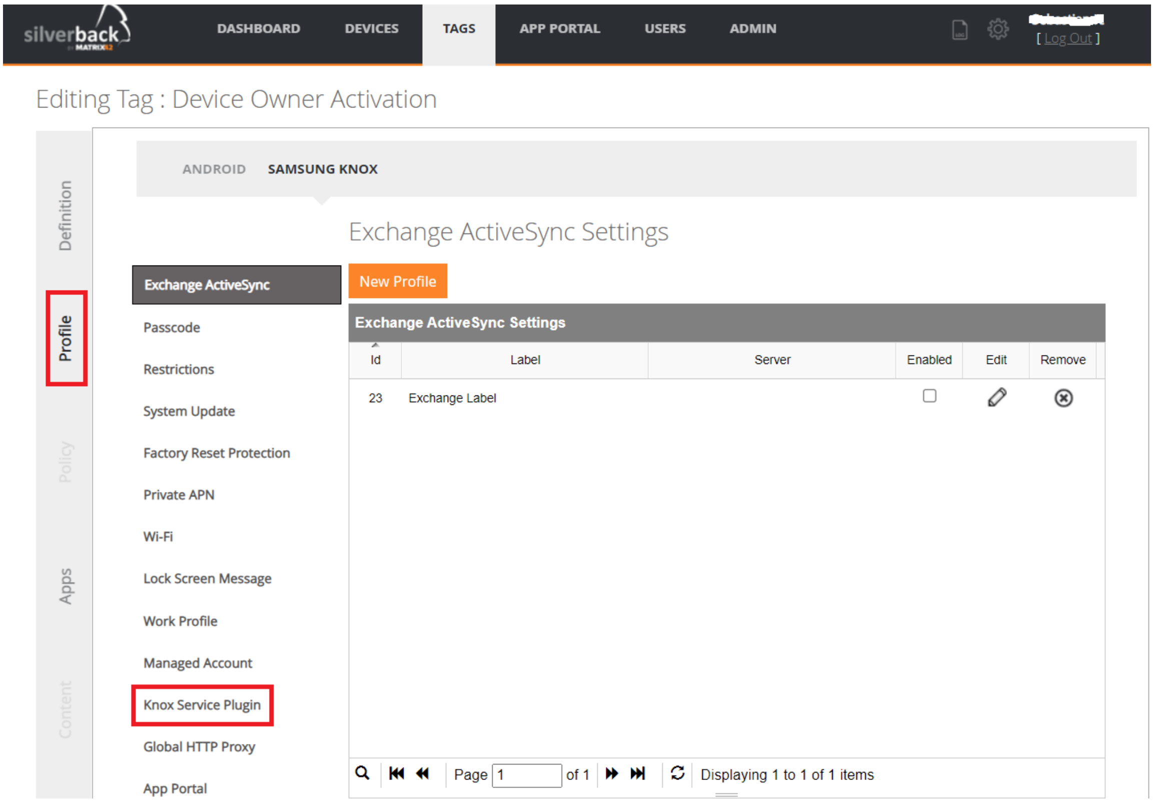
Last Manual Push: N/A

Auto Population □

Click New Tag or use an existing one

- Under Definition
  - Enter a Name, e.g. Knox Service Plugin
  - Enable Apps in Features
  - Enable Samsung Knox as device type
  - Press Save

- Choose Profile and KSP tab



Editing Tag : Device Owner Activation

Exchange ActiveSync Settings

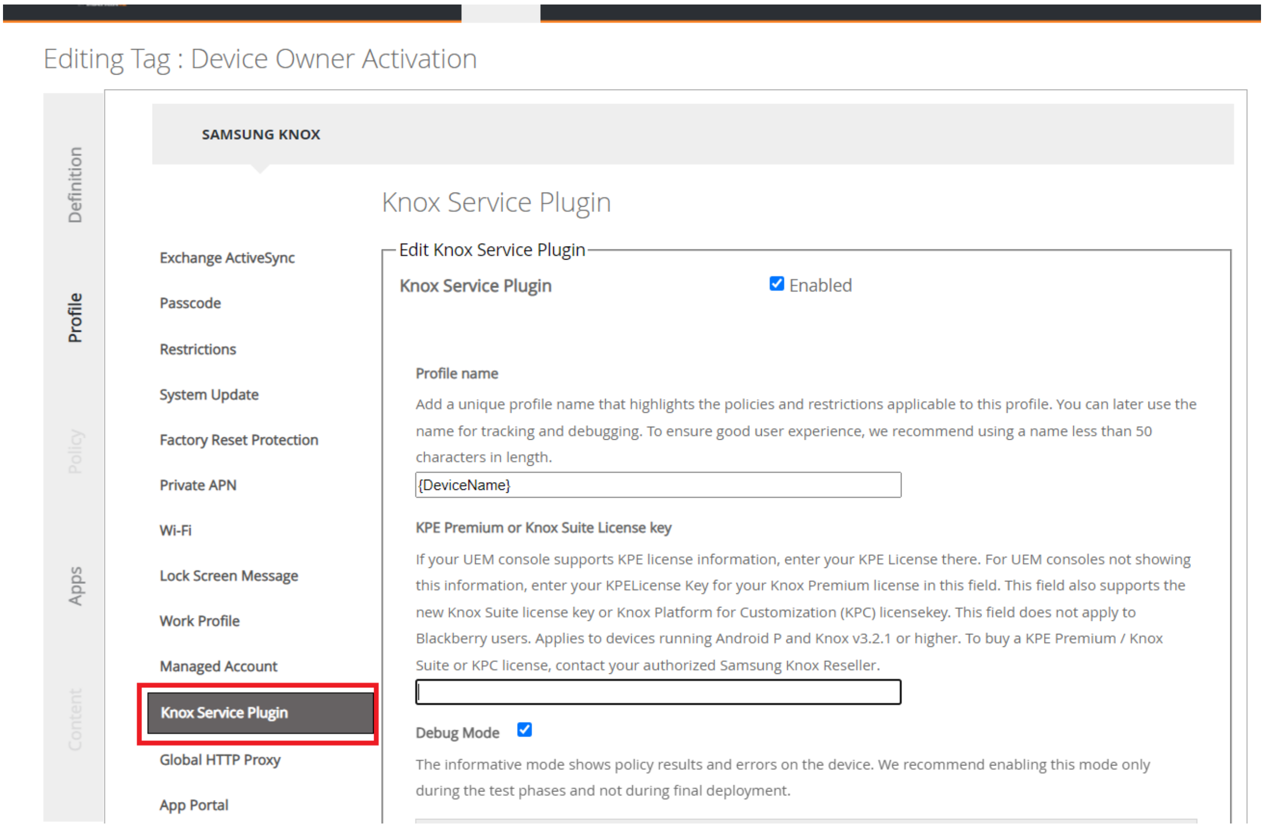
Exchange ActiveSync Settings

Id	Label	Server	Enabled	Edit	Remove
23	Exchange Label		☐	✎	⊗

Page 1 of 1

Displaying 1 to 1 of 1 items

Edit your Managed Configuration


Editing Tag : Device Owner Activation

Knox Service Plugin

Edit Knox Service Plugin

Knox Service Plugin ☑ Enabled

Profile name

Add a unique profile name that highlights the policies and restrictions applicable to this profile. You can later use the name for tracking and debugging. To ensure good user experience, we recommend using a name less than 50 characters in length.

{DeviceName}

KPE Premium or Knox Suite License key

If your UEM console supports KPE license information, enter your KPE License there. For UEM consoles not showing this information, enter your KPELicense Key for your Knox Premium license in this field. This field also supports the new Knox Suite license key or Knox Platform for Customization (KPC) licensekey. This field does not apply to Blackberry users. Applies to devices running Android P and Knox v3.2.1 or higher. To buy a KPE Premium / Knox Suite or KPC license, contact your authorized Samsung Knox Reseller.

Debug Mode ☑

The informative mode shows policy results and errors on the device. We recommend enabling this mode only during the test phases and not during final deployment.

- Enter a Profile name
- Enter your KPE Premium License Key (optional for Premium marked features)
- Enable Debug Mode (for testing purpose)
- Configure additional policies and profiles
- Press Save

For full information about the various KPE features and policies currently available with KSP, see KSP features and KPE functionality.

Next steps - deploy KSP to devices

Now that you've set up and configured KSP in your Matrix MDM console, you need to deploy the app to your managed devices.

Step 3. Matrix42 MDM: Deploy

This section provides instructions on how to deploy KSP policies in Matrix MDM.

Deploy KSP

Adding additional Admin Tags allows Administrators to specify Groups or levels of security to their Silverback Installation. Once a Device is enrolled it should already have its ‘Base Level of Security’ so Administrators can now create additional Tags and apply these to selected devices which will then receive the updated settings.

New Tag

- To create a new Tag navigate to Tags
- Click New Tag
- Enter a friendly name (required)
- Enter a description (required)
- Select the Enabled Features Area
  - Profile
  - Policy
  - Apps
  - Content
- Select the Device Types (required)

  - iPhone
  - iPad
  - iPod
  - Android
  - Samsung Knox
  - Windows 10
  - Windows 10 Mobile
  - macOS
  - AppleTV
- Enable Auto Population (optional)
- Click Save

After clicking Save all Enabled Features will be activated in the left panel.

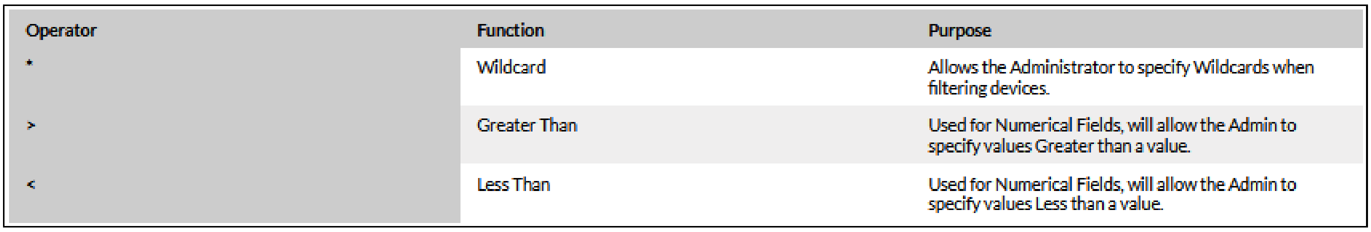
Auto Population

Once an Admin Tag has been created, you can set up conditions so that devices enrolling into Silverback are auto-assigned upon enrollment. Using the information captured during enrollment, Silverback will determine if the incoming device needs to have Tags associated with it.

Device Variables

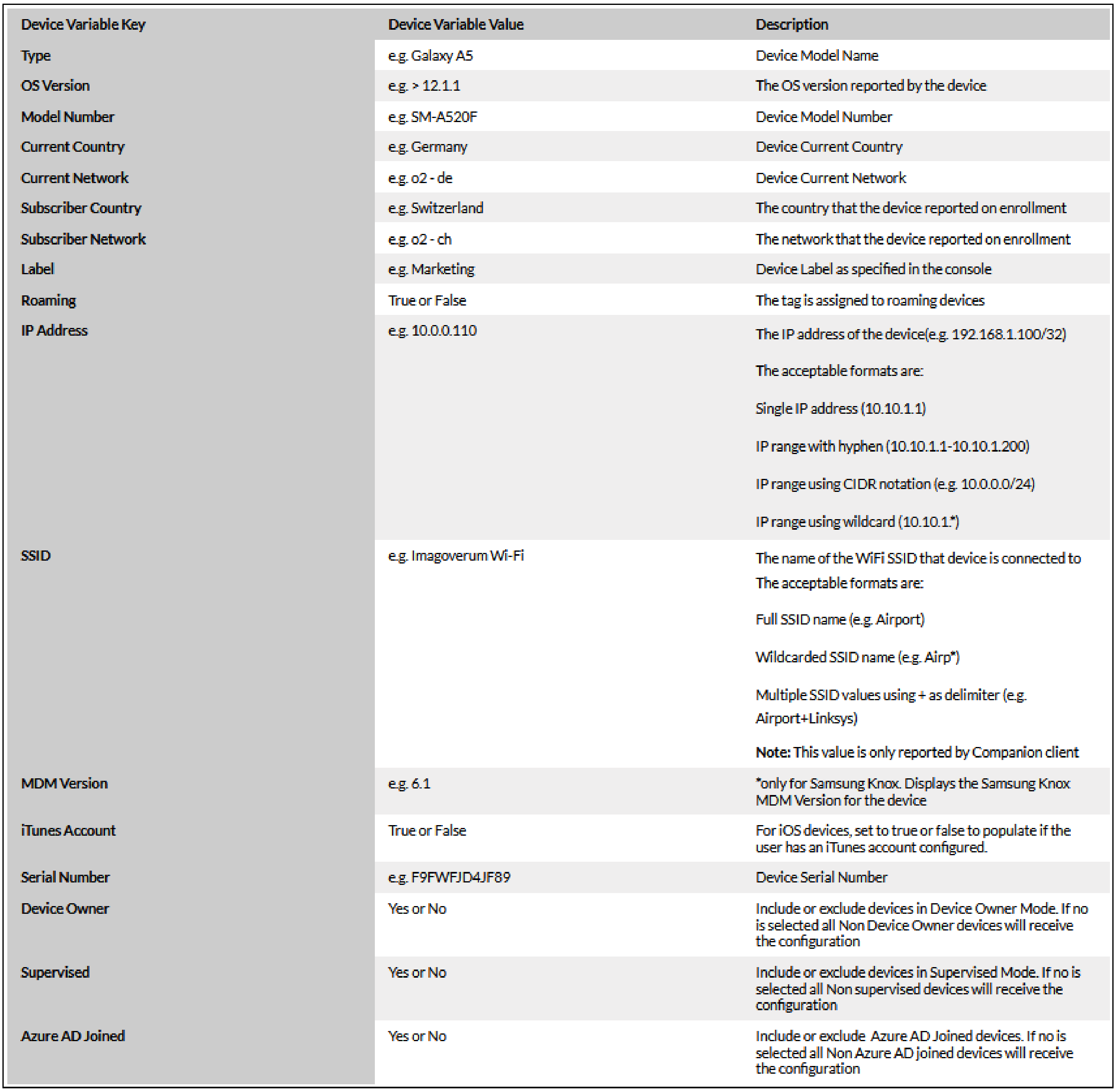
Operators

The Device Variable field does not always have to be ‘absolute’, by using a wildcard (*) character in the Device Variable Value field the scope of the Auto-Population is widened to allow more devices.



Operator	Function	Purpose
*	Wildcard	Allows the Administrator to specify Wildcards when filtering devices.
>	Greater Than	Used for Numerical Fields, will allow the Admin to specify values Greater than a value.
<	Less Than	Used for Numerical Fields, will allow the Admin to specify values Less than a value.

Variables



Device Variable Key	Device Variable Value	Description
Type	e.g. Galaxy A5	Device Model Name
OS Version	e.g. > 12.1.1	The OS version reported by the device
Model Number	e.g. SM-A520F	Device Model Number
Current Country	e.g. Germany	Device Current Country
Current Network	e.g. o2 - de	Device Current Network
Subscriber Country	e.g. Switzerland	The country that the device reported on enrollment
Subscriber Network	e.g. o2 - ch	The network that the device reported on enrollment
Label	e.g. Marketing	Device Label as specified in the console
Roaming	True or False	The tag is assigned to roaming devices
IP Address	e.g. 10.0.0.110	The IP address of the device(e.g. 192.168.1.100/32) The acceptable formats are: Single IP address (10.10.1.1) IP range with hyphen (10.10.1.1-10.10.1.200) IP range using CIDR notation (e.g. 10.0.0.0/24) IP range using wildcard (10.10.1.*)
SSID	e.g. Imagoverum Wi-Fi	The name of the WiFi SSID that device is connected to The acceptable formats are: Full SSID name (e.g. Airport) Wildcarded SSID name (e.g. Airp*) Multiple SSID values using + as delimiter (e.g. Airport+Linksys) **Note:** This value is only reported by Companion client
MDM Version	e.g. 6.1	*only for Samsung Knox. Displays the Samsung Knox MDM Version for the device
iTunes Account	True or False	For iOS devices, set to true or false to populate if the user has an iTunes account configured.
Serial Number	e.g. F9FWFJD4JF89	Device Serial Number
Device Owner	Yes or No	Include or exclude devices in Device Owner Mode. If no is selected all Non Device Owner devices will receive the configuration
Supervised	Yes or No	Include or exclude devices in Supervised Mode. If no is selected all Non supervised devices will receive the configuration
Azure AD Joined	Yes or No	Include or exclude Azure AD Joined devices. If no is selected all Non Azure AD joined devices will receive the configuration

User Variables

LDAP Base DN

In some scenarios, it is necessary to specify the Base DN where the LDAP filter should be performed. The Base DN should be entered into the text box provided, with a Full DN Syntax (Distinguished Name), which can be found using Active Directory User and Computers or another LDAP Browser.

E.g. MemberOf=OU=Frankfurt,DC=imagoverum,DC=com

LDAP Filter

Auto Populating an Admin Tag can also be done using containers that exist within your LDAP schema (or Active Directory). This means that if you have setup distribution groups for individual departments, you can auto assign Tags based on these groups. When adding an LDAP Filter it must be done in Full DN Syntax (Distinguished Name), which can be found using Active Directory User and Computers or another LDAP Browser. An example of Full DN Syntax is displayed below:

Full DN Syntax Example for a Sales Department Distribution group: ***MemberOf=CN=Sales Department, CN=Groups,DC=imagoverum,DC=com***

Ignore Empty Results

The option for "Ignore Empty Results" will tell the server to not remove users from the Tag, if the response from LDAP is empty. In some scenarios an LDAP source can return a valid, successful result however without any LDAP results. Normally this would cause Silverback to remove all users from this Tag. If your LDAP source is returning empty results validly, then use this option to ensure minimal user interruption.

Selected Ownership

Define to which Ownership Type the Tag should be applied. You can choose between All, Corporate and Personal

Manually Associate Devices

- After saving the configured Tag click Associated Devices
- You will see a list of already associated devices
- Click Attach More Device
- Select applicable Devices from the List
- Click Attach Selected Devices
- To detach devices use the Detach functionality.

Export

To Export a list of users associated with a specific Tag, use the following steps:

- Click the Export button and choose the location to save the output file (in XLS Format).

Push

- Click Push to Devices to force a policy update for all associated devices.

Next steps - KSP debug mode

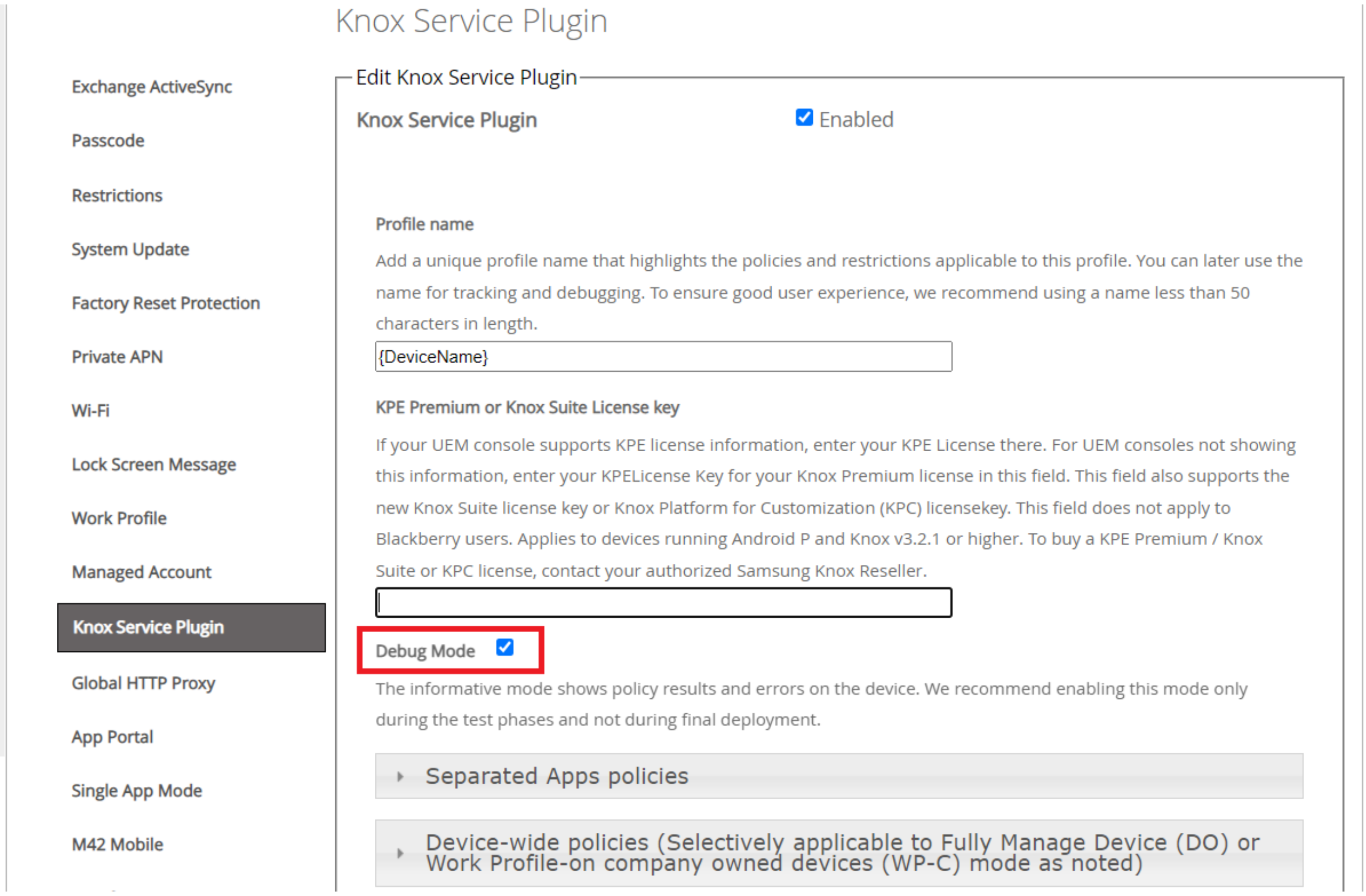
Now you can check the results and policy errors on the devices.

Step 4. Matrix42 MDM: Debug mode

This section provides instructions on how to debug KSP application in Matrix MDM.

How to use KSP debug mode

Debug mode can be helpful in testing and deploying your setup. By default, KSP runs in the background and has no user interface. Debug mode allows you to view the results and policy errors on the device so you can verify that your configurations are correct. When enabled, it runs an application that displays the policy status. This application should start automatically when a new policy is received.



Knox Service Plugin

Edit Knox Service Plugin

Knox Service Plugin ☑ Enabled

Profile name

Add a unique profile name that highlights the policies and restrictions applicable to this profile. You can later use the name for tracking and debugging. To ensure good user experience, we recommend using a name less than 50 characters in length.

{DeviceName}

KPE Premium or Knox Suite License key

If your UEM console supports KPE license information, enter your KPE License there. For UEM consoles not showing this information, enter your KPELicense Key for your Knox Premium license in this field. This field also supports the new Knox Suite license key or Knox Platform for Customization (KPC) licensekey. This field does not apply to Blackberry users. Applies to devices running Android P and Knox v3.2.1 or higher. To buy a KPE Premium / Knox Suite or KPC license, contact your authorized Samsung Knox Reseller.

Debug Mode ☑

The informative mode shows policy results and errors on the device. We recommend enabling this mode only during the test phases and not during final deployment.

Separated Apps policies
Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted)

Feedback can be delivered async and with delay so you can manually send a Refresh Info action to check if any feedback is available.

You can read more about Debug mode in the KNOX Documentation available here.

Next steps - KSP troubleshooting

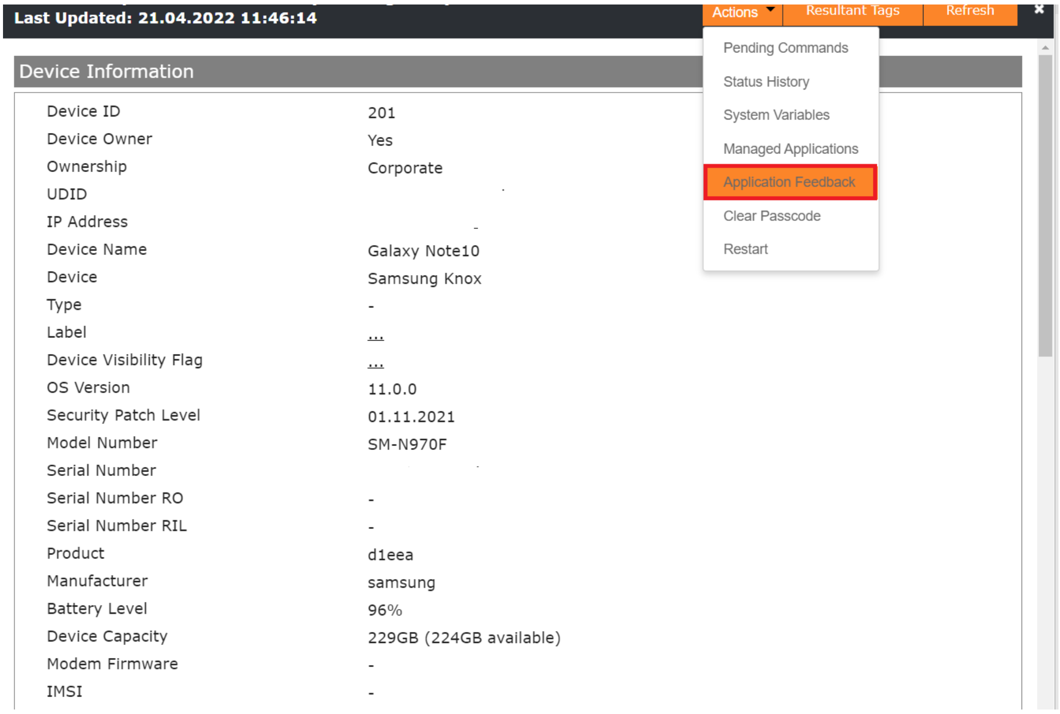
Now you can quick find info about KSP configuration errors.

Step 5. Matrix42 MDM: Troubleshooting

This section provides instructions on how to troubleshoot KSP application in Matrix MDM.

To check if a configuration was properly applied on a specific Samsung device (aka the Feedback Channel):

- From the **Device List** page, select a device then click on it to display the details page
- From the details page, click on the **Action drop down list at the right top of screen**
- **Press Application Feedback**

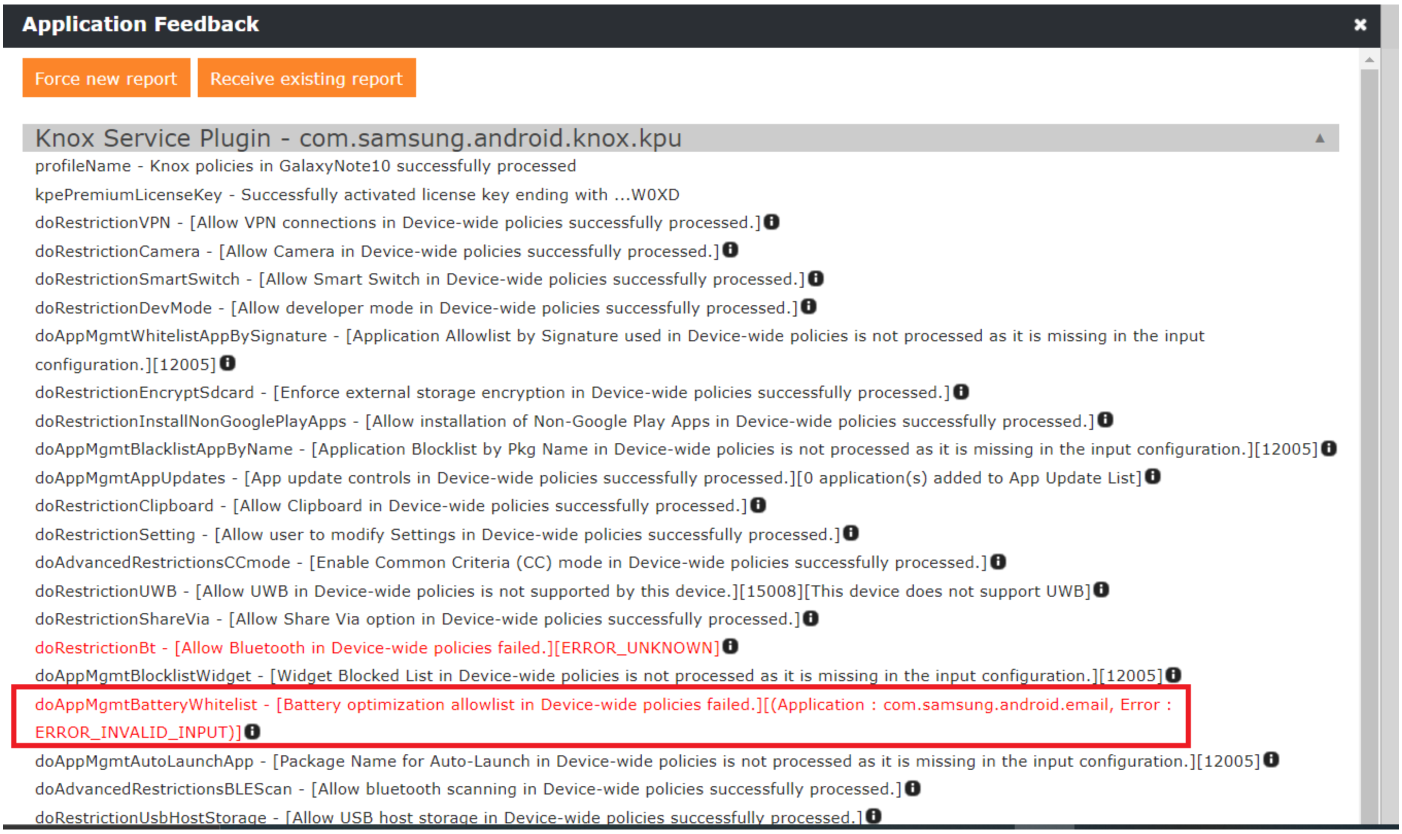


Last Updated: 21.04.2022 11:46:14

Device Information

Device ID	201
Device Owner	Yes
Ownership	Corporate
UDID	
IP Address	
Device Name	Galaxy Note10
Device	Samsung Knox
Type	-
Label	...
Device Visibility Flag	...
OS Version	11.0.0
Security Patch Level	01.11.2021
Model Number	SM-N970F
Serial Number	
Serial Number RO	-
Serial Number RIL	-
Product	d1eea
Manufacturer	samsung
Battery Level	96%
Device Capacity	229GB (224GB available)
Modem Firmware	-
IMSI	-

- Click Force new report



```
Knox Service Plugin - com.samsung.android.knox.kpu
profileName - Knox policies in GalaxyNote10 successfully processed
kpePremiumLicenseKey - Successfully activated license key ending with ...W0XD
doRestrictionVPN - [Allow VPN connections in Device-wide policies successfully processed.]
doRestrictionCamera - [Allow Camera in Device-wide policies successfully processed.]
doRestrictionSmartSwitch - [Allow Smart Switch in Device-wide policies successfully processed.]
doRestrictionDevMode - [Allow developer mode in Device-wide policies successfully processed.]
doAppMgmtWhitelistAppBySignature - [Application Allowlist by Signature used in Device-wide policies is not processed as it is missing in the input configuration.][12005]
doRestrictionEncryptSdcard - [Enforce external storage encryption in Device-wide policies successfully processed.]
doRestrictionInstallNonGooglePlayApps - [Allow installation of Non-Google Play Apps in Device-wide policies successfully processed.]
doAppMgmtBlacklistAppByName - [Application Blocklist by Pkg Name in Device-wide policies is not processed as it is missing in the input configuration.][12005]
doAppMgmtAppUpdates - [App update controls in Device-wide policies successfully processed.][0 application(s) added to App Update List]
doRestrictionClipboard - [Allow Clipboard in Device-wide policies successfully processed.]
doRestrictionSetting - [Allow user to modify Settings in Device-wide policies successfully processed.]
doAdvancedRestrictionsCCmode - [Enable Common Criteria (CC) mode in Device-wide policies successfully processed.]
doRestrictionUWB - [Allow UWB in Device-wide policies is not supported by this device.][15008][This device does not support UWB]
doRestrictionShareVia - [Allow Share Via option in Device-wide policies successfully processed.]
doRestrictionBt - [Allow Bluetooth in Device-wide policies failed.][ERROR_UNKNOWN]
doAppMgmtBlocklistWidget - [Widget Blocked List in Device-wide policies is not processed as it is missing in the input configuration.][12005]
doAppMgmtBatteryWhitelist - [Battery optimization allowlist in Device-wide policies failed.][(Application : com.samsung.android.email, Error : ERROR_INVALID_INPUT)]
doAppMgmtAutoLaunchApp - [Package Name for Auto-Launch in Device-wide policies is not processed as it is missing in the input configuration.][12005]
doAdvancedRestrictionsBLEScan - [Allow bluetooth scanning in Device-wide policies successfully processed.]
doRestrictionUsbHostStorage - [Allow USB host storage in Device-wide policies successfully processed.]
```

The info or error messages allow you to quickly identify a problem with the KSP configuration.

The list of errors with possible causes and suggested solutions is available here .

Useful links:

Matrix KSP admin guide: Matrix42 MDM admin guide

Samsung's KSP admin guide: Samsung KSP admin guide

KSP page on Google Play: Samsung KSP details