SAP SuccessFactors

PUBLIC

Document Version: August 2021 – 2021-08-23

Mobile Security Guide

THE BEST RUN SAP

Content

1 Change History

Learn about changes to the documentation for Mobile Security Guide in recent releases.

1H 2021

Type of Change	Description	More Info
Changed	We removed information about Jam features because Jam on SAP SuccessFactors Mobile apps is deleted as of the May 2021 release.	

2H 2020

Type of Change	Description	More Info
Changed	We updated information about session timeout settings.	Frequently Asked Questions [page 17]
Added	We added information about the application of multi-factor authentication (MFA).	Using Search-Based Activation [page 10]
Added	We added information about two-factor authentication (2FA) support.	Frequently Asked Questions [page 17]
Added	We added information about session timeout settings.	Frequently Asked Questions [page 17]

2 Introduction

There are two companion documents to assist Administrators in configuring and deploying SAP SuccessFactors Mobile. Please read both documents for a complete understanding.

- SAP SuccessFactors Mobile Security Guide
- SAP SuccessFactors Mobile Deployment Guide

At the end of this Security Guide is a section that contains Frequently Asked Questions. For more information, see the SAP SuccessFactors Mobile Security Overview.

2.1 Monthly Mobile Release Cycle

The SAP SuccessFactors Mobile app has a different release cycle from the SAP SuccessFactors web application.

The SAP SuccessFactors Mobile app is released each month (except for January) and is generally available through the Apple App Store and the Google Play Store. The SAP SuccessFactors Mobile Android app, for the China market, is only available through the Tencent App Store and is the only officially sanctioned Android app store for SAP in China. No other third-party app stores, in China, are to be used to download the Android SAP SuccessFactors Mobile app. We cannot distribute iOS .ipa or Android .apk files for customers' internal distribution channels.

To ensure that all SAP SuccessFactors Mobile app users can take advantage of data protection and privacy features, and the latest security updates, features, and bug fixes, customers should ensure that employees' devices are set to automatically upgrade (or have a process to upgrade employees' devices) to the most current release of the Mobile app.

SAP SuccessFactors Mobile provides support for only the current version of the app and the two previous versions. Support for older versions may change at SAP's sole discretion at any time.

2.2 Data Protection and Privacy

To ensure that all SAP SuccessFactors Mobile app users can take advantage of data protection and privacy features, and the latest security updates, features, and bug fixes, customers should upgrade to the most current release of the Mobile app.

The SAP SuccessFactors Data Privacy Consent Statement (DPCS) is used on the SAP SuccessFactors Mobile app. Administrators can configure and manage the DPCS through the desktop application. Go to the *Admin Center* > *Tools*. Search for and select **Data Privacy Statement**. For more information and instructions, see the Setting Up and Using Data Protection and Privacy guide.

> **i Note**
>
> - Data on the SAP SuccessFactors Mobile application and the Mobile server will be deleted when a user is deactivated. If this process cannot be completed due to some unforeseen error or interruption, some data might remain on the Mobile server. However, this data is never visible on the SAP SuccessFactors Mobile application.
> - Any data that is purged using the SAP SuccessFactors web application, might not be immediately purged from the Mobile app because the app may not be launched or online at that time. As soon as the Mobile app is launched and online, the data will be purged from the SAP SuccessFactors Mobile application.

3 Passwords

There are two different passwords used in the SAP SuccessFactors Mobile application:

- Web Login Authentication Password
  Employee company credentials that are entered on the mobile device once, at the time of activation.
- SAP SuccessFactors Mobile App Password
  During the mobile device activation phase, the user must choose a Mobile app password, if the company Password Policy requires it.
  The Mobile app will prompt the user to enter the Mobile App Password when the app is launched and when the app returns to the foreground, from the background or sleep state.
  Administrators enable this password feature through the *Admin Center* > *Enable Mobile Features* > *Mobile Security* > *Mobile Password* screen and define the company-wide *Mobile Password Policy*.

SAP SuccessFactors Mobile Administrators create company-wide password policies and can choose to make Mobile app passwords mandatory for every user. When enabling this functionality, the Administrator compels the user to choose a Mobile app password during the activation process. After this setting has been switched on, users who have already activated a device will be required to create a password that meets the password requirements.

Every time the Administrator changes the Password Policy, users are required to change or update their password. For example, if the Password Policy is changed from a 4-digit numeric password to an 8-character alphanumeric password, users will be forced to update their passwords.

Biometric Technologies

The SAP SuccessFactors Mobile application supports the following device-specific biometric technologies: iOS Touch ID, iOS Face ID, and Android Fingerprint. These technologies can be used as an alternative to entering a password manually.

> **i Note**
>
> Administrators can choose to enable the biometrics authentication option, but this cannot be mandatory because the choice to use biometrics is made only by the user on their mobile device. To switch on this feature, go to *Admin Center* > *Enable Mobile Features* > *Mobile Security* > *Mobile Password* > *Enable Fingerprint Support*.

Enable Password History Policy

Enabling this policy will force users to choose a password that is different from the last five recently used passwords.

Failed Unlock Attempts

The Administrator can choose the number of attempts a user can make, before the mobile application is locked. Once the application is locked, the Mobile app is deactivated and all data is deleted from the device. To unlock the application, the user must go through the activation process again.

Password Length

The Administrator can set the minimum length of the password to a value from 4 to 255 characters. The default value is 6 digits.

Password Expiration

The Administrator can set the password expiration duration in days. The default is set to zero, which means the password will not expire. The Administrator can set the value from 0 days to 365 days.

Minimum Unique Characters in Password

The Administrator can set the minimum number of unique characters required. As the number of unique characters in a password increases, the strength of the password increases by avoiding simple (less secure) repetitive sequences. The Administrator can set the range from 0 to 4 unique characters.

4 Mobile Device Management (MDM) Support

If your company chooses to use a Mobile Device Management (MDM) solution, the SAP SuccessFactors Mobile Deployment Guide contains a section dedicated to Mobile Device Management. Please refer to it for full details and instructions. The information in that section is provided to help you deploy SAP SuccessFactors Mobile using your MDM solution of choice. Using MDM is not required to deploy SAP SuccessFactors Mobile.

Please contact your MDM provider for specific support questions in relation to deploying the Mobile app with their product.

Generic Configuration Information

SAP SuccessFactors simplifies mobile deployment by adopting the standard set by the App Configuration for Enterprise community to build native support for MDM solutions. You can read more about AppConfig at https://www.appconfig.org.

By following this standard, we leverage capabilities built natively into the application to offer MDM support.

On Android, we use MDM capabilities made available through Android for Work. For this reason, we are only able to support the Android devices that are listed here: https://www.android.com/enterprise/devices/

Certified MDM Vendors

The following MDMs have been certified and we continue to work to certify additional MDM vendors:

- VMware AirWatch (iOS and Android)
- MobileIron (iOS and Android)
- SAP Mobile Secure (iOS and Android)
- IBM MaaS360 (iOS and Android)
- Microsoft Intune (iOS and Android)

4.1 Application Distribution Using MDM

All MDM solutions provide a secure, standard way to enable secure distribution of apps, setting and profile information from the MDM console to managed devices. SAP SuccessFactors utilizes these as part of our MDM support to simplify activation and to restrict deployment only to managed devices.

In addition, some MDM providers enable additional security features with their own proprietary SDKs that software providers must integrate into the Mobile app before the app can take advantage of these features. Other providers

utilize a technology called app wrapping in which they can guarantee that the app cannot perform any actions not approved by the IT Administrator. This technology requires software providers to distribute the raw executable file (iOS .ipa or Android .apk). SAP SuccessFactors Mobile does not integrate third-party MDM SDKs and we do not support app wrapping technology as both would introduce distribution and support issues for our customers.

The SAP SuccessFactors Mobile app is distributed only through the Apple App Store and the Google Play Store. The SAP SuccessFactors Mobile Android app, for the China market, is only available through the Tencent App Store. This is the only officially sanctioned Android app store for SAP in China. Your chosen MDM system needs to support the App Catalog function to point to the vendor's default app store. We cannot distribute iOS .ipa or Android .apk files for customers' internal distribution channels.

For more information, see the SAP SuccessFactors Mobile Security Overview.

4.2 Restricting Activation on Non-Managed Devices

Context

> **i** Note
>
> Once restricted access is turned on, previous instances of SAP SuccessFactors Mobile, downloaded through the Apple App Store, are deactivated.

Restricting activation on non-managed devices ensures that only devices controlled by your MDM solution are allowed to activate the SAP SuccessFactors Mobile app.

To enable this option:

Procedure

1. Navigate to the MDM settings from the *Admin Center* > *Enable Mobile Features* > *Mobile Device Management* > *Additional MDM Functionality*.
2. Place a check in the Restrict activation on non-managed devices checkbox.

   If the device is unmanaged, the profile is immediately deleted, and an error message is displayed.

   Each time the Mobile app is launched, a comparison is performed between the Key/Value pair in the managed device and the one sent by the server. If there is a mismatch, the mobile user is deactivated.

5 Activating the Mobile Application

There are four ways to activate the SAP SuccessFactors Mobile application on mobile devices.

- Search-Based Activation
- Email-Based Activation
- MDM-Based Activation
- QR Code Activation

5.1 Using Search-Based Activation

The first time the SAP SuccessFactors Mobile application is launched, you can activate the Mobile app by entering your company name or company URL to search for a match.

Context

Multi-factor authentication (MFA) applies to mobile apps. Mobile apps inherit the full set of MFA mechanisms from the web application.

Procedure

1. The user downloads and launches the application on their mobile device.
2. A login screen is displayed where the user can enter their Company Name or Company URL.

   When a match is identified, the user will be directed to their company's login page.

   If multiple matches or results are found, please edit your search terms to be more specific and search again.
3. On your company's login page, enter your company login credentials. If successful, the Mobile App is activated.

   If the Company Name or Company URL was not identified, the user has the option to activate using the QR Code. Since a match was not discovered, please contact request Product Support to file ticket to have your company name added to the activation database.

   The SAP SuccessFactors login page cannot be accessed from the general internet, you may need to work with your Identity Provider (IdP) to adjust accessibility of the login page to the general internet. If the permission structure surrounding the login page makes it impractical to make the login page accessible to the general internet, you may want consider implementing VPN tunneling. (For example, using Mobile Device Management (MDM) software (from companies such as AirWatch and MobileIron) or other third-party tunneling software.) You can also investigate using the QR Code Activation option.

5.2 Using Email-Based Activation

Context

Procedure

1. The user receives an email with a request to activate the SAP SuccessFactors Mobile app from their mobile device.
2. The user opens the email on their mobile device and clicks the *activation link*. The application is launched on the mobile device.
3. A login screen is displayed and the user enters their **username** and **password** to activate the Mobile app. If successful, the Mobile App is activated.

> **i** Note
>
> If Single Sign-On is enabled, the mobile device will be silently activated without the user entering a username and password. See the Leveraging Single Sign-On (SSO) section for more information.

5.3 Using MDM-Based Activation

Context

Procedure

1. The user launches the SAP SuccessFactors Mobile application on their mobile device.

   The Mobile app recognizes the key/value pair pushed by the MDM solution and initiates Simple Activation instead of the normal activation process. See the SAP SuccessFactors Mobile Deployment Guide's **Simple Activation** section for information on the Key/Value pairs.
2. A login screen is displayed and the user enters their **username** and **password**. If successful, the Mobile App is activated.

> **i Note**
>
> If Single Sign-On is enabled, the mobile device will be silently activated without the user entering a username and password. See the Leveraging Single Sign-On (SSO) section for more information.

5.4 Using QR Code Activation

The first time the SAP SuccessFactors Mobile application is launched, you can activate the Mobile app by entering your company name or company URL. If a company name or URL match cannot be found, you have the option to activate by selecting the Log In with QR Code button.

To activate your SAP SuccessFactors Mobile application using the QR code, choose one of these two options:

- Company-wide QR Code Activation
- Personal QR Code Activation

5.4.1 Using a Company-wide QR Code Activation

Context

Procedure

1. Go to the SAP SuccessFactors web application login screen.
2. Click the *Activate Mobile App Using QR Code* link below the log in button on this screen.
3. Use the camera on your mobile device to scan the QR code on the screen.
4. The user enters their **`username`** and **`password`** to log in to the desktop application. If successful, the SAP SuccessFactors Mobile App is activated.

5.4.2 Using a Personal QR Code Activation

Context

Procedure

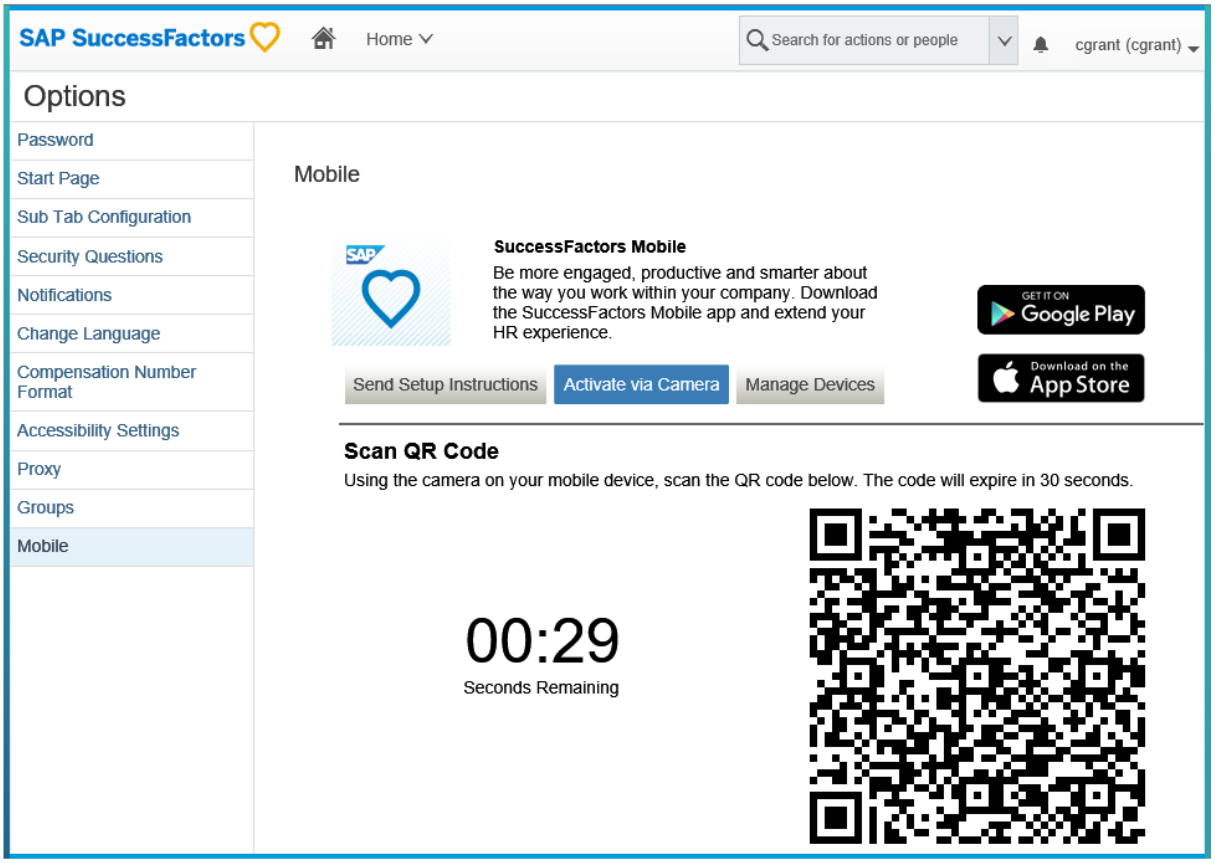
1. Go to the SAP SuccessFactors web application and log in.
2. Click the dropdown menu (in the upper right corner of the screen by your profile photo) and select *Options*.
3. In the Options screen, select *Mobile*.

   The Mobile screen offers two ways to activate your SAP SuccessFactors Mobile app:

   - On the Send Setup Instructions screen you can enter your **`email address`** and click *Send Email* to receive step-by-step instructions.
   - On the Activate via Camera screen you can scan the QR Code to activate your mobile device.
4. Click the *Activate via Camera* button.

   Use the camera on your mobile device to scan the displayed QR code. If successful, the SAP SuccessFactors Mobile App is activated.

   The QR code will expire in 30 seconds. If the QR Code expires, click the *Get New Code* button to generate a new QR Code. This QR Code is personal to you, and can only be used by you, because it was provided after you logged in to SAP SuccessFactors.



Personal QR Code Activation

6 Leveraging Single Sign-On (SSO)

Mobile Device Management (MDM) solutions have the capability of pushing digital certificates directly to mobile apps in order to enable SSO for mobile apps. However, the SAP SuccessFactors Mobile app does not use this feature.

SAP SuccessFactors Mobile customers that use SSO to access the SAP SuccessFactors web application can take advantage of that SSO service when activating their mobile devices. These customers must have browser-based SAML or SAML 2.0 SSO configured and working in their instance before they can leverage that SSO setup to also perform activations for SAP SuccessFactors Mobile app users. For more information and instructions on setting up SSO, please refer to the SAP SuccessFactors SAML2 Single Sign-On document.

The following describes the SSO-based Mobile authentication process.

- The user starts the Mobile app authentication process. (As described in the Activating the Mobile Application section.)
- If the SSO method is configured, a SAML SSO call is initiated in the default web browser on the mobile device.

  > **i Note**
  >
  > This process does not rely on MDM or any other specific Mobile app feature. It uses the pre-configured SAML SSO that users can access over a browser. On Android devices, a browser must be part of the Android for Work profile for this operation to be successful.

- The Mobile app hands over to the web browser which attempts to reach a URL (similar to: https://SF_DC/sf/mobileactivation?company=xxx&view=mobile). This URL is specific to the data center and instance for the customer. See the Simple Activation section for information on the Key/Value pairs.
  The Simple Activation section lists your two MDM Key/Value pairs:
  - SFSF_DomainName: <test.app-server-domain.com>
  - SFSF_Instance: <YourCompanyInstanceName>
- This is the beginning of what is called the Service Provider (SP) initiated login. When theSAP SuccessFactors server gets this URL and if the user is not logged in to the SAP SuccessFactors web application, the server sends a SAML Request back to the browser. The SAML Request tells the IdP (Identity Provider) that a user wants to log in to SAP SuccessFactors. The IdP is set up to receive SSO traffic from the instance.
- The IDP now authenticates the user through the customer's previously-configured authentication process.
- Once authentication is complete, the IdP sends a SAML Response back to SAP SuccessFactors in the web browser. It also sends a RelayState value with the destination of the Mobile Activation page.
- The SAP SuccessFactors server verifies the SSO and logs in the user. After login, the browser redirects to the Mobile Activation page in the SAP SuccessFactors web application, where the user completes the activation.

7 App Deactivation

Deactivation remotely removes all application-specific information (stored on the device) from the deactivated device.

This prevents future use of the application until a new activation is performed.

There are two types of deactivation for the SAP SuccessFactors Mobile application:

- Administrator Initiated Deactivation
- Automatic Deactivation

Administrator Initiated Deactivation

If a device is lost or stolen, Administrators can manually deactivate the SAP SuccessFactors Mobile application on a specific device through the *Admin Center* > *Manage Mobile Users* screen. It displays a list of names and the number of devices for each mobile user. The administrator can use the deactivate icon (garbage bin) to deactivate any device by name. Please refer to the Managing Mobile Users topic in the SAP SuccessFactors Mobile Deployment guide for details.

Automatic Deactivation

The SAP SuccessFactors Mobile application is automatically deactivated in the following situations:

- An employee leaves the company.
  As soon as a user is terminated in SAP SuccessFactors, the mobile server receives a deactivation notification. The SAP SuccessFactors Mobile application is deactivated and the user's account is deactivated.
  Data on the SAP SuccessFactors Mobile application and the Mobile server will be deleted when a user is deactivated. If this process cannot be completed due to some unforeseen error or interruption, some data might remain on the Mobile server. However, this data is never visible on the SAP SuccessFactors Mobile application.
- A user exceeds the password policy for failed unlock attempts.
  This only applies when the administrator has enabled Mobile Password and has configured the additional settings through the *Admin Center* > *Enable Mobile Features* > *Mobile Password Policy* screen.
  If the end-user exceeds the permitted number of failed unlock attempts, the SAP SuccessFactors Mobile application is deactivated.
- If the end-user's password is expired, the SAP SuccessFactors Mobile application is deactivated.

8 Frequently Asked Questions

Privacy and Permissions

Is sensitive information captured in log files?

Sensitive information is not revealed in debugging messages, log files, environment variables, or thread or core dumps.

Is information shared with third-parties?

We do not allow third-parties to create mobile applications for our platform. We do not share any information with any third-parties.

Does the Mobile app require access to features, such as Calendar or Camera?

To improve the user experience and to enable some features, the Mobile app gives the user an option to grant permission to access the following features:

- Camera—for scanning a QR Code and for replacing your Profile photo
- Contacts—for saving contact information to your Contacts
- Photo Library—for replacing your Profile photo

How are access permissions and privileges granted to the user?

The Mobile app uses the same Role-Based Permissions infrastructure that is defined for the user in the SAP SuccessFactors web application. Permissions are checked when the Mobile app is started and when each feature is accessed.

Data Storage

What is stored on-device?

What is stored on the mobile device depends on whether the *On-device Secure Storage* checkbox is checked or not. This checkbox is found at: *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Security* > *On-device Secure Storage*.

What is stored on the mobile device when the On-device Secure Storage checkbox is unchecked?

The On-device Secure Storage is always used to secure sensitive information. This checkbox is checked (or enabled) by default, so that on-device secure storage (persistent caching) is enabled. All on-device data is stored and encrypted. Administrators can opt to uncheck (or disable) this feature. However, SAP SuccessFactors recommend that Administrators do **not** uncheck this checkbox, unless your security requirements dictate otherwise, because it may affect the Mobile app performance.

When the checkbox is unchecked (or disabled), some data is still stored using On-device Secure Storage, but we limit the stored information to only the following essential items listed here. All on-device data is stored and encrypted.

The stored items include the user's:

- Name
- Photo
- Job title
- Email
- Hire date
- Language
- OAuth authentication tokens
- Learning content for offline purposes
- SAP SuccessFactors Logon Company ID
- SAP SuccessFactors Logon Username

What is stored on the mobile device when the On-device Secure Storage checkbox is checked?

The On-device Secure Storage is always used to secure sensitive information. This checkbox is checked (or enabled) by default, so that on-device secure storage (persistent caching) is enabled. All on-device data is stored and encrypted. Persistent caching provides an additional benefit because it improves the performance of the Mobile app.

Security

What types of encryption are used for secure communication?

All remote connections are performed over Transport Layer Security TLS 1.2.

The Apple App Transport Security (ATS) is enforced for communication on iOS devices and the connection must satisfy the ATS requirements. For complete requirements, see the Requirements for Connecting Using ATS section at the Apple Developer website.

If your server does not meet these standards, you may encounter an error message, such as: "Your server's security level is insufficient for creating a secure connection to the app. Please contact your IT Admin.".

To test your secure connection, you may want to use a public SSL testing service, for example: https://www.ssllabs.com/ssltest/. Check the handshake simulation results for Apple ATS.

What is the on-device secure storage memory encryption process?

The **On-device Secure Storage** encryption process uses the user's Mobile app password to protect the data. When the Mobile app is accessed, the user must enter a password to unlock the SAP SuccessFactors persistent storage and gain access to the app.

When the Mobile app goes into the background, the SAP SuccessFactors persistent storage is locked and the encryption key is released. To reopen the persistent storage (when the app is returned to the foreground), the user must re-enter their Mobile app password.

The Mobile app uses an additional OS-specific protection so that the app and data are unavailable when the mobile device is locked. For example, iOS uses the **protectionComplete** attribute to accomplish this protection.

Are credentials stored in the Mobile app?

User credentials are not stored in the SAP SuccessFactors Mobile app or on the mobile device. Authentication always occurs in the SAP SuccessFactors web application and respects your SAP SuccessFactors deployment security and restriction settings.

The Mobile app only requests the user to enter credentials (in the app) during the initial (activation) log in. The user is not asked to enter their credentials at any other time. This avoids phishing and other security risks.

How is stored data protected on the mobile device?

The SAP SuccessFactors Mobile app protects data stored on-device using a two-layer approach. The app uses the available protection mechanisms offered by the mobile operating system inside the application's sandbox environment. The data is also protected by application-level encryption based on 128-bit Advanced Encryption Standard (AES) method.

Are security tests and code scanning performed?

The SAP SuccessFactors Mobile team performs penetration testing and threat modeling for the Mobile app. Both sets of tests undergo internal audits by the SAP Security team. Every quarter this information is available on request. Also, Fortify is used (for both iOS and Android) to perform source code scanning.

What policies can be set for the Mobile app password?

The Administrator can set the password policy using the SAP SuccessFactors *Admin Center* > *Enable Mobile Features* screen. For more information, see the Passwords section or the SAP SuccessFactors Mobile Deployment Guide.

Is data stored on the mobile device? Is it encrypted?

Data is cached to improve application performance. Data is encrypted using the 128-bit AES method.

Can I use OS-specific security to unlock the application?

We support certain OS-specific device technologies that provide adequate protection for the app data as a substitution for the application password, including: Apple Touch ID, Apple Face ID, and Android Fingerprint. We currently do not support Android screen patterns for unlocking the app, because it does not provide a sufficient level of security.

Are passwords hashed and stored on the mobile device?

The SAP SuccessFactors Mobile app passwords are not stored on the mobile device. Passwords are hashed and salted.

Why is the SAP SuccessFactors Mobile app reporting that my device is jailbroken or rooted?

The SAP SuccessFactors Mobile app looks for suspicious software that is typically used to gain administrator-level access to the mobile device operating system. The Mobile app will detect any jailbroken (iOS) or rooted (Android) mobile devices and close the SAP SuccessFactors Mobile app immediately, after alerting the user. Some Android device manufacturers include software that is typically used to gain root access to the device, as part of their ROM image. If the SAP SuccessFactors Mobile app detects this suspicious software, the user will not be able to activate the Mobile app on that device.

Authentication

How are the OAuth tokens stored?

OAuth Access and Refresh tokens are stored in the SAP SuccessFactors Mobile persistent storage and is encrypted using the 128-bit AES method.

What is the lifetime of OAuth tokens?

The OAuth Access token expires after every 24 hour period and attempts to renew automatically.

The OAuth Refresh token is renewed based on the Reauthentication Duration setting configured through the *Admin Center* > *Enable Mobile Features* > *Require Reauthentication* screen. It is used to keep the user active on the app. When the refresh token expires, the user must enter their SAP SuccessFactors username and password to reauthenticate.

The Access Token and Refresh Token are two different tokens. The Access token is used for authentication and the Refresh token is used to maintain access for the app user.

Can I use an RSA token for Mobile authentication?

RSA is not an available option.

Is two-factor authentication (2FA) supported?

From 2008 mobile release (August 2020), we support 2FA on both iOS and Android once it is enabled on the SSO.

After activation and authorization, are OAuth tokens stored on the mobile device?

Yes. Once the Mobile app is activated and authorized, the SAP SuccessFactors server grants OAuth access and refresh tokens and pushes the tokens to the Mobile app. The tokens are stored in on-device persistent storage and encrypted according to the 128-bit AES method.

How is the authorization token stored and secured on both iOS and Android devices?

After authentication is complete, OAuth Access and Refresh tokens, which register a user's mobile device as activated, are stored and secured in the SAP SuccessFactors Mobile on-device secure storage. This storage is encrypted according to the 128-bit AES method. The encryption key to the storage is derived from the user's password for the Mobile app. When the Mobile app goes into the background, the encryption key is released, making the stored data inaccessible.

The complexity of the (user-level) Mobile app password is configured by your Administrator. The password is temporarily held in memory in the form of a hash, in the Mobile app, until it becomes part of the encryption key.

Device Management and Limitations

What is the maximum number of devices that can be enrolled?

The limit may be specified by the MDM software, but is unlimited by default.

Does the Mobile app have inactivity timeout settings?

Yes. You can configure how long the app can be idle before the session times out, using the *Mobile App Session Timeout* setting. To do that, go to *Admin Center* > *Enable Mobile Features* > *Mobile App Password* and select *Mobile App Session Timeout*. Then choose from the available expiration times.

Which MDMs are supported?

Please see the Certified MDM Vendors section for a list of supported MDM providers.

Can I prevent the mobile device from taking screenshots?

The SAP SuccessFactors Mobile app can't prevent screenshots from being taken because this functionality is device-specific. However, a security policy can be distributed to the Mobile app and may be supported by some MDM providers. Contact your MDM provider for details.

Can I use multiple MDM systems?

SAP SuccessFactors Mobile can be configured, using the *Admin Center* > *Enable Mobile Features* screen, for use with only one MDM system. If customers have multiple instances, each instance can be configured to use different MDM systems.

Distribution

Does SAP SuccessFactors certify delivery of the Mobile app through Citrix XenMobile?

For a variety of practical and security-related reasons, MDM providers that require integration with their custom SDK (for example, Citrix, Good Technology, and Blackberry) are not supported. For more information, see the Master Device Management section.

Connectivity

How can I limit the IP addresses that are accessing my SAP SuccessFactors system?

The Mobile app does not require a VPN connection. If your IT Department requires a limitation, you should investigate using MDM VPN tunneling. The customer must require that VPN software is installed and used on their mobile devices each time the SAP SuccessFactors Mobile app is accessed.

If your SAP SuccessFactors login URL cannot be accessed via the general internet, you can try one of the following possible solutions:

1. The customer should make their Identity Provider site accessible to the general internet.
2. The customer should investigate using MDM VPN tunneling.
3. The customer must require that VPN software is installed and used on their mobile devices each time the SAP SuccessFactors Mobile app is accessed.

If these options are not possible, using QR Code Activation is still an option.

Options 2 and 3 are essentially the same but are two different approaches. MDM tunneling is a software configuration of Mobile Device Management (MDM) software (from companies such as AirWatch and MobileIron)

that will push the configuration and force the use of a VPN anytime the SAP SuccessFactors Mobile app is accessed. Option 3 is the same but is an option if your IT Department chooses not to use MDM software.

All three solutions require assistance from your company's IT Department and are outside the realm of what Product Support can do to support the customer.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP