

Knox Service Plugin for Chimpa 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: Chimpa MDM - Add to UEM console

<https://www.chimpa.eu/en/> is a secure, mobile device management portal that works with KSP.

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

Before you begin

Before you begin, however, ensure that you have:

1. Access to the <https://www.chimpa.eu/en/contact/> console.
2. Linked your Chimpa 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 Chimpa MDM console, see https://wiki.chimpa.eu/docs/en/doc_0

How to add Knox Service Plugin to Chimpa






OEMConfig is a new standard that allows you to create and remotely push configurations to apps through an XML schema.

KSP is Samsung's OEMConfig based solution that enables IT admins to apply advanced Knox Platform for Enterprise (KPE) restrictions and configurations as soon as they're available.

Chimpa MDM pre-approves KSP in the Google Play Managed.

Minimum device requirements for KSP: Android 9+ (Knox 3.2.1+), Android 8.0 (Knox v3.x) requires a fully managed device (Supervised / DO) provisioning.

Full instructions on the configuration of MGP can be found [here](#).

LICENZE		Cerca...		↺	+
	NOME	ASSEGNATE	DISPONIBILI		
	Ketnet Junior	0	∞	✕	⚙️
	Minha Prova - Aluno	0	∞	✕	⚙️
	Slack	3	∞	✕	⚙️
	Google Chrome: Fast & Secure	94	∞	✕	⚙️
	Asana: organize team projects	0	∞	✕	⚙️

For more information on customize apps parameters to the Managed App Catalog, see https://wiki.chimpa.eu/docs/en/doc_6_0_2

Next steps - Configure KSP

Step 2: Chimpa MDM - Configure

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

To use KSP it is necessary to configure a [Samsung Knox](#) Payload in a group's or devices Android profile.

Organization > New profile

Search parameter

General

Mandatory

Passcode

Not Configured

Restrictions

Not Configured

Certificates

Not Configured

Network

Not Configured

Web Content Filter

Not Configured

VPN Always-ON

Not Configured

Cellular

Not Configured

Wallpaper

Not Configured

Lock Screen Message

Not Configured

Monitoring

Not Configured

Geofence

Not Configured

Power management

Not Configured

Video sources management

Not Configured

Video Settings

Not Configured

Samsung Knox

1 Payload Configured

Permitted Google Accounts

Not Configured

DNS Settings

Not Configured

Profile name *Field id: (profileName)*

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. Default value: Knox profile

Knox profile Wildcard

KPE Premium or Knox Suite License key *Field id: (kpePremiumLicenseKey)*

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.

Wildcard

Debug Mode *Field id: (verboseMode)*

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.

No

SEPARATED APPS POLICIES *(Field id: appSepPolicies)*

A group of policies and restriction that are applicable to Separated apps.

DEVICE-WIDE POLICIES (SELECTIVELY APPLICABLE TO FULLY MANAGE DEVICE (DO) OR WORK PROFILE-ON COMPANY OWNED DEVICES (WP-C) MODE AS NOTED) *(Field id: doPolicies)*

A global group of policies and restrictions that are applicable to all users of the device. This list includes items that impact all users on the device, whether they

WORK PROFILE POLICIES (PROFILE OWNER) *(Field id: poPolicies)*

A group of policies and restrictions that are applicable to the Work profile user of the device. Starting Knox 3.0, a KPE Premium license activation is required for using any policy in the work profile.

DEX CUSTOMIZATION PROFILE (PREMIUM) *(Field id: profileDexCustomization)*

A group of settings that help customize Samsung DeX experience for the user. These features are available only with a KPE Premium license.

DEVICE AND SETTINGS CUSTOMIZATION PROFILE (PREMIUM) *(Field id: profileDeviceCustomization)*

A group of controls to configure and customize the device user's experience. These features are available only with a KPE Premium license with customization permissions.

Cancel Save

Edit KSP policies

Click Samsung Knox payload configuration tab. KSP provides a number of configurable parameters. To facilitate navigation in the settings, you can use the search field.

Organization > New profile

Search parameter

General

Mandatory

Passcode

Not Configured

Restrictions

Not Configured

Certificates

Not Configured

Network

Not Configured

Web Content Filter

Not Configured

VPN Always-ON

Not Configured

Cellular

Not Configured

Wallpaper

Not Configured

Lock Screen Message

Not Configured

Monitoring

Not Configured

Geofence

Not Configured

Power management

Not Configured

Video sources management

Not Configured

Video Settings

Not Configured

Samsung Knox

1 Payload Configured

Permitted Google Accounts

Not Configured

DNS Settings

Not Configured

Profile name *Field id: (profileName)*

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. Default value: Knox profile

Knox profile Wildcard

KPE Premium or Knox Suite License key *Field id: (kpePremiumLicenseKey)*

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.

Wildcard

Debug Mode *Field id: (verboseMode)*

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.

No

SEPARATED APPS POLICIES *(Field id: appSepPolicies)*

A group of policies and restriction that are applicable to Separated apps.

DEVICE-WIDE POLICIES (SELECTIVELY APPLICABLE TO FULLY MANAGE DEVICE (DO) OR WORK PROFILE-ON COMPANY OWNED DEVICES (WP-C) MODE AS NOTED) *(Field id: doPolicies)*

A global group of policies and restrictions that are applicable to all users of the device. This list includes items that impact all users on the device, whether they

WORK PROFILE POLICIES (PROFILE OWNER) *(Field id: poPolicies)*

A group of policies and restrictions that are applicable to the Work profile user of the device. Starting Knox 3.0, a KPE Premium license activation is required for using any policy in the work profile.

DEX CUSTOMIZATION PROFILE (PREMIUM) *(Field id: profileDexCustomization)*

A group of settings that help customize Samsung DeX experience for the user. These features are available only with a KPE Premium license.

DEVICE AND SETTINGS CUSTOMIZATION PROFILE (PREMIUM) *(Field id: profileDeviceCustomization)*

A group of controls to configure and customize the device user's experience. These features are available only with a KPE Premium license with customization permissions.

Click **Save**. The KSP App Configurations settings page save polices that are currently applied to KSP.

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 Chimpa MDM console, you need to deploy the app to your managed devices.

Step 3. Chimpa MDM: Deploy

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

Deploy KSP

Once set up, Knox Service Plugin is ready to be deployed to your devices. All you have to do is to press confirm button after you save configuration.

Configuration "Knox Service Plugin"

RUNTIME PERMISSIONS

MANAGED CONFIG

Search name...

-

^ SEPARATED APPS POLICIES (Field id: appSepPolicies)

A group of policies and restriction that are applicable to Separated apps.

Enable Separated Apps Field id: (appSepPoliciesIsControlled)

Turn Separated Apps policies on or off. Enable this option before using any of the Separated Apps policies. If this option is disabled, KSP will apply policy to remove Separated Apps from the device, all apps installed inside Separated Apps will be uninstalled from the device.

No

^ ALLOW LIST POLICY (Field id: appSepAllowListingPolicies) /SEPARATED APPS POLICIES

A group of policies for specifying the list of apps to be separated and whether the specified list of apps should be installed outside or inside of the separate space.Available Knox 3.7 or higher

Location for Separate Apps installation Field id: (appSepAllowListingAppsLocation)

If the value is set to Outside, List of specified apps will be installed outside (i.e. in user0), apps not in the list will be installed inside. if the value is set to Inside, List of specified apps will be installed inside (i.e. inside separate space), apps not in the list will be installed outside

Outside

These configurations will be applied only on devices with Android Lollipop 5.0 and later

Cancel

Apply

Next steps - KSP debug mode

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

Step 4. Chimpa MDM: Debug mode

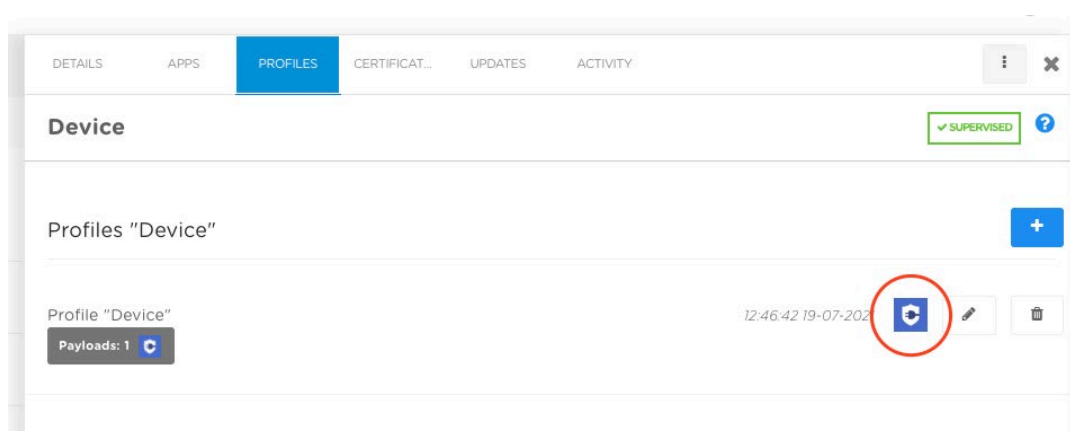
This section provides instructions on how to debug KSP application in Chimpa MDM.



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.

Once the Payload has been configured, it is possible to consult the Feedback Channel to verify that the parameters have been applied correctly in two ways:

- If the payload has been configured in a device profile, click on KSP icon next to profile edit button



- If the payload has been configured in a group profile, click on  button to the right of the profile and in the list of devices and click on the  icon

Managed Config Feedback			
Updated at: 07:30:48 of 06-16-2021			
Path	Policy	Status	Detail
Root	Profile name	✓	profileName Knox policies in KVP successfully processed
Root	KPE Premium or Knox Suite License key	✓	kpePremiumLicenseKey Successfully activated license key ending with ...LOJS
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Allow microphone	✓	doRestrictionMic [Allow microphone in Device-wide policies successfully processed.]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Allow WiFi	✓	doRestrictionWifi [Allow WiFi in Device-wide policies successfully processed.]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Allow WiFi Direct	✓	doRestrictionWifiDirect [Allow WiFi Direct in Device-wide policies successfully processed.]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Allow Bluetooth	✗	doRestrictionBt [Allow Bluetooth in Device-wide policies failed.] [ERROR_UNKNOWN]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Allow cellular data	✓	doRestrictionCellular [Allow cellular data in Device-wide policies successfully processed.]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions	Tethering controls	✓	doRestrictionTethering [Tethering controls in Device-wide policies successfully processed.]
Root > Device-wide policies (Selectively applicable to Fully Manage Device (DO) or Work Profile-on company owned devices (WP-C) mode as noted) > Device Restrictions			
Close			

Note: 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](#).

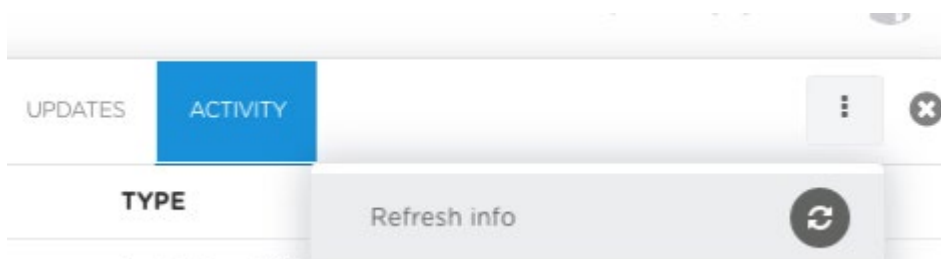
Next steps - KSP troubleshooting

Now you can quick find info about KSP configuration errors.

Step 5. Chimpa MDM: Troubleshooting

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

Check in Activity if the status of the Refresh Info action has been set to Delivered.



You can also check feedbacks in the Activity logs clicking over the single action's status (shown with an "i" icon).

> MANAGEMENT > DEVICES		DETAILS	APPS	PROFILES	CERTIFIC...	RESTRICT...	UPDATES	ACTIVITY		
		SENT	DELIVERED		TYPE			STATUS		
		15:14:09 25-05-2020	--		Refresh info			Pending		
		14:44:15 25-05-2020	--		Refresh info			Cancelled		
		14:36:41 25-05-2020	14:36:41 25-05-2020		Set Managed Config Knox Ser...			Delivered		
		13:46:08 25-05-2020	14:27:41 25-05-2020		Refresh info			Delivered		
		13:41:52 25-05-2020	--		Refresh info			Cancelled		
		13:15:52 25-05-2020	--		Set Managed Config Knox Ser...			Error		
		SEVERITYINFO key:"profileName" message:Knox policies in sssffPro222s successfully processed SEVERITYINFO key:"doDexDisablePackages" message:[0 application(s) disabled for Dex] SEVERITYINFO key:"kpePremiumLicenseKey" message:Successfully activated license key ending with ...K3BQ SEVERITYINFO key:"doRestrictionVPN" message:[Allow VPN connections in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionCamera" message:[Allow Camera in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionDevMode" message:[Allow developer mode in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doDexEnforceEthernet" message:[Enforce the use of Ethernet connection in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionEncryptSdcard" message:[Enforce external storage encryption in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionInstallNonGooglePlayApps" message:[Allow installation of Non-Google Play Apps in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionSetting" message:[Allow user to modify Settings in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doPasswordDisableKeyguardFeature" message:[Disable Keyguard Feature in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionBluetooth" message:[Allow Bluetooth in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionShareVia" message:[Allow Share Via option in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doPasswordQualityDefinition" message:[Define Password Quality in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doPasswordMaxFailedAttemptToWipeData" message:[Maximum Failed Password Attempt to Wipe Data in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionUsbHostStorage" message:[Allow USB host storage in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionWifiDirect" message:[Allow WiFi Direct in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionCellular" message:[Allow cellular data in Device-wide policies (Device Owner) successfully processed.] SEVERITYERROR key:"doRestrictionUsbExceptionList" message:[Setup USB exception list in Device-wide policies (Device Owner) failed.][ERROR_UNKNOWN] SEVERITYINFO key:"doRestrictionUsbDebug" message:[Allow USB debugging in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionUsbMediaPlayer" message:[Allow USB media player in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doFirewallPolicy" message:[Firewall and Proxy policy in Device-wide policies (Device Owner) successfully processed.] SEVERITYINFO key:"doRestrictionDataSaver" message:[Allow data saver mode in Device-wide policies (Device Owner) successfully processed.]								

The 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:

Chimpa KSP admin guide: https://wiki.chimpa.eu/docs/en/doc_11_11

Samsung's KSP admin guide: <https://docs.samsungknox.com/admin/knox-service-plugin/welcome.htm>

KSP page on Google Play: <https://play.google.com/store/apps/details?id=com.samsung.android.knox.kpu>