Mobile Device Management
SAP SuccessFactors Mobile

June 2016
Customers and Partners
Legal Disclaimer

Coding Samples
Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility
The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language
As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks
The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).
1.1. **Mobile Device Management**

1.1.1. Android Support

1.1.2. Simple Activation of the SAP SuccessFactors Mobile Application

1.1.3. Restricting Access to Managed Devices

1.1.4. One step activation and Single Sign On

1.1.5. Jailbroken or Rooted devices
1. Mobile Device Management

Mobile Device Management (MDM) is a 3rd party solution that securely manages mobile devices in the enterprise and enables both corporate-supplied and Bring Your Own Device (BYOD) mobile deployment strategies. The SAP SuccessFactors Suite integrates with these solutions to ensure secure deployment and activation of the SAP SuccessFactors Mobile application. Please refer to the SAP SuccessFactors Mobile app roadmap for a list of supported MDM vendors.

SAP SuccessFactors MDM integration allows 2 different activation scenarios that can be easily enabled from the SAP SuccessFactors Web Admin panel:

1. Simple activation where user only needs username/password to activate.
2. Restrict user activation on non-managed devices.

Both scenarios involve obtaining a set of key / value pairs from the SAP SuccessFactors web admin panel and pushing these key / value pairs to the device via the MDM solution. The customer can log into the SAP SuccessFactors web admin center to see which values to push to the device for the desired feature. See the below example:
1.1.1. Android Support

To utilize an MDM solution with Android devices, the SAP SuccessFactors Mobile application requires Google’s “Android for Work” framework. Customer should choose an MDM vendor that support the Android for Work framework. The SAP SuccessFactors Mobile application support Android for Work framework on devices with Android 5.0 “Lollipop” OS version or higher. Please refer to Google’s Android for Work supported device list.

1.1.2. Simple Activation of the SAP SuccessFactors Mobile Application

This feature allows the IT admin to enable a simple activation where the end user only needs to provide a username and password to activate the device. Within this section you should see the SFSF_DomainName and SFSF_Instance keys and values. Copy these keys and values and add them to your MDM solution to push these keys to a mobile device managed by your MDM solution. Check
your MDM solution to ensure that these keys and values have been successfully pushed to the mobile device and to make sure that the values do not have any leading or trailing spaces before installing the SAP SuccessFactors mobile application on the device.

In the example above, it would be:

**SFSF_DomainName** : salesdemo4.successfactors.com  
**SFSF_Instance** : Sapphire03

When the app starts the activation flow, it recognizes if these values are set by the MDM solution and initiates simple activation instead of the normal code activation. In this scenario, user needs to input the username/password in order to activate, see example screenshot below:

To enable simple activation follow these steps:

1. Push the mobile application on all MDM enabled devices. Previous versions of the application that were downloaded from iTunes will be deactivated once restricted access is turned on.
2. Go to MDM settings in Admin tools from the Admin Tools >>> Mobile>> Enable Mobile Features >> Mobile Settings Page.
3. Copy the SFSF_DomainName and SFSF_Instance key/value pairs like in the example shown below, and add them to the MDM system as an App Managed Configuration.
4. SAP SuccessFactors Mobile application will now use the simple activation process for those managed devices. This means that the user will only have to authenticate (following the existing SAP SuccessFactors authentication mechanism in place for this instance) in order to activate the SAP SuccessFactors Mobile application.

Note: By default, the mobile application respects the authentication set up for the specific instance of SAP SuccessFactors that is described in the keys. SSO can be configured on SAP SuccessFactors backend or MDM side for silent authentication. Please refer to SSO configuration guide. If that authentication fails, the app displays the default activation screen and prompts the user to go through activation using the displayed Activation code.

1.1.3. Restricting Access to Managed Devices

Restricting activation to manage devices ensures that only devices controlled by your MDM solution will be allowed to activate the SAP SuccessFactors mobile application. To enable this option, login to the SAP SuccessFactors Web Admin Center and find the Mobile Device Management section. Within this section check the “Restrict Activations to managed devices” check box. Copy the SuccessFactors key and value that is in this section. Add them to your MDM solution to push these keys to a mobile device managed by your MDM solution. Check your MDM solution to ensure that these keys and values have been successfully pushed to the mobile device.

On the mobile device, when the SAP SuccessFactors Mobile app is launched, it will compare the value of the SAP SuccessFactors key from the service against the value from the MDM system. If no such value found from the MDM system (i.e. device is not managed) or if the value is not identical to the one from the SAP SuccessFactors service (i.e. device is not managed by that customer), the app will immediately delete the user profile and show this screen.
To restrict access to the SAP SuccessFactors Mobile application to managed devices only, follow the given steps:

1. Push the mobile application on all MDM enabled devices. Previous versions of the application that were downloaded from iTunes will be deactivated once restricted access is turned on.

2. Go to MDM settings in Admin tools from the Admin Tools >> Mobile>> Enable Mobile Features >> Mobile Settings Page.

3. Copy the SuccessFactors key/value pair like the example shown below and add it to the MDM system as an App Managed Configuration.

```
Restrict Activations to managed devices
Please pass this unique key/value pair to your Managed devices
SuccessFactors: C61C9246-7610-31b8-6117-d24f7b5063ca
```

4. Once you have pushed the application and copied the key, we recommend that you wait for a week to turn on restriction of access, to allow the propagation of the SFSF Key/Value pair.

5. In the Mobile Settings page, check the "Restrict Activations to managed devices" box.
6. The following pop up box will appear:

![Confirmation](image)

7. Click "Turn ON" to begin restricted activation.
8. Restricted access is now turned on for mobile users with MDM enabled devices with user accounts in that instance of SAP SuccessFactors.

Note: Once the administrator has enabled the restriction of activation for an SF instance, the SAP SuccessFactors mobile application checks whether the key/value pair presented by the SAP
SuccessFactors server is the same as the one stored in the MDM configuration. The user is able to proceed with activation and usage only if they match.

Each time the mobile application is launched, the SAP SuccessFactors Mobile application checks if the key/value pair in the managed device is the same as the one sent by the SAP SuccessFactors server. If not, the mobile user is de-activated.

1.1.4. One step activation and Single Sign On

MDM solutions have the capability of pushing digital certificates to enable SSO for mobile apps. The SAP SuccessFactors mobile application takes advantage of this as well by utilizing the default mobile browser for application login. To enable a complete activation and Single Sign On solution, use the steps above to setup Simple Activation and optionally Restricting activation to manage devices. Next, follow the instructions for your MDM solution to generate and push an authentication certificate to the mobile device as well. When all key & values and certificates have been pushed to the device, the SAP SuccessFactors mobile app when installed and launched should bypass all authentication screens and take the user directly to the application home screen.

We recommend that you test each step individually before attempting this configuration to ensure easy diagnosis of problems.

1.1.5. Jailbroken or Rooted devices

The SAP SuccessFactors application will not allow activation on a jailbroken or rooted device to safeguard the information accessed by the application. If the device is jailbroken or rooted or hacking tool is installed after activation, SAP SuccessFactors mobile application has several jailbroken detection code build-in and automatically de-activate application and delete all data.

We highly recommend that the MDM administrator remove all enterprise managed applications once jail breaking is detected on a managed device.

Next, the SAP SuccessFactors admin can regenerate a new key / value pair to ensure activation is restricted to managed devices. Once the new key / value pair has been propagated to the devices, the administrator can delete the old key from the MDM system. All devices that do not have the updated key / value pair will be de-activated.

*Generating a new SAP SuccessFactors Key-Value*

Click on the Settings wheel to regenerate a new Key/Value pair if needed.
An admin can now delete the old key and propagate the new one to managed devices.