SAP SuccessFactors

PUBLIC

Document Version: April 2023 – 2025-07-01

Mobile Deployment Guide

THE BEST RUN SAP

Content

1 SAP SuccessFactors Mobile Deployment

SAP SuccessFactors Mobile currently supports the most popular mobile platforms in the market, iOS and Android.

We have experienced firsthand how mobility can change the productivity of an entire workforce. SAP SuccessFactors customers all over the world are taking advantage of the SAP SuccessFactors Mobile app. In a multi-device, multi-screen world we think about the Mobile app not just as a way to expand access to your most critical HR systems but also as an opportunity to enable people to work differently.

We are so confident about the transformative power mobile HR can have in your organization that we want to make it easy for customers like you to try, experiment, and see it for yourself. We have put together this Deployment Guide to help you successfully roll out our SAP SuccessFactors Mobile app to your workforce.

This document provides administrators with step-by-step instructions for the deployment of SAP SuccessFactors Mobile.

For details on device requirements, see IT Landscape Requirements for SAP SuccessFactors. Note: The **Mobile Application Support for SAP SuccessFactors** section contains information about supported devices.

1.1 Monthly Mobile Release Cycle

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

Except in January, April, and October, the SAP SuccessFactors Mobile app is released every month and 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 approved Android app store for SAP in China. Do not go to other third-party app stores in China 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.

1.2 Data Protection and Privacy

To ensure that all SAP SuccessFactors Mobile 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.

> ⓘ 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.
> - For the iOS SAP SuccessFactors Mobile app downloaded from Apple App Store for mainland China market and the Android SAP SuccessFactors Mobile app downloaded from Tencent App Store, a privacy statement, that is to comply with the latest China Cyber Security Law requirement, is prompted when users use the mobile app for the first time or with a version upgrade, regardless of their organization's DPCS settings. Users will need to read through and agree to the statement to proceed with mobile access.

1.3 Setting Up SAP SuccessFactors Mobile

Deploy and manage SAP SuccessFactors Mobile for your organization.

Procedure

1. Go to *Admin Center* > *Mobile Settings*.
2. Switch between the *Enable Mobile Features* and *Manage Mobile Users* tabs to set up mobile policies for your organization as desired.

2 Enabling Mobile Features

Configure Mobile App features, for all authorized mobile users and mobile devices.

Prerequisites

You have the following role-based permissions:

- *Administrator* > *Manage System Properties* > *Mobile Settings*
- *Administrator* > *Manage System Properties* > *Mobile Device Deactivation*

Context

Use the *Enable Mobile Features* screen to configure all features available on the SAP SuccessFactors Mobile app for iOS and Android. It includes mobile-specific features, such as the Mobile App Password Policy, Mobile Device Management, and On-Device Support, as well as settings to enable SAP SuccessFactors module features on mobile, email notification settings, and mobile themes settings.

Procedure

1. Go to *Admin Center* > *Enable Mobile Features*.
2. Choose the *Enable Mobile Features* tab.

   You see the following tabs:
   - Mobile Specific
   - Modules
   - Email Notifications
   - Mobile Themes
3. To turn a feature on or off, for all authorized mobile users, select or deselect the relevant checkbox.

   > ⚠ Caution
   >
   > If you see a ⚙ (Settings) icon appears next to the feature, selecting the checkbox **isn't** sufficient to turn it on. Be sure to configure the additional settings for that feature.
4. To configuration additional settings for a feature, choose the ⚙ (Settings) icon next to the feature name and follow onscreen instructions.
5. Choose *Save*.

2.1 Require Reauthentication in the Mobile App

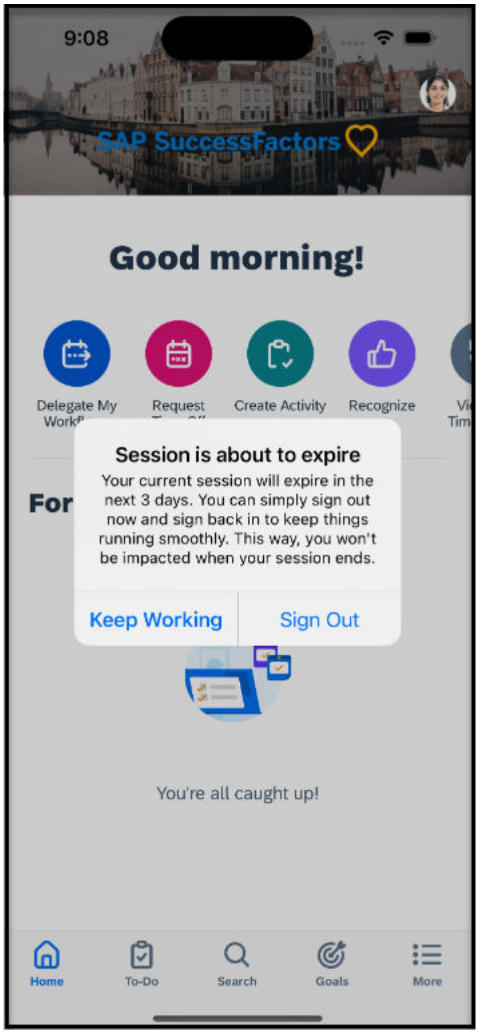
Learn about and update the duration period for the *Require Reauthentication* setting in the Mobile app.

Context

The *Require Reauthentication* feature requires users to reauthenticate their Mobile Profile periodically. As of the 1H 2024 release, this setting is enabled by default with a duration period of 180 days, however the time interval before the session expires and reauthentication is required can be adjusted by the administrator.

How Does the Session Expiration and Sign-In Process Work?

- Users are notified within 7 days of their session expiring, so that they can proactively reauthenticate before that time.
- The notification message appears when users open their profile in the mobile app.



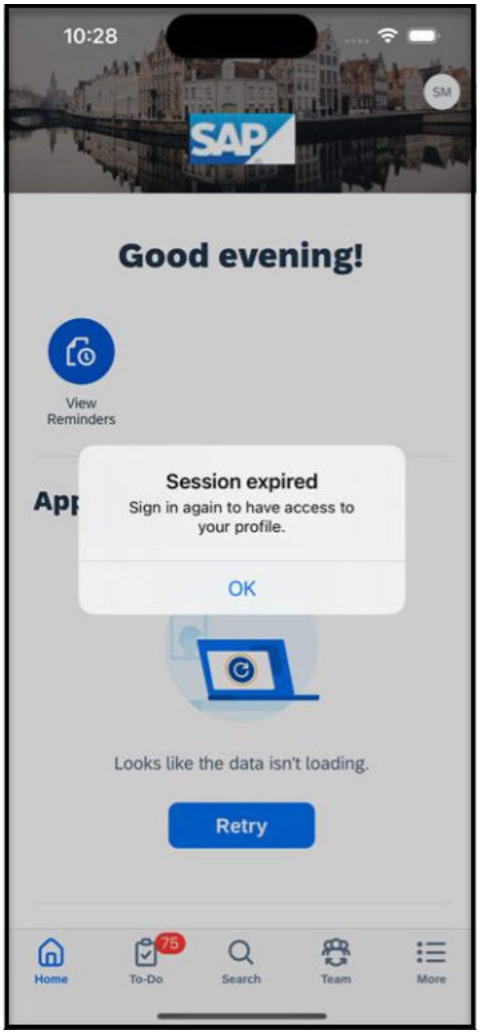
Session is about to expire

Your current session will expire in the next 3 days. You can simply sign out now and sign back in to keep things running smoothly. This way, you won't be impacted when your session ends.

You're all caught up!

- If the reauthentication duration period is less than 7 days, this notification is not displayed.

- If the user doesn't sign out within the specified time period, they are signed out automatically and see a message asking them to sign in again.



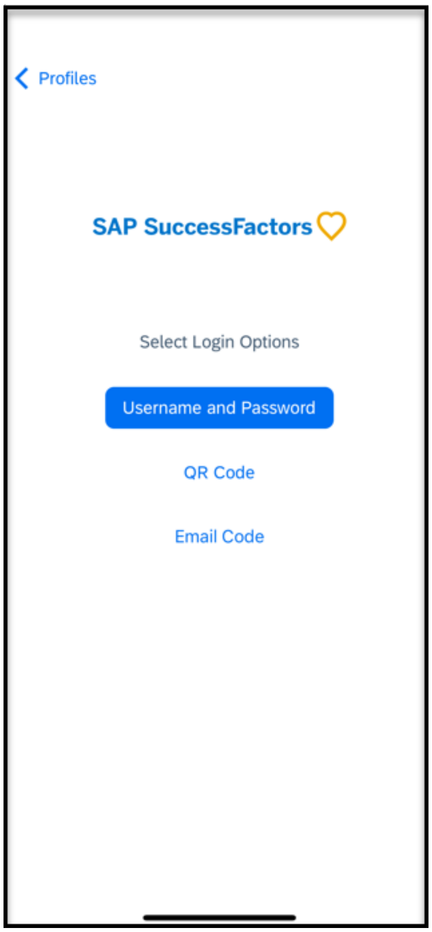
Good evening!

Session expired

Sign in again to have access to your profile.

Looks like the data isn't loading.

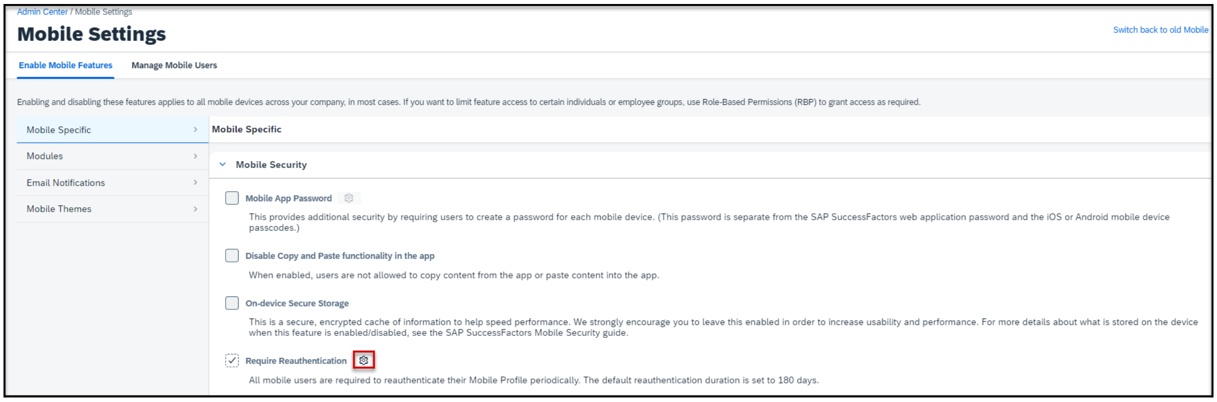
- When the user is signed out, whether due to this automatic process or by manually signing out themselves, they must sign in again to use the app.
- Signed out users do not need to activate the app (connect the app with their company or instance) again; that connection remains intact. They only need to authenticate again using one of the methods available on the *Select Login Options* screen.



For more information on the login methods available, refer to **Logging Into the Mobile App** in the **Related Information**section.

Procedure

1. Navigate to the *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Require Reauthentication* setting.
2. Click the gear icon next to this setting .



Enabling and disabling these features applies to all mobile devices across your company, in most cases. If you want to limit feature access to certain individuals or employee groups, use Role-Based Permissions (RBP) to grant access as required.

□ Mobile App Password

This provides additional security by requiring users to create a password for each mobile device. (This password is separate from the SAP SuccessFactors web application password and the iOS or Android mobile device passcodes.)

□ Disable Copy and Paste functionality in the app

When enabled, users are not allowed to copy content from the app or paste content into the app.

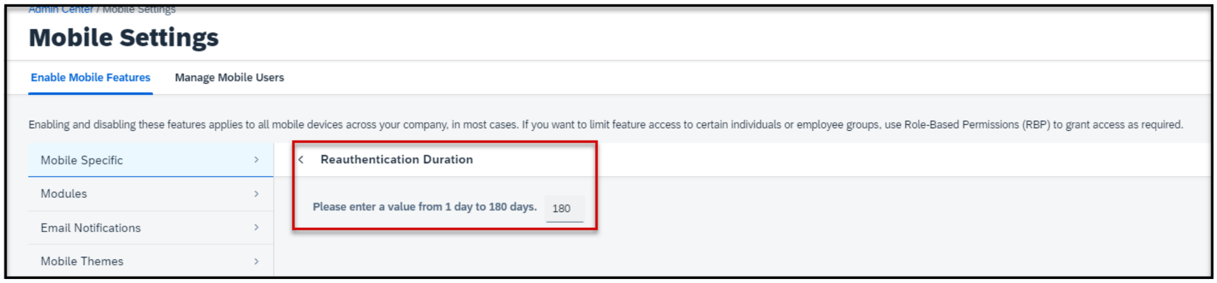
□ On-device Secure Storage

This is a secure, encrypted cache of information to help speed performance. We strongly encourage you to leave this enabled in order to increase usability and performance. For more details about what is stored on the device when this feature is enabled/disabled, see the SAP SuccessFactors Mobile Security guide.

☑ Require Reauthentication

All mobile users are required to reauthenticate their Mobile Profile periodically. The default reauthentication duration is set to 180 days.

3. On the *Reauthentication Duration* screen, update the number of days after which you'd like reauthentication to be required.



Admin Center / Mobile Settings

Mobile Settings

Enabling and disabling these features applies to all mobile devices across your company, in most cases. If you want to limit feature access to certain individuals or employee groups, use Role-Based Permissions (RBP) to grant access as required.

Reauthentication Duration

Please enter a value from 1 day to 180 days. 180

4. Click *Save*.

> ⓘ Note
>
> If you are using an iOS device and are unable to sign back in after being signed out, refer to KBA 3470014 for assistance.

3 Granting Permission Roles

You can grant various permissions to users for using the SAP SuccessFactors Mobile app.

The following sections describe permissions required for using the mobile apps.

Granting Mobile Access to Users

To allow all users or targeted user groups to access the mobile app, ensure they have *User Permissions* > *General User Permission* > *Mobile Access* permission.

Enabling Users to Search for Employees

The Mobile app search feature allows employees to search for colleagues across their organization. If the search function does not produce any results, then it is necessary to verify that certain role-based permissions are configured to allow users to view the first name, last name, and status. Administrators must grant specific View permissions their users.

Ensure that all users have view permission to the First Name, Last Name, and Status fields under *User Permissions* > *Employee Data*.

3.1 Enabling Managers to Access Team Tab

Use Role-Based Permissions (RBP) to enable managers to manage their teams through the SAP SuccessFactors Mobile app.

Context

Grant appropriate permissions to managers so that they can see the *Team* tab in the app (iOS: on the tab bar; Android: on the navigation menu). In the *Team* view, they can review or change information for their reports.

Procedure

1. Go to *Admin Center* › *Manage Permission Roles*.
2. In the page, select the role assigned to the intended managers and add the permissions it should have. If the existing roles don't meet your needs, create a new one.
3. Make sure the permissions below are selected correctly.
    - Permissions under *User Permissions* › *Employee Data* to *View* and *Edit*: *# of Team Members*, *Status*, *First Name*, *Last Name*, and *Manager*

        > ⓘ Note
        >
        > If you can't find *# of Team Members* and *Status* in the list, you should first go to *Admin Center* › *Manage Business Configurations* › *Employee Profile* › *Standard*, and enable the *teamMembersSize* and *status* fields. You can also contact your implementation partner to enable the fields through Provisioning.

    - Permissions under *User Permissions* › *General User Permission*: *Mobile Access*, *Organization Chart Navigation Permission*, *Company Info Access*, and *User Search*
    - *User Permissions* › *Succession Planners* › *Succession Org Chart Permission* (This permission is a must, if your instance is using the legacy org chart and the *Limit org chart access to succession org chart users* option is enabled in Provisioning.)

        > → Remember
        >
        > As a customer, you don't have access to Provisioning. To complete tasks in Provisioning, contact your implementation partner or Account Executive. For any non-implementation tasks, contact Technical Support.

4. Define the target population of this role. Make sure not to select the option *Exclude granted users from having the same access to themselves*, because managers themselves should also be included in the target population.
5. Save your changes.

Results

Managers can see the *Team* tab in the app.

4 Enabling Mobile Access for Proxy Users

The proxy feature allows one person to access another person's user account and act on their behalf, for a specific purpose and in specified areas of the system. With proper configuration, users who proxy as another person in the web application can also access the other person’s account on a mobile device.

Prerequisites

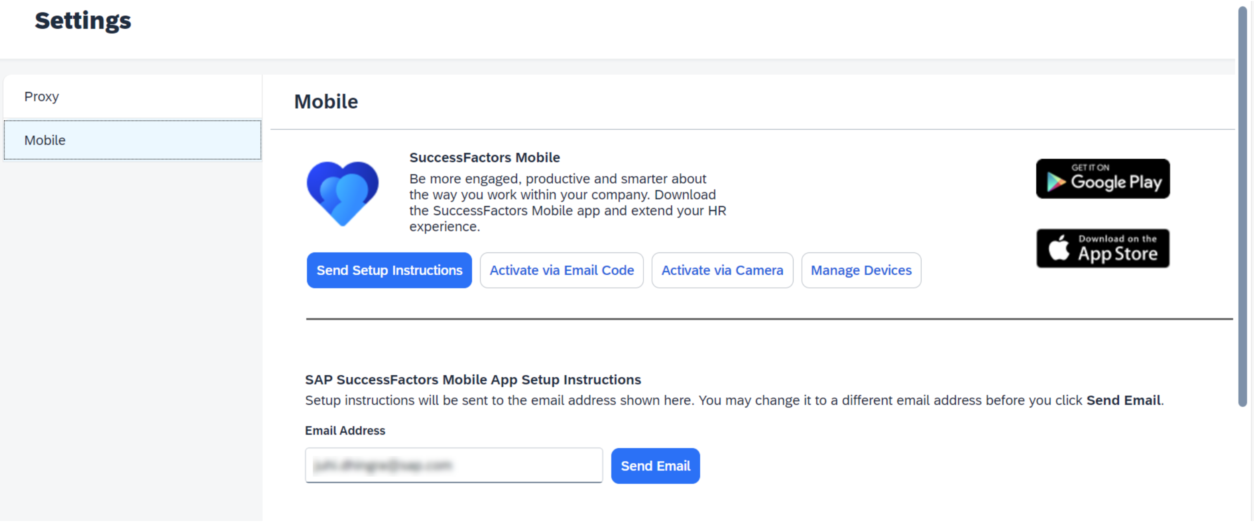
You have ▶ *Administrator Permissions* › *Manager User* › *Proxy Management* › permission.

Procedure

1. Go to ▶ *Admin Center* › *Proxy Management* ›.
2. In the *Make Assignments* section, specify the following:
   - Who will act as the proxy (username): Enter the username value of the user that will be allowed to proxy.
   - What account holder will the proxy act on behalf of (username): Enter the username value of the user that will be allowed to proxy as. You can use the auto complete values provided or click on “Find user” to locate the desired target user.
   - Grant Proxy Rights: Select the modules that you wish this proxy to have access to once proxying as the account holder. Select the option "Options (Mobile)" to allow the proxy to access the Mobile activation page under the Settings menu item.
3. **Optional:** Set a time range during which the proxy assignment is allowed.
4. Save your changes.

Results

With the proxy configuration saved and active, when the user proxies as the specified account holder, they’ll see the following page under the *Settings* menu item. They can choose Mobile to obtain mobile access to the account holder.



SuccessFactors Mobile

Be more engaged, productive and smarter about the way you work within your company. Download the SuccessFactors Mobile app and extend your HR experience.

SAP SuccessFactors Mobile App Setup Instructions

Setup instructions will be sent to the email address shown here. You may change it to a different email address before you click **Send Email**.

Email Address

[redacted]

Mobile Activation Page for Proxy User

> ⓘ Note
>
> After this feature is enabled, when user A proxies as user B and goes to the Mobile activation page in the web application, the QR code shown for activation via camera refers to user B. When user A switches back to be themselves and goes to the Mobile activation page again, the reference will still be pointing to user B. User A must completely log out after having proxied as someone else to allow the reference to be reset.

5 Enabling the Mobile App for Multiple Profiles

Enable multiple profiles so that multiple people can use the SAP SuccessFactors Mobile app on a shared device.

Context

The *Multiple Profiles* feature enables multiple people, such as deskless workers, to use the Mobile app on a shared device. Each profile in the Mobile app corresponds with a user account in the **same** SAP SuccessFactors system. For privacy and security, mobile passwords are required for all profiles and notifications and caching are disabled.

> ⓘ Note
>
> As of February 2025, you can no longer use *Multiple Profiles* to switch between a "production" system and a "test" system. To connect to test system, you need to deactivate and reactivate the app or use a different device.

Procedure

1. Launch the SAP SuccessFactors Mobile app and go to ▶ *More* ▶ *Settings* ▶. (For Android, tap the ☰ *menu* icon, then *Settings*.)
2. Enable the *Multiple Profiles* setting.
   A mobile password is required. If you don't have one yet, you're asked to create one.

Results

You can now add multiple profiles in the app. Other people who use the same company system can now add their own profiles on the *Profiles* launch screen.

> ⓘ Note
>
> - A mobile password is required for every profile.
> - Notifications and caching are disabled.
> - As the first user, you're designated as the "owner" of the device on the *Profiles* launch screen.

Next Steps

Next time you launch the app, you see the *Profiles* screen first. Enter your mobile password to continue or ask other users of the device to create their own profiles.

As the device owner, you can manage user profiles at ▶ *More* ▶ *Settings* ▶ *Manage Profiles* ◀.

6 Enabling Email Notification Templates

Context

This feature enables you to customize an email template used to send a single email notification to all users that have been granted *Mobile Access* through Role-Based Permsisions.

> ⓘ Note
>
> Use the Mobile Email Notification feature to simplify mobile user activation and encourage Mobile adoption.

Users receive an email that contains two links that provide the following options:

- Download and install the SAP SuccessFactors Mobile app from the corresponding app store. The app automatically redirects you based on the mobile operating system detected.
- Activate the Mobile app from the device. This process leverages the standard SAP SuccessFactors web application login process.
  Once this email notification feature is activated, any current and future users granted mobile access receive this one-time email notification. Also, individual users can send the setup instructions email notification from the *[Avatar Image]* > *Settings* > *Mobile* > *SAP SuccessFactors Mobile App Setup Instructions* section and click *Send Email*.

To enable this Mobile Email Notification:

Procedure

1. Navigate to Admin Tools and click *Mobile* and select *Email Notification Templates Settings* to open this screen.
2. In the E-Mail Notification Templates list, click the *Mobile Activation Notification with QR code* link. The template is displayed at the bottom of the page.
3. Modify the *Mobile Activation Notification with QR code* displayed email template.
4. At the bottom of the template section, click *Save Changes*.
5. At the bottom of the screen, click *Save Notification Settings*.

7 Enabling Mobile Policy Notifications

Configure a periodic message to display on iOS and Android apps.

Prerequisites

- The setting ▶ *Admin Center* ▸ *Mobile* ▸ *Mobile Features* ◀ is enabled.
- The setting ▶ *Admin Center* ▸ *Mobile* ▸ *Mobile Features* ▸ *Mobile Specific* ▸ *Enable Mobile Policy Notifications* ◀ is enabled.
- In Permissions Settings, you have created a target group of individuals or group of employees who **won't** receive the mobile policy notifications.
- The setting ▶ *Admin Center* ▸ *Permission Role Detail* ▸ *Permission Settings* ▸ *Manage User* ▸ *Avoid Notifications about Mobile Usage Company Policy* ◀ is enabled.
- Grant permission to the target group to avoid them getting the notifications.

Procedure

1. Go to ▶ *Admin Center* ▸ *Mobile* ▸ *Mobile Features* ▸ *Mobile Specific* ▸ *Enable Mobile Policy Notifications* ◀.
2. Select the settings icon to go to the *Enable Mobile Policy Notifications* feature settings.
3. Create an English version of your policy message and fill out all available fields.

Field	Description
Language	You can add as many languages as your company requires. Before moving on to adding or editing other languages, please save your changes in each language first.
Frequency	Frequency can be set to monthly, quarterly, or annually. This setting determines the length of time employees need to acknowledge the company's policy. Once the frequency is set and the Hourly Worker Policy is completed and saved, then employees receive the notification the day the policy was saved and at the frequency set for the policy. For example, if the administrator saved the hourly worker policy as monthly, then the employee will see the policy that day when opening their SAP SuccessFactors Mobile application and one month after the date the administrator saved the policy.
Title	Title your policy message.

Field	Description
Description	Add your policy message. Note that messages are limited to a 1,000 characters.

4. Save the message.

> ⓘ Note
>
> Every time you change your policy message, please save your changes before you add or change the policy message in other languages. Otherwise, you lose changes made in your current language.

5. If needed, create a mobile policy notification in additional languages by selecting *Add Language*, and then selecting a language.
6. Fill out all available fields in the new language.
7. Save your changes.

8 Viewing Mobile Adoption

Context

To download a list of Mobile users and the number of devices each user has activated:

Procedure

1. Navigate to the ▶ *Mobile Settings* ▶ *Manage Mobile Users* ▶ screen.

   The Manage Mobile Users administration screen displays all the users that have activated at least one mobile device. This list also shows how many devices have been activated for each user.
2. Click the *Export All Mobile Users* button.

   The export will allow you to download the list of Mobile users in your company. This gives you insight into which of your employees have downloaded the Mobile app and the number of devices they have activated.

9 Managing Mobile Users

You can view information about SAP SuccessFactors Mobile app users, export a mobile user report or deactivate a device for specific users.

Procedure

1. Go to *Admin Center* > *Mobile Settings* > *Manage Mobile Users*.

   A *Mobile Users* list is displayed, showing *Name*, *User Name*, and *# of Devices* (number of devices) for each user.
2. Specify items to be displayed per page or jump to a certain page of the list.
3. Choose *Export All Mobile Users*.

   A report in the .csv format is generated.
4. Use the *Search for people* field to search for a specific mobile user.

   The *Devices* list shows all activated devices for the user.
5. In a user's device list, choose the garbage bin icon at the right side of a device row to deactivate the device.

   This action:

   - Deactivates and remotely removes the application from the specified device.
   - Prevents future use of the application on the device until a new activation is performed.
   - Removes all application-specific information stored on the device.

10 Configuring the Mobile Password Policy

Configure the SAP SuccessFactors Mobile password policy and settings.

Context

As an administrator, you can choose whether to require a mobile password for every user of the SAP SuccessFactors Mobile app, the password requirements, and whether biometric identification is allowed.

The mobile password is different from the SAP SuccessFactors login password that's for authentication throughout the system. The SAP SuccessFactors login password is only used once in the mobile app, during activation. The mobile password is required every time the app is launched, or when it returns to the foreground or from a sleep state.

When the *Mobile App Password* option is enabled, all users of the SAP SuccessFactors Mobile app are required to create a mobile password during the activation process. Users who have already activated a device are required to create a mobile password the next time they use the app. Anytime you change the SAP SuccessFactors Mobile password settings, users are required to change or update their password accordingly. For example, if password requirements are changed from a 4-digit numeric password to an 8-character alphanumeric password, users are required to update their passwords the next time they use the app.

> ⓘ Note
>
> The SAP SuccessFactors Mobile app supports device-specific biometric technologies (such as iOS Touch ID, iOS Face ID, and Android Fingerprint) as an alternative to entering your password manually. However, if the *Multiple Profiles* feature is enabled on a shared device, only the device owner (first profile added) can authenticate with biometric technologies. Other profiles have to enter their mobile password manually.

Procedure

1. Go to *Admin Center* › *Enable Mobile Features* › *Mobile Specific*.
2. Select the *Mobile App Password* setting to require all users to create a mobile password.
3. Choose ⚙ (Settings) to configure the password policy settings.

   The Mobile App Password Policy screen is displayed.
4. Select and configure one or more of the following features, following onscreen instructions.
   - *Enable Biometric Support*
   - *Enable Password History Policy*
   - *Mobile App Session Timeout*
   - *Enable Quick Profile Switching on Shared Devices*

Related Information

Passwords

11 Configuring Mobile Device Management (MDM) Applications

A Mobile Device Management (MDM) application is a third-party solution that securely manages mobile devices in the enterprise and supports both corporate-supplied and Bring Your Own Device (BYOD) mobile deployment strategies. The SAP SuccessFactors HCM suite integrates with these solutions to ensure secure deployment and activation of the SAP SuccessFactors Mobile app.

To deliver native support for MDM, SAP SuccessFactors follows standards set by the AppConfig Community, a community of industry leading Device Management solution providers and app developers.

The following MDM vendors have been certified for iOS and Android:

- VMware Workspace ONE
- MobileIron
- SAP Mobile Secure
- IBM MaaS360
- Microsoft Intune

We continue to work to certify additional MDM vendors.

> ⓘ Note
>
> Be sure that your chosen MDM solution supports the App Catalog function to point to the vendor’s default app store. The SAP SuccessFactors Mobile app is distributed only through the Apple App Store and the Google Play Store or, for the China market, through the Tencent App Store, the only officially sanctioned Android app store for SAP in China. We cannot distribute iOS .ipa or Android .apk files for other distribution channels.
>
> For more information, refer to the Mobile Security Guide.

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

11.1 Enabling Simple Activation

Enable simple activation by adding information about your SAP SuccessFactors system to your MDM solution, so that it can be transmitted automatically to managed devices during activation.

Context

With simple activation, your MDM solution identifies the company instance, so that mobile users don't have to. Domain and instance information is transmitted automatically from your MDM solution to managed devices.

During activation, mobile users don't need to provide this information, using a Company ID or QR code. Instead, they only need to provide their username and password (either by manual entry or through SSO, if configured).

Procedure

1. In the SAP SuccessFactors web application, go to *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile Device Management* > *Enable Simple Activation*.

   You can see two key-value pairs listed.

   MDM Key/Value Pairs:

Key	Value
SFSF_DomainName	This key is the domain where your system is located. Example: `<app-server-domain.com>`
SFSF_Instance	This key is the Company ID of your system. Example: `<YourCompanyInstanceName>`

2. Copy both key-value pairs and add them to your MDM system as an **App-Managed Configuration**.
3. Check your MDM solution to ensure that these key-value pairs have been successfully pushed to all mobile devices. Verify that the pushed values **don't have any leading or trailing spaces**.

Results

When the SAP SuccessFactors Mobile app starts the activation flow on a managed device, it recognizes the values set by your MDM solution and initiates simple activation, only requiring the user to input their username and password.

11.2 Restricting Activation on Managed Devices

Restrict activation to **only** managed devices.

Context

Restricting activation on non-managed devices ensures that **only** devices controlled by your MDM solution are allowed to activate the SAP SuccessFactors Mobile app and log in with a username and password.

ⓘ Note

You can only restrict activation on managed devices for users who log in with a username and password. Mobile users can still **activate and log in to the Mobile app on non-managed devices using a QR code** found at *Settings* > *Mobile* > *Activate via Camera*.

⚠ Caution

When activation is restricted to managed devices, the mobile profile is immediately deleted on non-managed devices and an error message is displayed. Previous instances of the SAP SuccessFactors Mobile app, downloaded through from an app store, are deactivated.

Procedure

1. In the SAP SuccessFactors web application, go to *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile Device Management*.
2. Copy down the following key-value pairs, so that you can add them to your MDM solution.

   In the *Enable Simple Activation* section:

Key	Description
SFSF_DomainName	This key is the domain where your system is located. Example: `<app-server-domain.com>`
SFSF_Instance	This key is the Company ID of your system. Example: `<YourCompanyInstanceName>`

   In the *Enable Managed Device Features* section, at the bottom:

Key	Description
SuccessFactors	This key is a randomly generated, unique identifier. When the SAP SuccessFactors Mobile app is launched, it searches for the *SuccessFactors* value pushed from your MDM solution. If it's not found, the device is considered **non-managed**. You can regenerate a new value at any time. Example: `<1234abcd-1234-abcd-1234-1234abcd1234>`

3. Add all three key-value pairs to your MDM system as an **App-Managed Configuration**.
4. Check your MDM solution to ensure that these keys and values have been successfully pushed to all mobile devices. Verify that the pushed values **don't have any leading or trailing spaces**.

> ⓘ Note
>
> Once the SAP SuccessFactors application has been pushed to your mobile device and the key has been copied, we recommend that you check with your MDM provider to estimate how long it may take for the propagation of the key-value pair.

5. In the SAP SuccessFactors web application, go to *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile Device Management* > *Enable Managed Device Features*.
6. Select *Restrict activation to managed devices*.

   You're asked to confirm.
7. To confirm, choose *Turn ON*, then *OK*.

Results

On non-managed devices, the profile is immediately deleted and an error message is displayed.

On managed devices, each time the Mobile app is launched, it compares the key-value pair in the managed device with the one sent by the server. If there's a mismatch, the Mobile app is deactivated.

11.3 Restrict Non-Managed Devices from Mobile Device Management

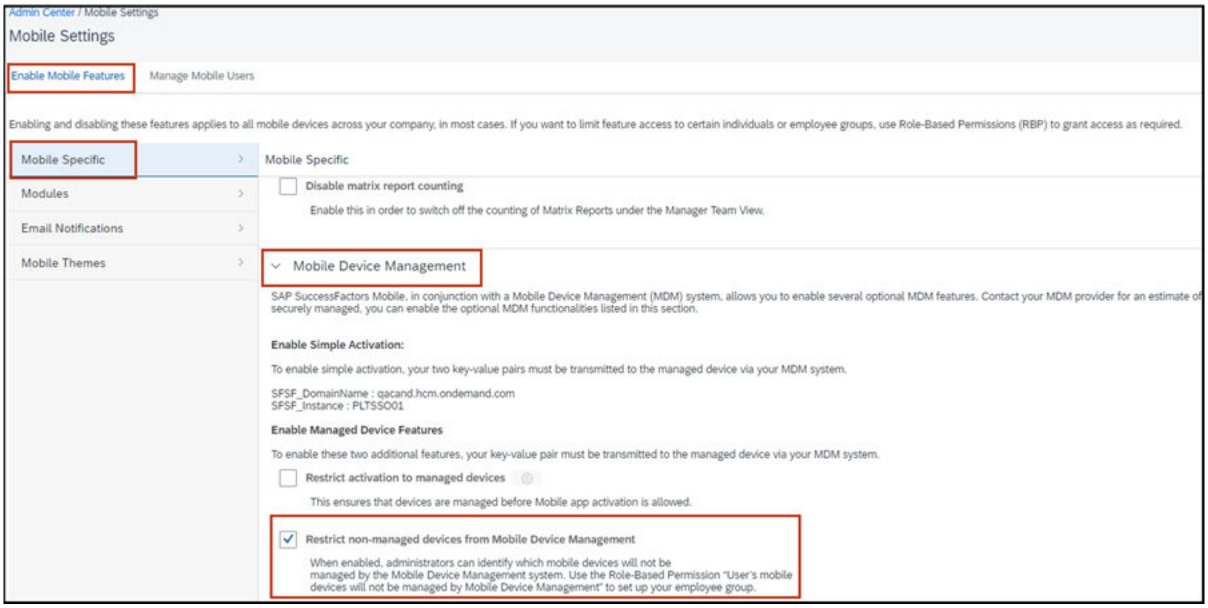
Ensure that certain non-managed devices are excluded from mobile device management.

Context

Administrators can specify which mobile devices will not be managed by Mobile Device Management when this feature is enabled.

Procedure

1. In the SAP SuccessFactors web application, go to the *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile Device Management* section.
2. Enable the *Restrict non-managed devices from Mobile Device Management* feature.



Enabling and disabling these features applies to all mobile devices across your company, in most cases. If you want to limit feature access to certain individuals or employee groups, use Role-Based Permissions (RBP) to grant access as required.

Mobile Specific

□ **Disable matrix report counting**

Enable this in order to switch off the counting of Matrix Reports under the Manager Team View.

Mobile Device Management

SAP SuccessFactors Mobile, in conjunction with a Mobile Device Management (MDM) system, allows you to enable several optional MDM features. Contact your MDM provider for an estimate of
securely managed, you can enable the optional MDM functionalities listed in this section.

Enable Simple Activation:

To enable simple activation, your two key-value pairs must be transmitted to the managed device via your MDM system.

SFSF_DomainName : qacand.hcm.ondemand.com
SFSF_Instance : PLTSSO01

Enable Managed Device Features

To enable these two additional features, your key-value pair must be transmitted to the managed device via your MDM system.

□ **Restrict activation to managed devices**

This ensures that devices are managed before Mobile app activation is allowed.

☑ **Restrict non-managed devices from Mobile Device Management**

When enabled, administrators can identify which mobile devices will not be managed by the Mobile Device Management system. Use the Role-Based Permission "User's mobile devices will not be managed by Mobile Device Management" to set up your employee group.

A confirmation window appears.

3. Select *Turn ON*, then *OK*.

Results

Administrators now have the ability to identify which mobile devices will not be managed by the Mobile Device Management system.

11.4 Opting Out of Mobile App Passwords on Managed Devices

You can choose not to require passwords on mobile devices that are securely managed by your MDM solution, making the Mobile app easier for people to use.

Context

Only opt out of using mobile app passwords if all your organization's devices are securely managed by your MDM solution.

> ⓘ Note
>
> Before enabling this option, we highly recommend that you require a **strong device-level password** for all mobile devices in your organization.

Procedure

1. In the SAP SuccessFactors web application, go to *Admin Center* > *Enable Mobile Features* > *Mobile Device Management* > *Additional MDM Functionality*.
2. Select *Do not require the profile password on managed devices*.

   You're asked to confirm.
3. To confirm, choose *Turn ON*, then *OK*.

11.5 Regenerating the Key/Value Pair

Regenerate the key/value pair used for Mobile Device Management (MDM).

Context

For additional security, you can regenerate and repropagate Key/Value pairs to managed devices. One scenario is in response to jailbreaking or rooting of a managed device. In this case, you can regenerate the Key/Value pair, propagate to all managed devices, and then delete the old Key/Value pair from the MDM system. All devices that **don't** have the updated Key/Value pair are **deactivated**.

Procedure

1. To open MDF settings, go to *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile Device Management*.
2. Choose the ⚙ (Settings) icon next to the *Restrict activation to managed devices* feature setting.
3. Click the *Regenerate Key/Value Pair* button.
4. Select the old Key/Value pair and click the *Delete* icon to remove it. Now, propagate the new Key/Value pair to the managed devices.

12 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 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.

  > ⓘ 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.

13 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

13.1 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, ID, or 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, ID, or 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, ID, or URL was not identified, the user has the option to activate using the QR Code. Since a match was not discovered, please contact Technical Support to file a 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.

13.2 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.

   > ⓘ 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.

13.3 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.

ⓘ 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.

13.4 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

13.4.1 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.

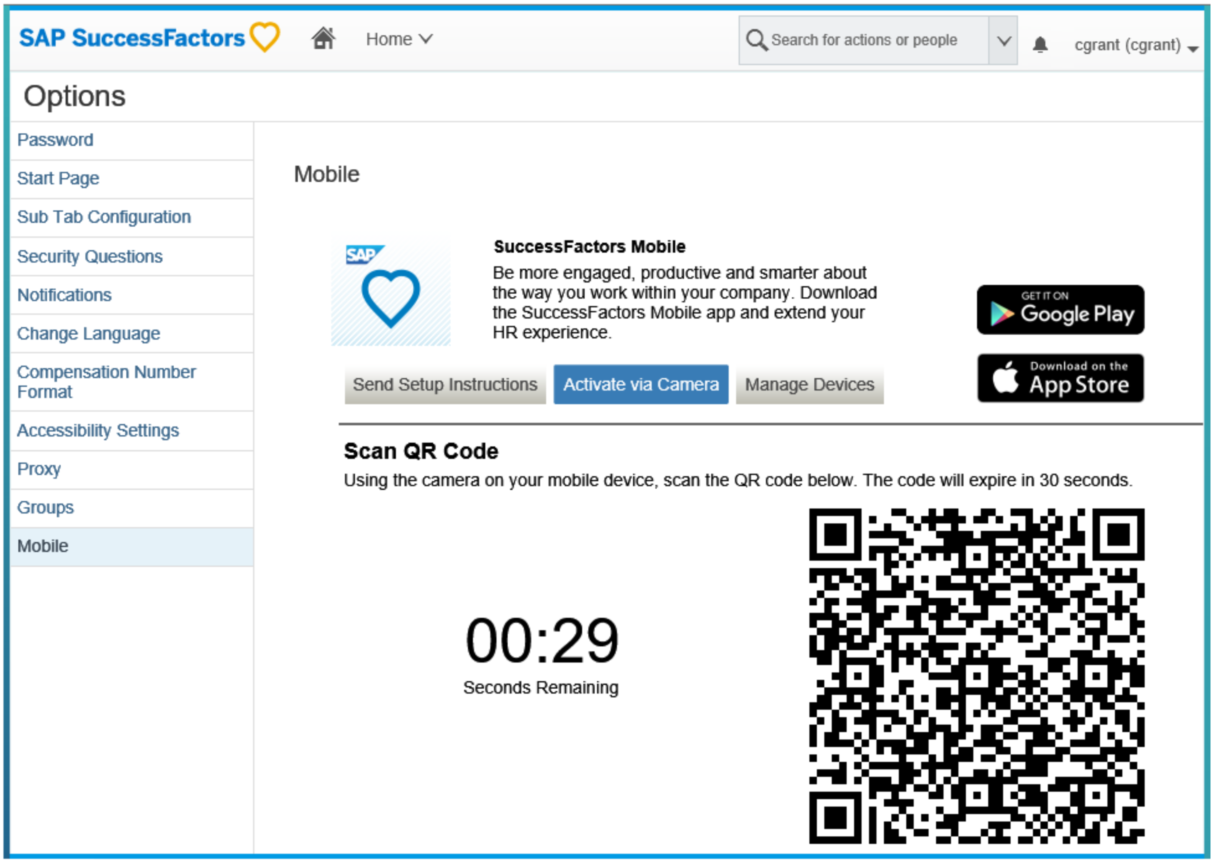
13.4.2 Using a Personal QR Code Activation

Procedure

1. Log into the SAP SuccessFactors web application.
2. Go to your personal *Mobile* settings page.
   - Use the *Activate Mobile App* quick action on the home page, if it's available to you.
   - Otherwise, open the account navigation menu in the page header (under your avatar photo) and choose *Settings*. Then choose the *Mobile* tab.
3. Choose a method for activating the SAP SuccessFactors Mobile app on your device.
   - Use *Send Setup Instructions* screen to enter your email address and send yourself step-by-step instructions.
   - Use *Activate via Camera* to generate a temporary QR code that you can scan.
4. To activate with a QR code, choose *Activate via Camera*. Then use the camera on your mobile device to scan the QR code.

   If successful, the SAP SuccessFactors Mobile app is activated.

   This QR code is personal and can only be used by you. It expires after 30 seconds. If it expires, choose *Get New Code* to generate a new one.



Mobile

SuccessFactors Mobile

Be more engaged, productive and smarter about the way you work within your company. Download the SuccessFactors Mobile app and extend your HR experience.

Scan QR Code

Using the camera on your mobile device, scan the QR code below. The code will expire in 30 seconds.

Personal QR Code Activation

13.4.2.1 Mobile Activation on the Home Page

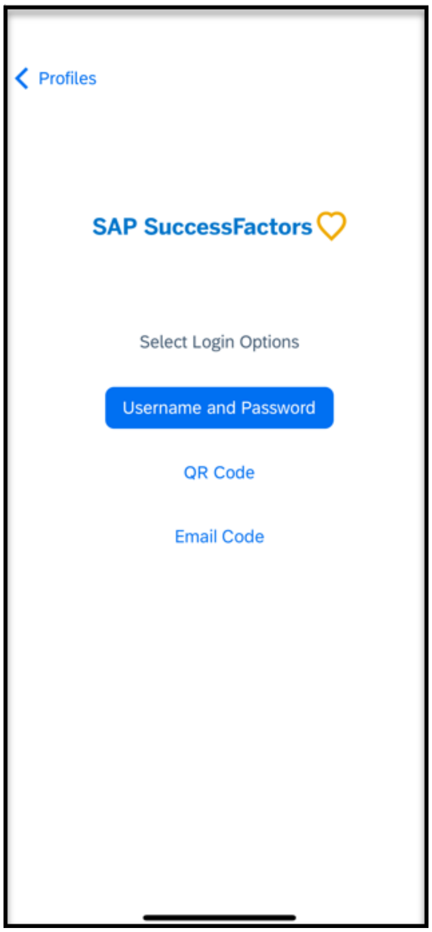
Learn about mobile activation features on the home page.

Name	Description	Where Shown	When Shown	Prerequisites	On Mobile App?
Activate Mobile App	Takes you to your account settings so you can activate the mobile app on your device.	*Quick Actions*	Always shown, based on system configuration and user permission.	• You have *Mobile Access* permission. • It's selected at *Manage Home Page* > *Quick Actions* .	No ⓘ Note Not applicable to the mobile application.

14 Logging into the Mobile App

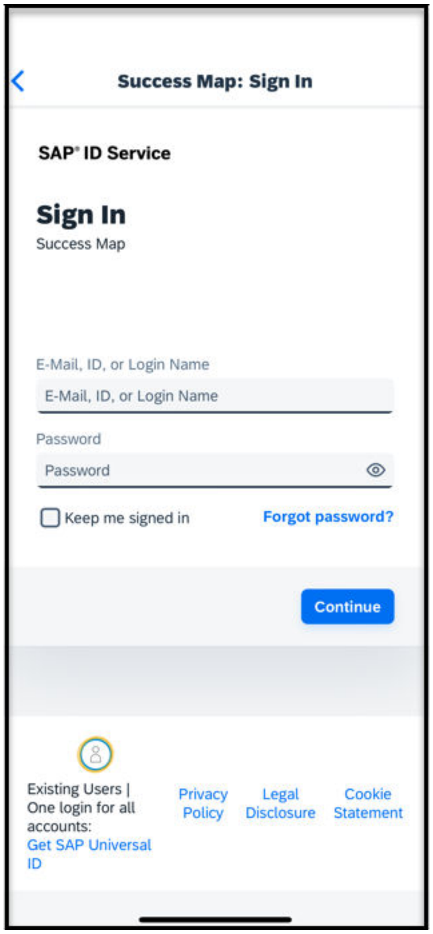
Sign into the mobile app using the login method of your choice.

When users are signed out from the mobile app, they can authenticate again using one of the methods available on the *Select Login Options* screen:



Based on your preference, choose one of the following options:

- **Username and Password**: This option takes the user to the configured login screen, be it the SAP SuccessFactors default or a company-provided SSO like Microsoft. The behavior of SSO scenarios depends on the company's configuration of their SSO provider. In some configurations, the user will need to enter their credentials. In other scenarios, SSO login may be automatic.



Success Map: Sign In

SAP® ID Service

Sign In

Success Map

E-Mail, ID, or Login Name

E-Mail, ID, or Login Name

Password

Password

□ Keep me signed in

Forgot password?

Continue

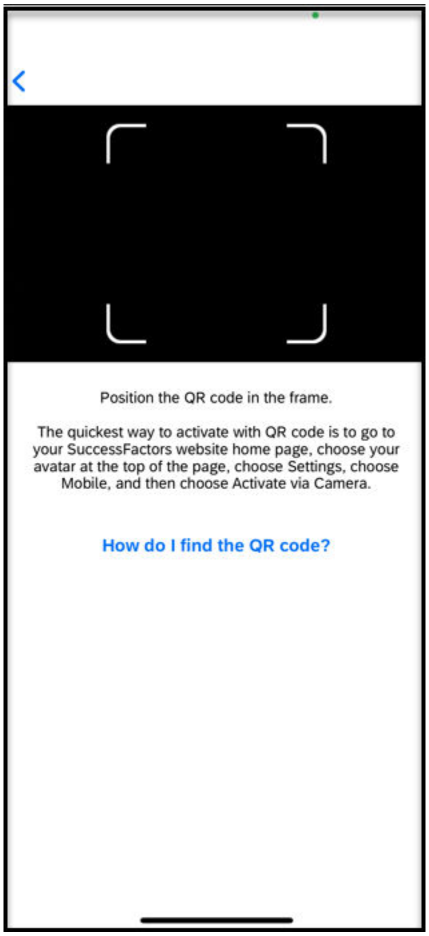
Existing Users | One login for all accounts: Get SAP Universal ID

Privacy Policy

Legal Disclosure

Cookie Statement

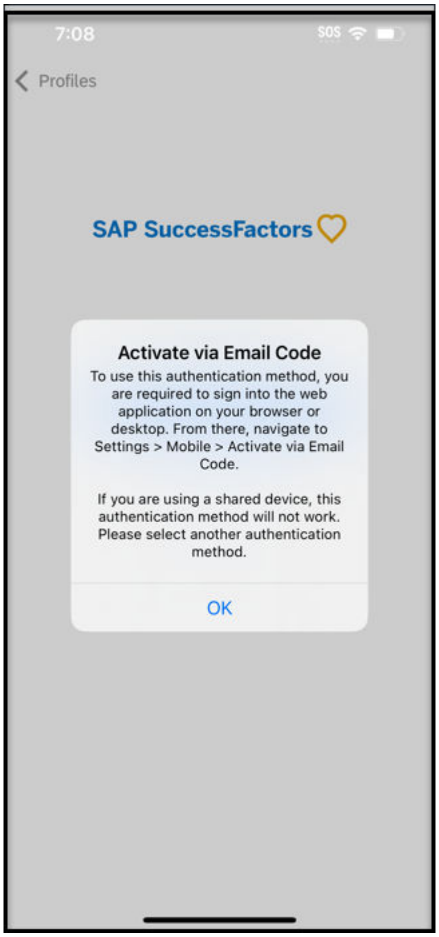
- **QR Code**: This option takes the user to a screen on which they can capture a QR code generated on the SAP SuccessFactors website by going to *Settings* > *Mobile* > *Activate via Camera*.



Position the QR code in the frame.

The quickest way to activate with QR code is to go to your SuccessFactors website home page, choose your avatar at the top of the page, choose Settings, choose Mobile, and then choose Activate via Camera.

- **Email Code**: This option presents a message that instructs the user to go to the *Settings* > *Mobile* > *Activate via Email Code* screen.



Activate via Email Code

To use this authentication method, you are required to sign into the web application on your browser or desktop. From there, navigate to Settings > Mobile > Activate via Email Code.

If you are using a shared device, this authentication method will not work. Please select another authentication method.

15 Increasing Mobile Adoption

The SAP SuccessFactors Mobile platform offers you the capability to deep link to specific parts of the Mobile app. This feature makes it easier for people to access SAP SuccessFactors Mobile functionality.

Deep Link Directly to Mobile Features

Mobile deep linking provides the ability to navigate to a specific screen or a specific action in a mobile application.

There are two kinds of deep links: content deep links and navigational deep links. A content deep link is typically provided through an email notification. Navigational deep links are used to launch the SAP SuccessFactors Mobile app for a specific screen.

If the user does not have any additional feature enabled, the deep link will navigate to:

- The *Home* screen of the Android app
- The leftmost tab of the iOS app.

Navigational Deep Link supported URLs

Embed these deep link URLs to your custom application to launch the specified SAP SuccessFactors Mobile app screens. For example, use a deep link to the show the *Approvals* screen in the Mobile app from your mobile portal.

Navigational deep links currently supported

Deep Link URL	Destination Screen in Mobile App	Description
bizx://?urlType=deeplink&deeplinkType=launchApp	For iOS, the most left side tab menu page. For Android, the Home screen.	Launches to the Mobile app screen.
bizx://?urlType=deeplink&deeplinkType=teamSpace	The Team screen	Shows the Team tab (menu) if available.
bizx://?urlType=deeplink&deeplinkType=goals	Goals	Takes you to the Goals landing screen showing a list of performance goals.
bizx:///sf/devplan	Goals	Takes you to the Goals landing screen showing a list of development goals.
bizx://?urlType=deeplink&deeplinkType=approvals	The page containing the Approval list	Shows the list of approvals.
bizx://?urlType=deeplink&deeplinkType=toDos	To-Do tab	Shows the To-Do screen.

Deep Link URL	Destination Screen in Mobile App	Description
bizx://?urlType=deeplink&deeplinkType=peopleSearch	People Search screen	Shows the People Search screen.
bizx://?urlType=deeplink&deeplinkType=timeSheet	Time Sheet screen	Shows the Time Sheet screen.
bizx://?urlType=deeplink&deeplinkType=timeOff	Time Off screen	Shows the Time off screen.
bizx://?urlType=deeplink&deeplinkType=paySummary	Pay Summary screen	Shows the Pay Summary screen.
bizx://?urlType=deeplink&deeplinkType=profile	Profile screen	Shows the logged in user's profile screen.
bizx://?urlType=deeplink&deeplinkType=profile&profileId=<profileId>	Profile for a specific person	Shows the Profile for a specific person if the "&profileId=<profileId>" parameter is set. Since this is optional, if it's not provided, it only shows the Profile page for the currently logged in user.
bizx://?urlType=deeplink&deeplinkType=orgChart	Org Chart	Shows the Org Chart.
bizx://?urlType=deeplink&deeplinkType=orgChart&profileId=<profileId>	Org Chart for a specific user	Shows the specific user's org chart.
bizx://?urlType=deeplink&deeplinkType=learning	Learning screen	Shows the Learning screen.
bizx:///sf/recruiting/offerdetail?formDataId=<formDataId>&company=<companyId>	Job Offer Approval	Takes you to request details for Job Offer Approval.
bizx:///sf/recruiting/jobreqsummary?reqid=<reqId>	Job Requisition Approval	Takes you to the request details for Job Requisition Approval.
bizx:///sf/home	Home	Takes you to the Home screen.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback	Feedback	Takes you to your Continuous Feedback landing screen.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=received	Feedback Received	Takes you to your Feedback Received overview screen.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=received&recordId=<recordId>	Feedback Details of a received feedback	Takes you to the details screen of your specific received feedback based on its record ID.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=given	Feedback Given	Takes you to your Feedback Given overview screen.

Deep Link URL	Destination Screen in Mobile App	Description
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=given&recordId=<recordId>	Feedback Details of a given feedback	Takes you to the details screen of your specific given feedback based on its record ID.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=request	Request Sent	Takes you to the overview screen for your sent feedback requests.
bizx://?urlType=deeplink&deeplinkType=continuousfeedback&feedbackType=request&recordId=<recordId>	Request Details	Takes you to the details screen of your specific sent feedback request based on its record ID.
bizx://?urlType=deeplink&deeplinkType=myCPMActivities	My Activities	Takes you to your activities overview screen.
bizx://?urlType=deeplink&deeplinkType=myCPMActivities&initialHash=/activityList/<target user assignment id>	Activities	Takes you to the target user's Activities landing screen.
bizx:///sf/activities&initialHash=/activityList/<target user assignment id>		
bizx://?urlType=deeplink&deeplinkType=myCPMActivities&initialHash=/activity/<target user assignment id>/<record id>	Activity Details	Takes you to the details screen of the target user's specific activity.
bizx:///sf/activities&initialHash=/activity/<target user assignment id>/<record id>		
bizx://?urlType=deeplink&deeplinkType=myCPMActivities&initialHash=/achievement/<target user assignment id>/<record id>	Activity Details of an activity marked as an achievement	Takes you to the details screen of the target user's specific activity that has been marked as an achievement.
bizx:///sf/activities&initialHash=/achievement/<target user assignment id>/<record id>		
bizx:///sf/OMP/Mentoring/SignUp?programId=<program id>&p=mentor&menteeId=<user id>	Mentee	Takes you to a mentee's details screen.
bizx:///sf/mentoring	Mentoring	Takes you to the Mentoring landing screen.
bizx:///sf/latestpayperiod	Payment History	You can select a start and end date, and view all payslips generated during that period.

16 Authentication with BTP Mobile Services

Authentication with BTP Mobile Services is a prerequisite for using Joule in the SAP SuccessFactors mobile app.

If you want to adopt Joule, you first need to set up authentication with BTP Mobile Services in your system.

> ⚠ Caution
>
> When you enable authentication with BTP Mobile Services, it has the following impacts on all mobile users:
>
> - All mobile users are deactivated. They have to reactivate the app and authenticate with BTP Mobile Services. As with any deactivation of the app, all locally stored information is deleted, including offline learning progress.
> - Multi-profile mode is no longer supported. The *Multiple Profiles* option is removed from the *Settings* screen in the mobile app and the app can no longer be activated for multiple profiles. It can only be activated for one SAP SuccessFactors user account at a time.

It also has the following impacts:

- Some screens in the authentication flow within the mobile app are provided by BTP and look different. For example, the mobile app password is called a "passcode" and the screen where you create or enter the passcode looks different.
- You can no longer activate the app using a temporary activation code. The *Activate via Email Code* option is removed from user settings in the web application, at *Settings* > *Mobile*.
- Proxy users can no longer sign into the app as another user. If you're acting as a proxy for another user in the web application and then use a QR code to sign in, you're signed into the app as yourself, not the other user.
- The reauthentication duration, configured at *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Require Reauthentication*, is no longer enforced. It's always 180 days.
- IP restrictions, configured at *Admin Center* > *IP Restriction Management*, are no longer enforced.
- All records at *Admin Center* > *Mobile Settings* > *Manage Mobile Users* are cleared.
- The post-activation email notification, configured at *Admin Center* > *Enable Mobile Features* > *Email Notifications*, is no longer sent.

For the iOS app only:

- The password history policy, configured at *Admin Center* > *Enable Mobile Features* > *Mobile Specific* > *Mobile App Password*, is no longer enforced.
- If you sign out of the app on 1 device, you're signed out of the app on all other iOS devices that use the same user account.

For the Android app only:

- The option to enable biometric identification is removed from the *Settings* screen in the app. Instead, it's on the screen where you enter your passcode, when launching the app.

Related Information

Setting Up Joule in SAP SuccessFactors

17 Text Customization for Mobile Apps

You can customize text in the iOS and Android Mobile apps, using the *Manage Languages* tool.

Mobile app message keys and values are included in the CSV file you download from *Manage Languages*, containing default system text. You can then use the CSV file to upload new values for Mobile keys and they're reflected in the Mobile apps. Mobile message keys follow these naming conventions:

- All Mobile keys begin with the prefix `MOB_`.
- IOS keys end with the suffix `_ios`.
- Android keys end with the suffix `_android`.
- Keys that are used on both platforms don't have a suffix.

> → Tip
>
> Just like the web application, you can use the "English Debug" locale to identify which key corresponds to text on the screen. When the English Debug locale is selected in your language settings, message keys are displayed in the Mobile apps, in the place of the regular localized text value. For example, instead of the word "Home", in the iOS app you see the key `MOB_HOME_home_menu_home_ios`.

Related Information

Customizing UI Text with the Language Management Tool

18 Language Used for Mobile Apps

Understand how we determine which language to use in the iOS and Android Mobile apps.

Mobile apps use the language that's selected in your user preference settings for the SAP SuccessFactors system, not the languages selected in your device settings.

> ⓘ Note
>
> Occasionally, text appears in the mobile app that's generated by your device's operating system. If your device's language doesn't match the language selected in your SAP SuccessFactors user preference settings, you see a mix of two languages. For a more consistent experience, use the same language for both SAP SuccessFactors and your mobile device.

Related Information

Choosing a Language in Your Personal Settings

19 Change History

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

July 2025

Type of Change	Description	More Info
None	We didn’t update this document.	

May 2025

New features and enhancements listed below will be available in the app version scheduled for release after the 1H 2025 Production date.

Type of Change	Description	More Info
New	We added information about navigational deep links that are supported with this release.	Increasing Mobile Adoption [page 40]

February 2025

Type of Change	Description	More Info
Changed	We updated information about the *Multiple Profiles* feature.	Enabling the Mobile App for Multiple Profiles [page 15]

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 an 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.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP