

Configuring Device Single Sign-On (SSO)

fork and edit tutorial (<https://github.ibm.com/MFPSamples/DevCenter/tree/master/tutorials/en/foundation/8.0/authentication-and-security/device-ssu/index.md>) | report issue (<https://github.ibm.com/MFPSamples/DevCenter/issues/new>)

Overview

MobileFirst Foundation offers a Single Sign-On (SSO) feature which enables sharing the state of any custom security check between multiple applications on the same device. For example, using Device SSO allows users to successfully sign onto one application on their device and also be authenticated on other applications on the same device using the same implementation.

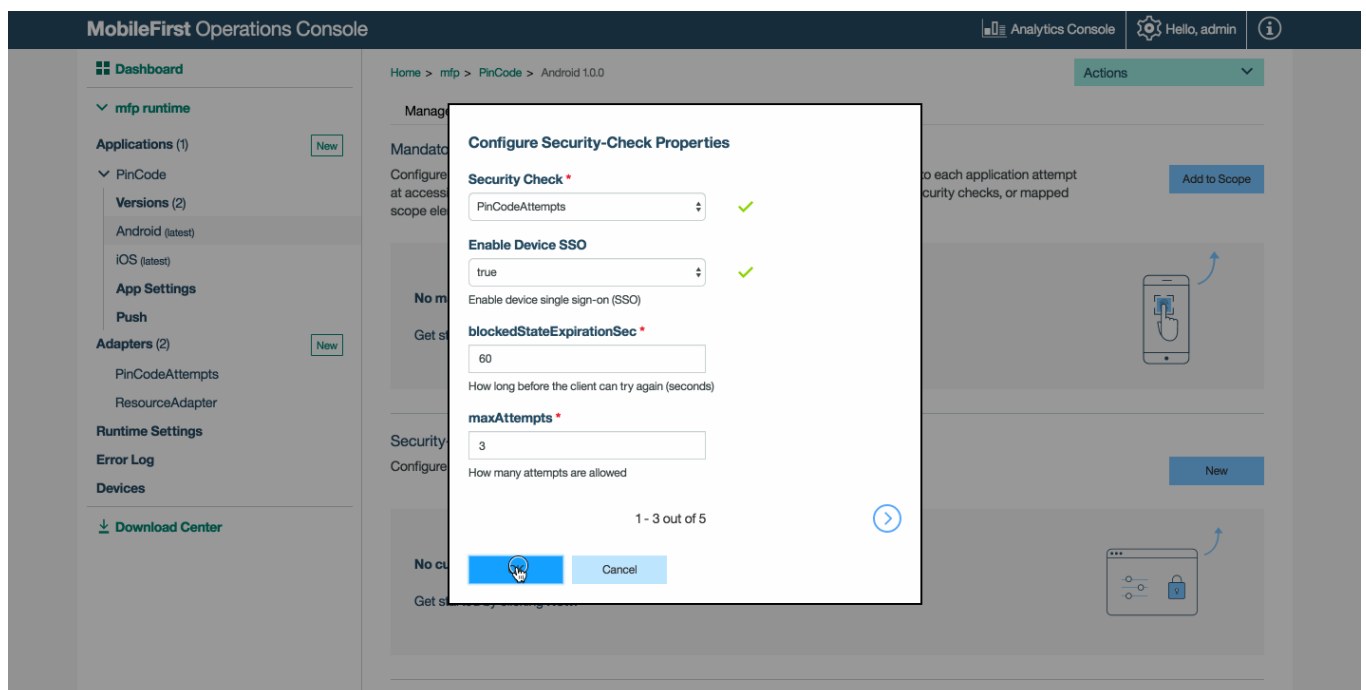
Prerequisite: Make sure to read the Authentication and Security (../) tutorials.

Configuring SSO

In the MobileFirst Operations Console:

1. Navigate to **[your application] → Security tab → Security-Check Configurations** section.
2. Click on the "New" button to create a new security check configuration, or the "Edit" icon if there is already an existing security check configuration.
3. In the **Configure Security-Check Properties** dialog, set the **Enable Device SSO** setting to **true** and press **OK**.

Repeat these steps for each of the applications you want to enable Device SSO for.



Using Device SSO with a Pre-Existing Sample

Read the Credential Validation (../credentials-validation/) tutorial as we will be using its sample to configure Device SSO.

For this demonstration the Cordova sample application will be used, however the same can be done also with the iOS, Android and Windows sample applications.

1. Follow the sample usage instructions (../credentials-validation/javascript/#cordova-sample-usage).

2. Repeat the steps with a different sample name and application identifier.
3. Run both applications on the same device. Notice how in each application you will be prompted for the pincode ("1234").
4. In the MobileFirst Operations Console, set `Enable Device SS0` to `true` for each of the applications as instructed above.
5. Quit both applications and try again. In the first application you will open, you will be prompted to enter the pincode once tapping the "Get Balance" button. Once opening the second and tapping the "Get Balance" button you will not need to enter the pincode again to get the balance.

Note that the `PinCodeAttempts` security check has a 60 seconds expiration token, so once trying again after 60 seconds the second application will require a pincode.

