SAMSUNG Knox

Whitepaper

Implementing FIDO Authentication in Knox™

March 2017

Copyright Notice

Document History

Date	Changes
March 2017	First version of document.

Contact Information

If you want to contact us about …	You have these options …
General Knox questions	Knox Portal, for comprehensive information about Knox
How to get Knox	Try Knox, to start a free trial, get pricing info, or buy Knox Contact Knox Sales, if you need help buying Knox
Technical questions	Knox Support, for self-help resources like videos, guides, and FAQs If you already have a Knox portal account, log in to see all the resources available to you. If you do not have an account, you can register for one.
Other support options	Contact Knox Support

Contents

Purpose

This document describes how to implement and configure FIDO authentication within Samsung Knox Workspace containers

Audience

This document is designed for EMM IT administrators.

Key words

- *Active Directory (AD) Container*—Container configured with Enterprise ID, so it is unlocked and used when the user provides their enterprise credentials. This feature reduces user's password fatigue by enabling the user to manage all enterprise resources with a single password. By enabling the SSO (Single-Sign-On) feature, the apps installed on the device can leverage the Enterprise ID and allow users seamless access without requiring additional credentials.
- *Enterprise ID*—Credential that recognizes the user on the enterprise domain which the user is associated. IT admins can use the user's enterprise ID to allow access to managed resources of the enterprise. If a user is using the enterprise ID to access the Knox Workspace container, they can access apps provided by the enterprise without the necessity of additional login processes.
- *FIDO (*Fast IDentity Online*)*—Online authentication method that uses a mobile device's biometric identification feature.

How to configure FIDO inside Knox container

To configure FIDO inside the Knox Workspace container, you have two options:

- Configure Active Directory container
- Configure FIDO client inside Knox container

Configure AD Container

You can configure Enterprise ID support for new Knox Workspace containers, as well as existing containers on a device. For new containers, the container creation parameters contain the information needed to configure the enterprise ID. For existing containers, you configure the enterprise ID for the container via the Password policy.

This section describes how to configure FIDO for new and existing Knox containers.

For new containers

Perform the following steps:

1. Install the Kerberos authenticator using: `ApplicationPolicy.installApplication`.

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/android/app/enterprise/ApplicationPolicy.html#installApplication(java.lang.String, boolean)

2. Use the `AuthenticationConfig` class to configure enterprise identity. This class includes all information including ID server configuration and enforcement specification. The object of this class delivers the parameter for `KnoxConfigurationType.setEnterpriseIdentityAuthentication`.

   If you want to enforce enterprise ID as the only option to unlock a Knox Workspace container, you must call `setForceEnterpriseIdentityLock` and `setAuthenticatorConfig` as well.

   Create the text file containing configuration information such as server URL and domain URL and apply the configuration value to the device.

   Example:

   ```
   authconfig.txt - LIBDEFAULTS_DEFAULT_REALM:SISOIDP.IN,
   FEDERATION_SERVER_URL:idpsrv.sisoidp.in
   ```

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/identity/AuthenticationConfig.html

3. To apply the `AuthenticationConfig` object on the device, set: `KnoxConfigurationType.setEnterpriseIdentityAuthentication`.

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/knox/container/KnoxConfigurationType.html#setEnterpriseIdentityAuthentication(com.sec.enterprise.identity.AuthenticationConfig)

4. Call `KnoxContainerManager.addConfigurationType` to create a custom container type and call `KnoxContainerManager.createContainer` to create a container as policy defines.

   For detailed information, please refer to the following URL:

https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/knox/container/KnoxContainerManager.html

5. If all polices and configurations are applied, then the enterprise ID is the only option for unlocking a Knox container during Knox container creation. Once this is accomplished, users can access the Knox container with their enterprise ID.

For existing containers

In this use case, there is no option of using the enterprise ID as the container unlock type. Only traditional options such as password/pattern/pin are available.

1. Install Kerberos authenticator on Knox container using: `ApplicationPolicy.installApplication`.

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/android/app/enterprise/ApplicationPolicy.html#installApplication(java.lang.String, boolean)

2. Use the `AuthenticationConfig` class to configure an enterprise ID as the unlock type. This class includes all required information, including ID server configuration and enforcement specification. The object of this class delivers the parameter for `PasswordPolicy.setEnterpriseIdentityAuthentication`.

   If you want to enforce the enterprise ID as the only option to unlock a Knox container, you must set: `AuthenticationConfig.setForceEnterpriseIdentityLock` and call `setAuthenticatorConfig` to configure the enterprise ID.

   Create the text file containing configuration information such as server URL and domain URL and apply the configuration value to the device.

   Example:

   ```
   authconfig.txt - LIBDEFAULTS_DEFAULT_REALM:SISOIDP.IN,
   FEDERATION_SERVER_URL:idpsrv.sisoidp.in
   ```

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/identity/AuthenticationConfig.html

3. In order to apply the `AuthenticationConfig` object on the device, set `setEnterpriseIdentityAuthentication`.

   For detailed information, please refer to the following URL:

https://seap.samsung.com/api-references/android-premium/reference/android/app/enterprise/PasswordPolicy.html#setEnterpriseIdentityAuthentication(com.sec.enterprise.identity.AuthenticationConfig

4. After you have completed the prior steps, apply the "enforce password change" policy to changing the typical lock types to enterprise ID as only unlock type. When you apply the policy, all of the setting values defined on `AuthenticationConfig` class is configured.

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/android/app/enterprise/PasswordPolicy.html#enforcePwdChange()

5. If all polices and configurations are applied, users are required to authenticate the previous unlock type and following authentication, the enterprise ID will be the only option for unlocking the Knox Workspace container. After setup completes, users can access Knox container with their enterprise ID.

Configure FIDO client inside Knox container

To configure the FIDO client inside a Knox Workspace container:

1. Set FIDO client information using the Container Configuration policy:

   ```
   public boolean setFIDOInfo (Bundle fidoinfo)
   ```

2. Set the following strings:

   - `ContainerConfigurationPolicy.FIDO_REQUEST_URI`
   - `ContainerConfigurationPolicy.FIDO_RESPONSE_URI`

   For detailed information, please refer to the following URL:

   https://seap.samsung.com/api-references/android-premium/reference/com/sec/enterprise/knox/container/ContainerConfigurationPolicy.html#setFIDOInfo(android.os.Bundle)

Verify FIDO server configuration

To complete the configuration, go to **Knox Settings > Lock type** and enable registered biometric data.