Configuring Device Single Sign-On (SSO)

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, by using Device SSO, users can successfully sign on to one application on their device and also be authenticated on other applications on the same device that uses the same implementation.

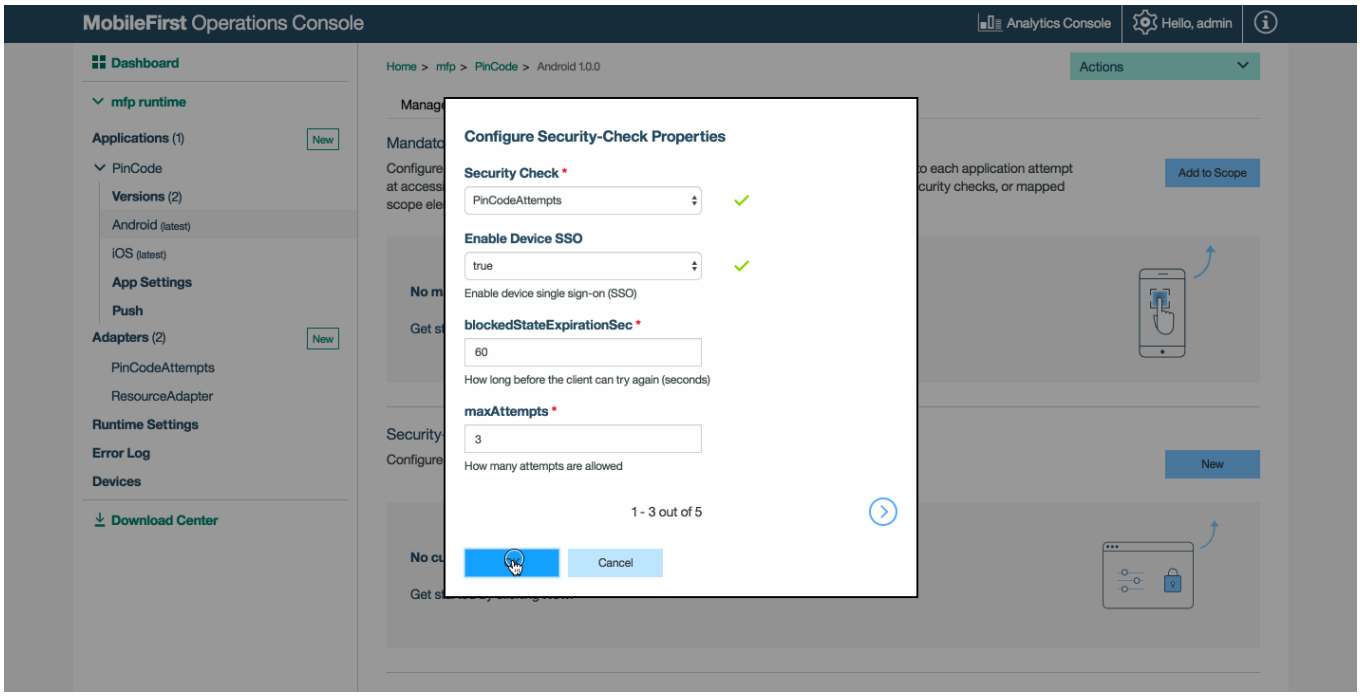
Prerequisite: Make sure to read the Authentication and Security (../) tutorials.

Configuring SSO

In the MobileFirst Operations Console:

1. Navigate to **[your application] → Security tab → Security-Check Configurations** section.
2. Click the **New** button to create a new security check configuration, or the **Edit** icon if a security check configuration already exists.
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 the enable Device SSO for.



You can also manually edit the application's configuration JSON file with the required configuration and push the changes back to a MobileFirst Server.

1. From a **command-line window**, navigate to the project's root folder and run the `mfpdev app pull`.
2. Open the configuration file, located in the **[project-folder\mobilefirst** folder.
3. Edit the file to enable device SSO for your selected custom security check: device SSO is enabled by setting the `enableSSO` property of a custom security check to `true`. The property configuration is contained within a security-check object that is nested in a `securityCheckConfigurations`

object. Locate these objects in your application descriptor file, or create them if they are missing. For example:

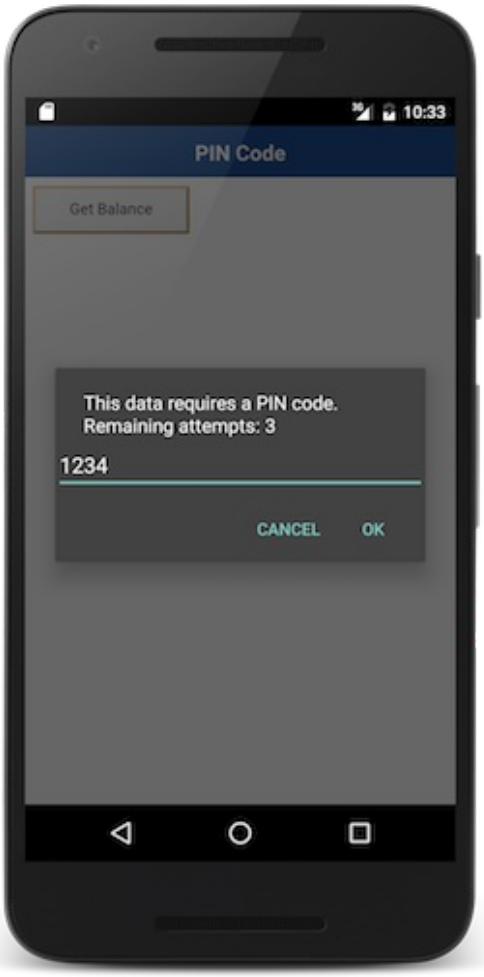
```
"securityCheckConfigurations": {
   "UserAuthentication": {
      ...
      ...
      "enableSSO": true
   }
}
```

4. Deploy the updated configuration JSON file by running the command: `mfpdev app push`.

Using Device SSO with a Pre-Existing Sample

Read the Credential Validation (../credentials-validation/) tutorial because its sample is used to configure Device SSO.
For this demonstration, the Cordova sample application is used, however you can do the same also with the iOS, Android, and Windows sample applications.

1. Follow the sample usage instructions (../credentials-validation/javascript/#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 are prompted for the pincode ("1234").
4. In the MobileFirst Operations Console, set `Enable Device SSO` to `true` for each of the applications, as instructed above.
5. Quit both applications and try again. In the first application you open, you are prompted to enter the pincode once by tapping the **Get Balance** button. After you open the second application and tap the **Get Balance** button, you do not need to enter the pincode again to get the balance. `Note that the`PinCodeAttempts` security check has a 60-second expiration token. Therefore, after one more attempt after 60 seconds, the second application requires a pincode.


10:33
PIN Code
Get Balance
This data requires a PIN code.
Remaining attempts: 3
1234
CANCEL
OK


10:32
PIN Code
Get Balance
19938.80