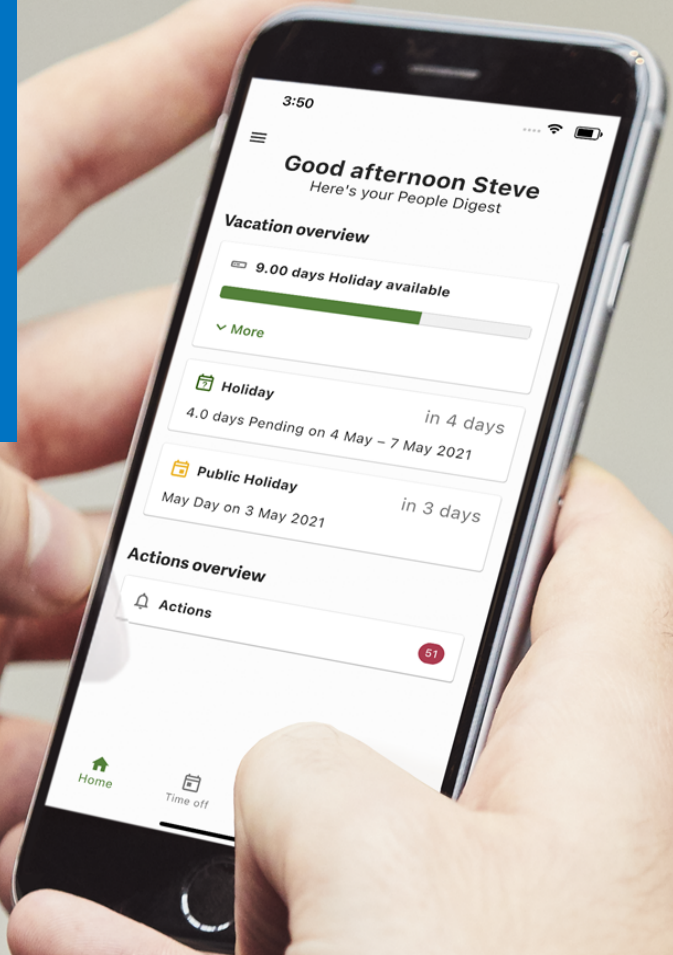


Sage People Mobile

R3 2022 | 1.6.0



Copyright Statement

© Sage 2022. All rights reserved.

This document contains information proprietary to Sage and may not be reproduced, disclosed, or used in whole or in part without the written permission of Sage.

Software, including but not limited to the code, user interface, structure, sequence, and organization, and documentation are protected by national copyright laws and international treaty provisions. This document is subject to U.S. and other national export regulations.

Sage takes care to ensure that the information in this document is accurate, but Sage does not guarantee the accuracy of the information or that use of the information will ensure correct and faultless operation of the service to which it relates. Sage, its agents and employees, shall not be held liable to or through any user for any loss or damage whatsoever resulting from reliance on the information contained in this document.

Nothing in this document alters the legal obligations, responsibilities or relationship between you and Sage as set out in the contract existing between us.

This document may contain screenshots captured from a standard Sage system populated with fictional characters and using licensed personal images. Any resemblance to real people is coincidental and unintended.

All trademarks and service marks mentioned in this document belong to their corresponding owners.

SP-MBL-CG-202207-R001.10

Contents

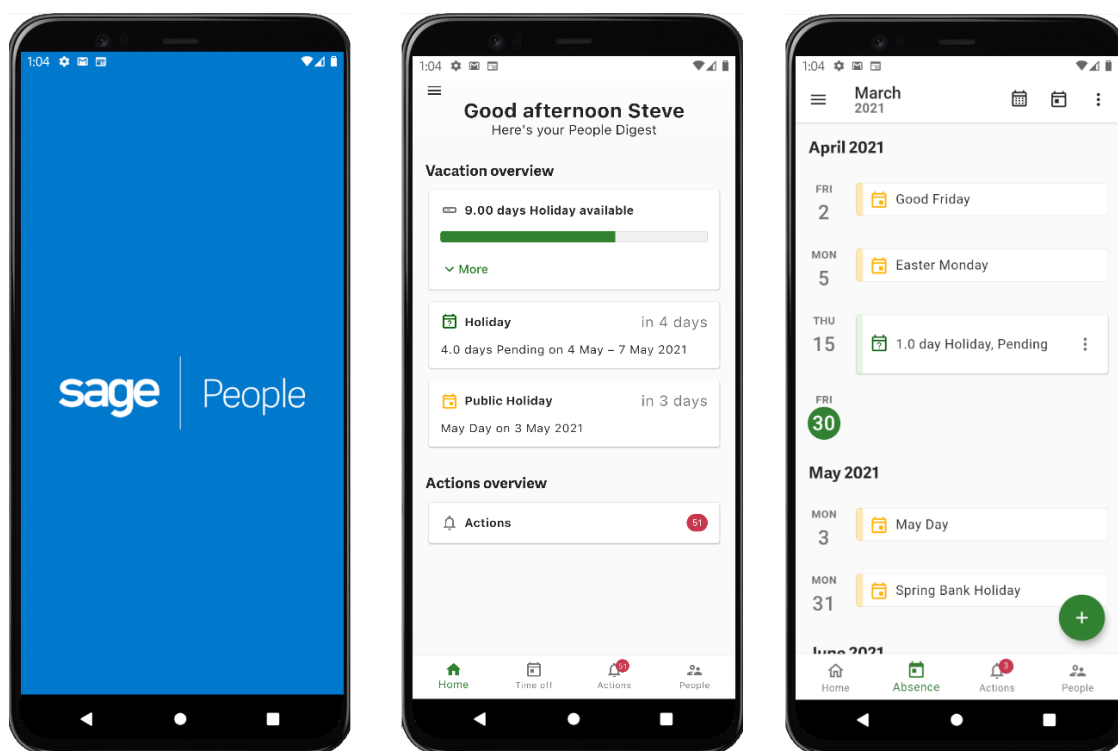
Sage People mobile	5
Requirements	5
Download the app	6
Configure mobile access	7
Enable mobile in the HCM package	7
Manage connected app settings	8
Assign the mobile app permission set	11
Edit user profiles	13
Activate mobile in your policies	16
Configure WX Processes	17
Configure push notifications	17
App notification settings	18
Registration for push notifications	19
Configure payslips	21
Assign the Payflow permission set	21
Enable the Payslips process for mobile	22
Enable payslips in the policy	23
Configure payroll field sets	23
Distribute the app to your users	27
Distribute a setup link	27
Troubleshooting	31
Users can't sign in to the app	31
Users cannot access time off or work details	31
The organization chart does not appear	32
Incorrect values are shown in the time off graph	32
Payslips are not ordered correctly	33

Security	34
Session management	34
Device security	35
Information stored on the device	35
Remote access revocation	36
Data integrity	36
Frequently asked questions	37
How do users sign in to the app?	37
How long does a user session last?	37
How do I remotely log out a team member's device?	37
What security features does the app use?	38
What data does the app store on the device?	38
How does the app secure local session information?	39
How can I delete data stored by the app?	39
What user telemetry is sent by the app?	39
Does the app track my activity or capture personal information?	40
What device permissions does the app require?	40
What accessibility features are supported?	40
Why aren't empty fields displayed on the My Work Details page?	40
Known and resolved issues	41
Known issues	41
Resolved issues	41
Limitations	42

Sage People mobile

The Sage People mobile app for Android and iOS provides seamless access to your people management system wherever you are. Designed to complement the desktop experience, the Sage People mobile app helps deliver better and faster workforce experiences, streamline HR processes, and provides employees with the ability to work effectively on the go.

Note This guide is for system administrators who are setting up access to the app for their organization. If you do not have system administrator permissions, contact the administrator for your organization. If you need assistance making the configuration changes detailed in this guide, contact your support representative.



Requirements

The app supports the following versions of Android and iOS:

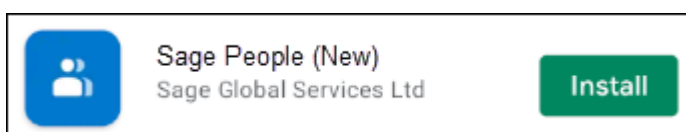
- Android 6 (Marshmallow) and later
- iOS 11.4 and later

To deploy the mobile app in your organization you must have the following Sage People packages, available from 2022 Release 3 (July 2022):

- **Human Capital Management (HCM)** package v36.02 and later.
- **Sage People Time** v34.10 and later.

Download the app

Users can download the **Sage People** app from the Google Play store or the iOS App Store.



Supported features:

- Book time off, manage attendance and absence
- View and update work details
- Get notified of pending actions and approvals
- Search your organization directory
- Access all processes for your organization using the WX mobile website.

Note The Sage People mobile app is continuously being improved with new features and enhancements. Users will be notified of new features within the app and through Sage People release notes when they become available.

Configure mobile access

Follow these steps to configure the Sage People mobile app for your organization.

Enable mobile in the HCM package

Enable mobile features in your organization's HCM package.

1. In Salesforce Lightning Experience, go to **Setup > Apps > Packaging > Installed Packages**.

In Salesforce Classic, go to **Setup > Installed Packages**.

ADMINISTRATION

- > Users
- > Data
- > Email

PLATFORM TOOLS

- ✓ Apps
 - App Manager
 - AppExchange Marketplace
 - > Connected Apps
 - > Lightning Bolt
 - > Mobile Apps
 - ✓ Packaging
 - Installed Packages**
 - Package Manager
 - Package Usage
 - > Feature Settings
 - > Einstein

Installed Packages

On AppExchange you can browse, test drive, download, and install pre-built apps and components right in Salesforce. Apps and components are installed in packages. Any custom apps, tabs, and custom objects are initially installed in the other features in setup or as a group by clicking Deploy.

Depending on the links next to an installed package, you can take different actions from this page. To remove a package, click **Uninstall**. To manage your package licenses, click **Manage Licenses**.

Action	Package Name	Publisher
Uninstall	#Sage People Analytics Pack 3	Sage People
Description 24th September update		
Uninstall Configure Manage Licenses	Sage People Compensation Planning	Compensation Planning Packaging Org
Uninstall Configure	Sage People US Tax Forms	The Sage Group plc
Uninstall Manage Licenses	Sage People Asvnc Reporting	The Sage Group plc
Uninstall Configure	Sage People - Human Capital Management	The Sage Group plc
Description Empower your team with: job description, performance m		
Uninstall	Salesforce Connected Apps	Salesforce.com
Description This package contains Connected Applications for all the		
Uninstall Configure Manage Licenses	Sage People Recruit	Fairsail
Description Specify job, attract candidates, take applications, select t		

2. Find the **Human Capital Management (HCM)** package and select **Configure**.
3. Under Features, find the Mobile Features setting and select the **Enabled** checkbox.

Mobile Features Show various mobile features and toggles in HCM and WX ☒

4. At the top of the page, select **Save**.

Note We recommend that you complete this step first. Until you have enabled mobile in the HCM package, you will not be able to activate mobile in your policies, or activate WX services for mobile.

Manage connected app settings

Connected app settings define the authentication requirements and timeout settings for users to access the app. There are separate connected apps for Android and iOS.

1. In Salesforce Lightning Experience, go to **Setup > Apps > Connected Apps > Manage Connected Apps**.

In Salesforce Classic, go to **Setup > Manage Apps > Connected Apps**.

PLATFORM TOOLS

- Apps
 - App Manager
 - AppExchange Marketplace
- Connected Apps
 - Connected Apps OAuth Usage
 - Manage Connected Apps**
 - Lightning Bolt
 - Mobile Apps
 - Packaging
 - Feature Settings
 - Einstein
 - Objects and Fields
 - Events
 - Process Automation
 - User Interface
 - Custom Code
 - Environments
 - User Engagement

Manage access to apps that connect to this Salesforce organization.

App Access Settings [Edit](#)

☒ Allow users to install canvas personal apps

View: [All](#) [Create New View](#)

Action	Master Label
Edit	Ant Migration Tool
Edit	DataLoader Bulk
Edit	DataLoader Partner
Edit	Force.com IDE
Edit	Payflow Staging AUS
Edit	restapi
Edit	Sage People Android
Edit	Sage People iOS
Edit	Sage People Mobile
Edit	Sage People Mobile Android
Edit	Sage People Mobile iOS
Edit	Salesforce for Outlook
Edit	Salesforce Mobile Dashboards
Edit	Salesforce Touch
Edit	Workbench

2. In the list, find the Sage People Mobile Android and Sage People Mobile iOS apps. Complete the remaining steps for each app.
3. Click **Edit** next to the app.
4. Leave the **Start URL** and **Mobile Start URL** fields in the Basic Information section blank.

5. Configure the following OAuth policy settings for the app, as required by your organization:

OAuth Policies

Permitted Users: **All users may self-authorize** (dropdown)

IP Relaxation: **Relax IP restrictions** (dropdown)

Enable Single Logout: ☐ ⓘ

Refresh Token Policy:

- ☐ Refresh token is valid until revoked
- ☐ Immediately expire refresh token
- ☐ Expire refresh token if not used for Day(s)
- ☒ Expire refresh token after 30 Day(s)

Session Policies

Timeout Value: 15 minutes

☐ High assurance session required

Permitted Users: defines whether users may self-authorize or must be pre-approved by the administrator.

- **All users may self authorize:** when signing in to the app with their credentials, users are asked to confirm that they allow the app to access their information.
- **Admin approved users are pre-authorized:** Users who are pre-approved are not shown the Allow Access screen when signing in. In order to pre-approve users, you must allow access to the connected app in the user's permission set or profile.

Note

For information about enabling pre-authorization for users, see:

- [Create a new permission set for pre-authorized users \(optional\)](#)
- [Pre-authorize users in the user profile \(optional\)](#)

IP Relaxation: defines how the organization's IP address restrictions are applied for access to the app. Typically, IP address restrictions are relaxed for use of the mobile app, to allow users to connect using different networks.

- **Enforce IP restrictions:** enforces IP restrictions configured for the organization, such as IP ranges assigned to a user profile.
- **Enforce IP restrictions, but relax for refresh tokens:** this option bypasses IP restrictions when the app uses a refresh tokens to request a new access token.
- **Relax IP restrictions for activated devices:** bypasses IP restrictions when the user successfully completes identity verification if accessing the service from a new browser or device.
- **Relax IP restrictions:** bypasses IP restrictions for the app.

Refresh Token Policy: users are required to re-authenticate using their sign in credentials when the token expires. Typically set to 30 or 60 days, depending on your organization's policy.

6. Set the session policy settings for the app, as required by your organization.
 - **Timeout Value:** defines how long an access token remains valid for an app session. When the access token expires, the app re-authenticates with the service in the background, as long as the refresh token is still valid. Set this according to your organization's security policy. If set to **None**, the timeout value defaults to the setting in the user profile. If the user profile does not have a setting, the organization's Session Settings are used.
 - **High assurance session required:** requires two-factor authentication when users sign in to the app. Recommended if you have two-factor authentication configured for your organization.

Set the radio button to **Raise the session level to high assurance**.



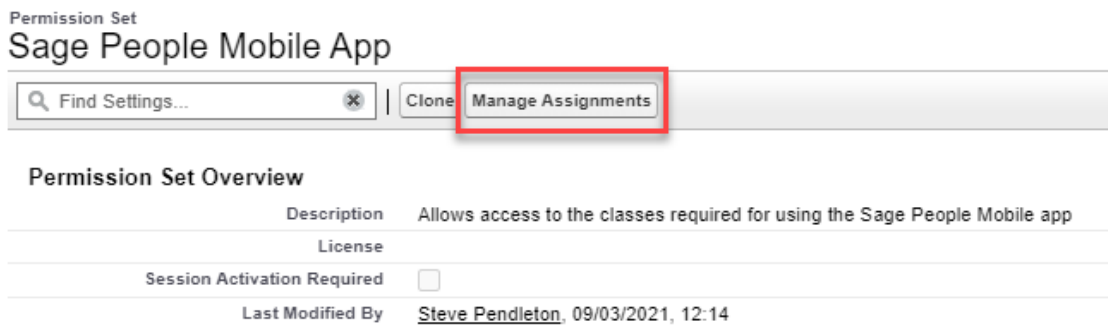
7. Select **Save**.
8. If you have both Android and iOS users in your organization, ensure you have configured settings for both connected apps.

Assign the mobile app permission set

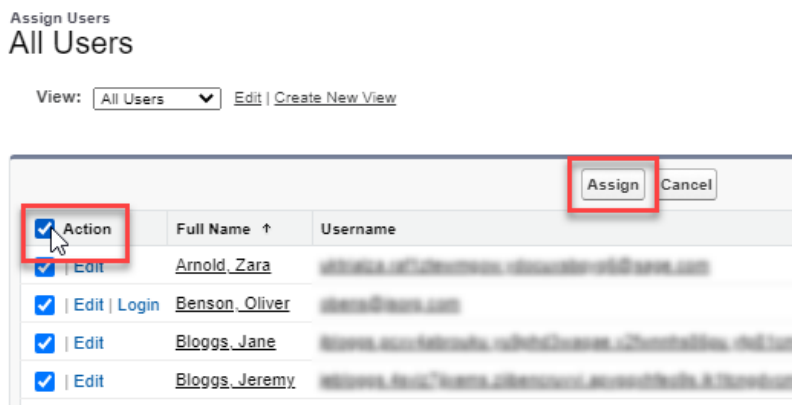
The Sage People Mobile App permission set enables assigned users to sign in to the app. Assigning the permission set to your users is the recommended way to assign these permissions. If you do not want to use permission sets, you can assign the appropriate permissions as part of the user profile. See [Edit user profiles](#).

Note Team members who do not have the correct permissions see the message "Unable to log in".

1. In Salesforce Lightning Experience, go to **Setup > Users > Permission Sets**.
In Salesforce Classic, go to **Setup > Manage Users > Permission Sets**.
2. Find the **Sage People Mobile App** permission set and click to open it.
3. Click the **Manage Assignments** button at the top of the page.



4. Click **Add Assignments**, and select the users who should have access to the app.
Tip: select the **Action** checkbox if you want to apply the permission set to all users.



5. Click **Assign**.

Create a new permission set for pre-authorized users (optional)

Note This step is only required if you want to pre-authorize users in your OAuth policy settings. Users can be pre-authorized either by using a permission set or in the user profile. See [Manage connected app settings](#).

To pre-authorize users for access to the app, you can clone the Sage People Mobile permission set (or create a new permission set), and assign the Sage People Mobile Android and Sage People Mobile iOS connected apps to the permission set.

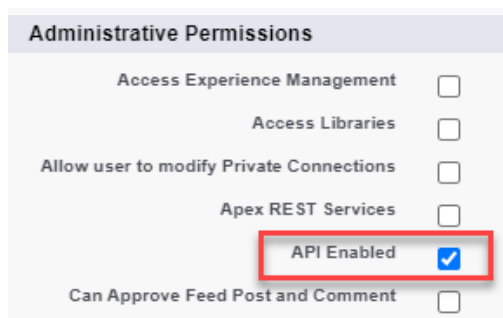
To clone the permission set and assign the connected apps:

1. In Salesforce Lightning Experience, go to **Setup > Users > Permission Sets**.
In Salesforce Classic, go to **Setup > Manage Users > Permission Sets**.
2. Find the **Sage People Mobile App** permission set and open it.
3. Click **Clone** at the top of the page.
4. Give the new permission set a new **Label**.
5. Click **Save**.
6. Under Apps, click **Assigned Connected Apps**.
7. Click **Edit**.
8. In the list of Installed Connected Apps, select **Sage People Mobile Android**. Click **Add** to move it to the Enabled Connected Apps list.
9. Select **Sage People Mobile iOS**. Select **Add** to move it to the Enabled Connected Apps list.
10. Select **Save**.
11. Assign the new permission set to your users. See [Assign the mobile app permission set](#).

Edit user profiles

Enable the Salesforce API in your user profiles:

1. In Salesforce Lightning Experience, go to **Setup > Users > Profiles**.
In Salesforce Classic, go to **Setup > Manage Users > Profiles**.
2. Find the profile assigned to the users who require access to the app. Click **Edit**.
3. Under Administrative Permissions, ensure the **API Enabled** checkbox is selected.



Administrative Permissions	
Access Experience Management	<input type="checkbox"/>
Access Libraries	<input type="checkbox"/>
Allow user to modify Private Connections	<input type="checkbox"/>
Apex REST Services	<input type="checkbox"/>
API Enabled	<input checked="" type="checkbox"/>
Can Approve Feed Post and Comment	<input type="checkbox"/>

4. Click **Save**.

Tip: Editing the profile applies the change to all users assigned to the profile.

Assigning mobile permissions as part of the profile (optional)

Note This step is not required if you have assigned users the **Sage People Mobile App** permission set.

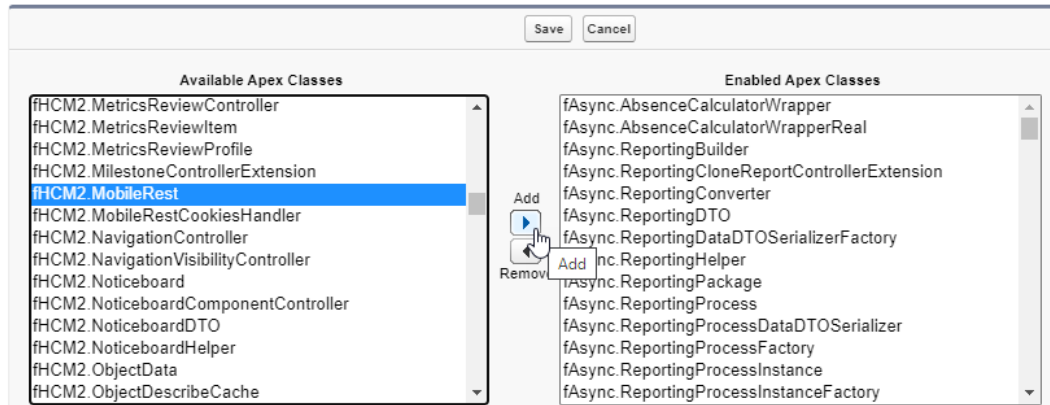
If you do not want to use the **Sage People Mobile App** permission set to assign permissions, you can assign mobile permissions as part of the user profile. This can be useful if you want to assign mobile permissions to all users in a profile, and control access to the app using the **Mobile Is Active** setting in a policy (see [Activate mobile in your policies](#)).

To assign required mobile permissions to a profile:

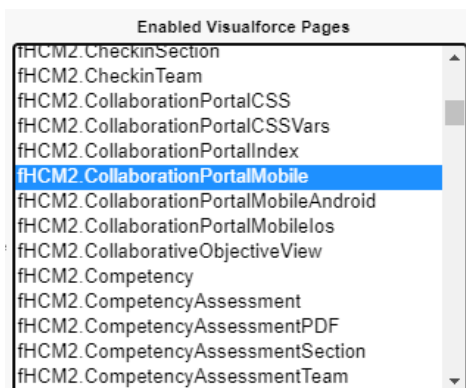
1. In Salesforce Lightning Experience, go to **Setup > Users > Profiles**.
In Salesforce Classic, go to **Setup > Manage Users > Profiles**.
2. Find the profile assigned to the users who require access to the app. Click the profile name.
3. At the top of the profile page, select **Enabled Apex Class Access**.
4. Click **Edit**.

- In the Available Apex Classes list, find the **fHCM2.MobileRest** class. Click the arrow to add this to the Enabled Apex Classes list.

Enable Apex Class Access



- Click **Save**.
- At the top of the profile page, select **Enabled Visualforce Page Access**.
- Click **Edit**.
- In the Available Visualforce Pages list, find the **fHCM2.CollaborationPortalMobile** page. Click the arrow to add this to the Enabled Visualforce Pages list.



- Click **Save**.

You have now assigned the required permissions directly to the user profile.

Pre-authorize users in the user profile (optional)

Note This step is only required if you want to pre-authorize users in your OAuth policy settings. Users can be pre-authorized either by using a permission set or in the user profile. See [Manage connected app settings](#).

To pre-authorize users for access to the app, you can add the Sage People Mobile Android and Sage People Mobile iOS connected apps to the user profile.

To add the connected apps to a user profile:

1. In Salesforce Lightning Experience, go to **Setup > Users > Profiles**.
In Salesforce Classic, go to **Setup > Manage Users > Profiles**.
2. Find the profile assigned to the users who require access to the app. Click **Edit**.
3. Under Connected App Access, select the **Sage People Mobile Android** and **Sage People Mobile iOS** checkboxes.
4. Select **Save**.

Activate mobile in your policies

All policies assigned to your app users must have the **Mobile Is Active** option enabled.

1. In Salesforce Lightning Experience, click the App Launcher and find the **Policies** item.

In Salesforce Classic, click the **Policies** tab.

2. In the Policies list, click the policy you want to edit.
3. Click **Edit**. Scroll down to the Mobile Features section, and select the **Mobile Is Active** checkbox.

Mobile Features

Mobile Is Active  ☒

4. Click **Save**.
5. When you have enabled this setting and saved the policy, a setup link is displayed on the Policy page, under Mobile Features. Copy the **Team Member Mobile App Link** URL:

Mobile Features

Mobile Is Active  

Team Member Mobile App Link

<https://sagepeople.page.link/?link=https://app.sagepeople.com/login?url%3Dhttps://sagepeople.com/sagepeople&ibi=com.sage.people&ofl=https://sagepeoplecommunity.sage.com/s/sage-people-new-mobile>

You can distribute this link to your users to enable them to download and configure the app on their devices.

Note Editing the policy applies the change to all users with the policy. To enable the app for a subset of users, consider creating a new policy that has the mobile app enabled.

Configure WX Processes

Any WX Processes that you want to be available in the app, either natively or through the in-app browser, must be active and must have the **Show In Mobile** checkbox selected.

1. In Salesforce Lightning Experience, select the App Launcher and open the **WX Services** item.
In Salesforce Classic, click the All Tabs button and open the **WX Services** tab.
2. Select the name of a service that hosts the processes that should be made available in the app.
3. Select the process name to open the process instance page, then select **Edit**.
4. Select the **Active** and **Show In Mobile** checkboxes.

Label: Vacation & Absence

Active: ☒

WX Service: Vacation & Absence

Order: 10

Start Date: [16/04/2021]

End Date: [16/04/2021]

Preferred Number Of Columns: 1

Show In Mobile: ☒

Show Title In Tile: ☒

5. Click **Save**.

Note Currently, the app natively supports the following WX process types:

- Time off (note: the legacy Absences process type is not supported)
- Work details
- Payslips

All other processes are accessed using the in-app browser. Processes must be active and have **Show in Mobile** enabled in order to be available in the app.

Configure push notifications

Push notifications enable Sage People to send information messages to the mobile app when an action event is triggered. Users can tap the notification on their device to view

the relevant action. Mobile push notifications use standard Sage People Action Events . Action Event Patterns are linked to policies to enable you to control this functionality per policy.

To configure push notifications for mobile:

1. In the HR Manager portal, go to **Action Event Patterns**.
2. Open the appropriate action event pattern, and select the event that you want to enable for mobile push notifications.
3. Select **Edit**.
4. In the **Push Notification Alert Message** field, enter the text of the message you want to appear in the mobile app. This field can contain merge fields to return values from records such as Team Member or Employment.

The screenshot shows the configuration interface for an Action Event Pattern. At the top right are 'Cancel' and 'Save' buttons. The 'Details' tab is selected, showing various configuration fields. The 'Event' field is set to 'Absence' and 'New'. The 'Email Template' is set to 'Unfiled Public Email Templates'. The 'Description' field contains the text 'Sends notification of new absence request trigger'. The 'Push Notification' tab is also visible, with the 'Push Notification Alert Message' field highlighted by a red rectangle.

5. Select **Save**.

When an action event with a **Push Notification Alert Message** configured is triggered, the notification message is sent to the user's app.

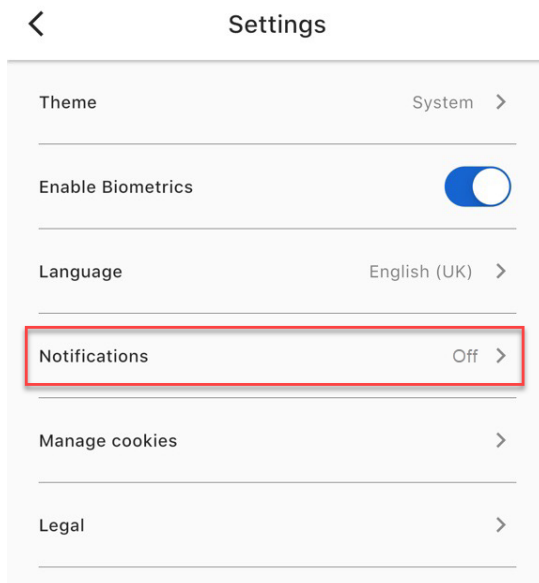
App notification settings

For push notifications to be displayed, notifications must be enabled for the app in the user's device notification preferences. For Android devices, this setting is enabled by default. For iOS, the device asks permission when the user first signs in to the app.

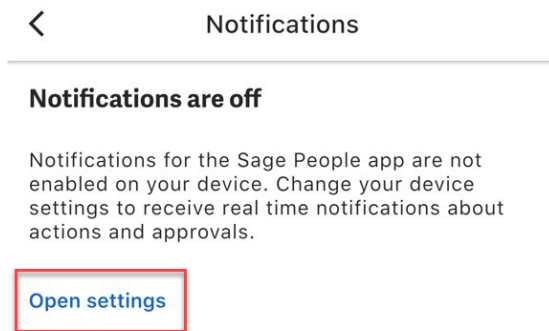
To check that notifications are enabled:

1. Open the menu and tap **Settings**.
2. The **Notifications** item displays whether notifications are on or off.

3. To enable notifications, tap **Notifications**.



4. Tap **Open settings** to be taken to your device notification preferences.

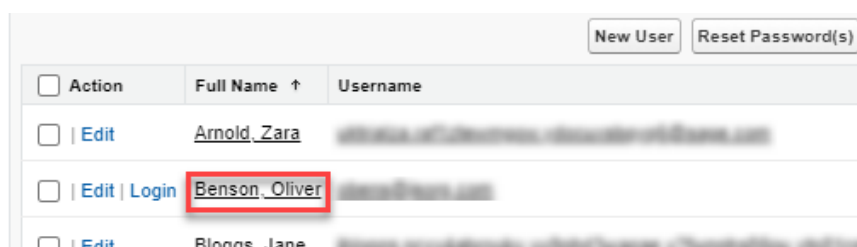


5. Enable notifications in your device settings.

Registration for push notifications

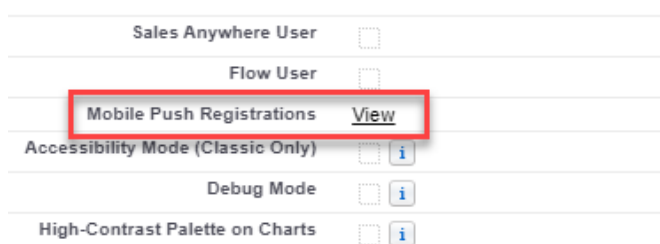
To check push registration details for a user account:

1. Go to **Setup > Users > Users**.
2. Select the Full Name of the user:



<input type="checkbox"/> Action	Full Name ↑	Username
<input type="checkbox"/> Edit	Arnold, Zara	arnold.zara@sagepeople.com
<input type="checkbox"/> Edit Login	Benson, Oliver	benson.oliver@sagepeople.com
<input type="checkbox"/> Edit	Blinnis, Jane	blinnis.jane@sagepeople.com

3. On the User Detail screen, select **View** beside Mobile Push Registrations:



Sales Anywhere User	<input type="checkbox"/>
Flow User	<input type="checkbox"/>
Mobile Push Registrations	View
Accessibility Mode (Classic Only)	<input type="checkbox"/> i
Debug Mode	<input type="checkbox"/> i
High-Contrast Palette on Charts	<input type="checkbox"/> i

The **Mobile Push Registrations** screen details any mobile apps that are registered to receive push notifications for the user.

Configure payslips

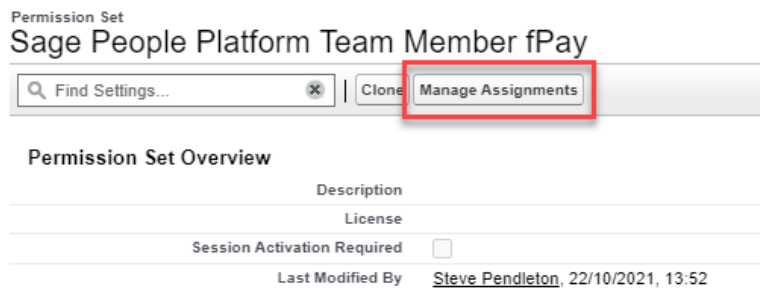
Payslips can be displayed in the mobile app if you have an active Payflow integration to your payroll provider. Payslips for mobile requires Payflow package version 32.3 or higher. For information on implementing Payflow for your organization, see the [Payflow Implementer's Guide](#).

Follow these steps to enable payslips for mobile:

- Assign the Payflow permission set
- Enable the Payslips process for mobile
- Enable Payslips in the policy
- Configure payroll field sets.

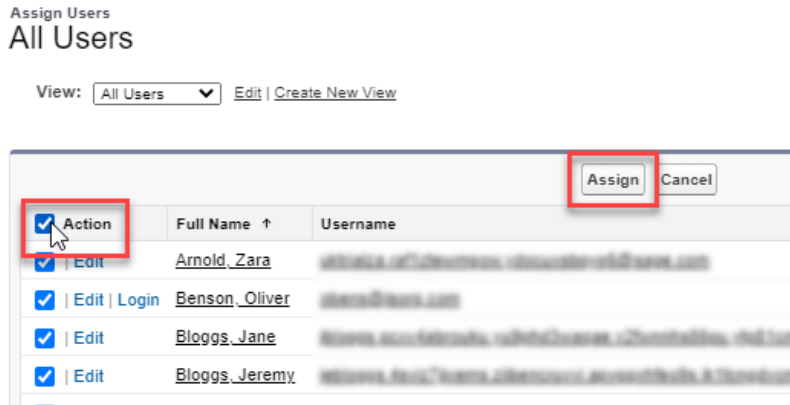
Assign the Payflow permission set

1. In Salesforce Lightning Experience, go to **Setup > Users > Permission Sets**.
In Salesforce Classic, go to **Setup > Manage Users > Permission Sets**.
2. Find the **Sage Platform Team Member fPay** permission set and click to open it.
3. Click the **Manage Assignments** button at the top of the page.



- Click **Add Assignments**, and select the users who should have access to the app.

Tip: select the **Action** checkbox if you want to apply the permission set to all users.



- Click **Assign**.

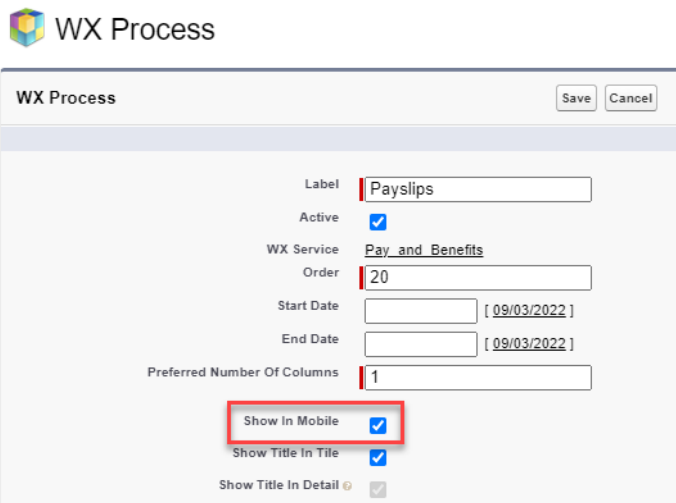
Enable the Payslips process for mobile

Ensure you have a Payslips process enabled for your organization. For help creating one, see [Creating a New WX Process](#) in the Sage People administrator help.

- In Salesforce Lightning Experience, select the App Launcher and open the **WX Services** item.

In Salesforce Classic, select the All Tabs button and open the **WX Services** tab.

- Open the service that hosts the Payslips process.
- Click the process name to open the process instance page, then click **Edit**.
- Enable **Show In Mobile** for the process.



WX Process

Save Cancel

Label Payslips

Active ☒

WX Service Pay and Benefits

Order 20

Start Date [09/03/2022]

End Date [09/03/2022]

Preferred Number Of Columns 1

Show In Mobile ☒

Show Title In Tile ☒

Show Title In Detail ☒

5. Select **Save**.

Enable payslips in the policy

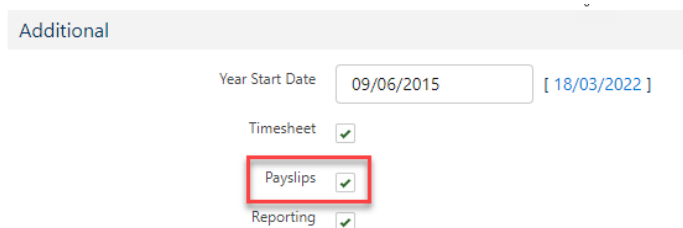
The Payslips setting must be enabled in any policies assigned to your app users for whom you want payslips to appear.

1. In Salesforce Lightning Experience, click the App Launcher and find the **Policies** item.

In Salesforce Classic, click the **Policies** tab.

2. In the Policies list, click the policy you want to edit.

3. Click **Edit**. Scroll down to the Additional section, and select the **Payslips** checkbox.



Additional

Year Start Date 09/06/2015 [18/03/2022]

Timesheet ☒

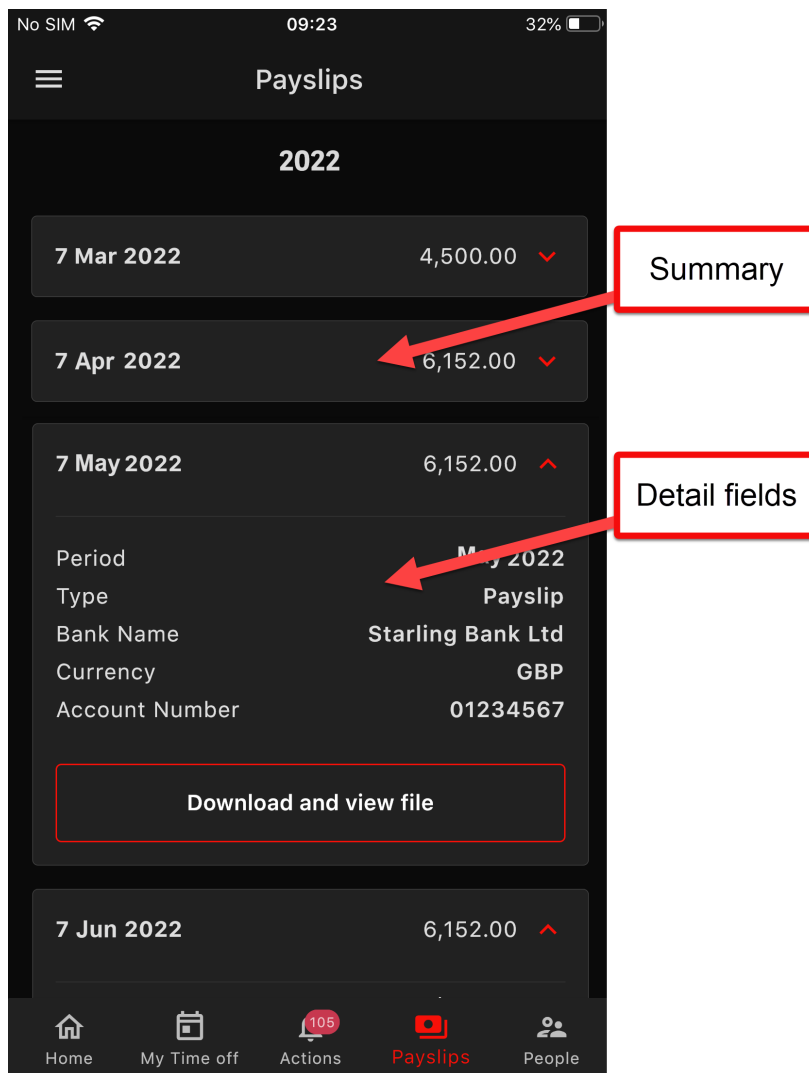
Payslips ☒

Reporting ☒

4. Select **Save**.

Configure payroll field sets

The detail fields displayed on the payslips page are controlled by the content of field sets in the Connector Line object.



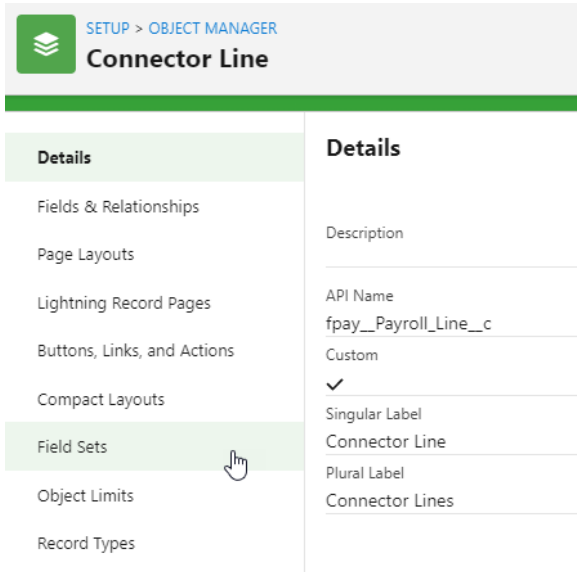
By default, the summary line displays the created date of the payroll line item. You can customize the information included on the payslips page by adding or removing fields from the following field sets:

- Payroll Line Summary
- Payroll Line Details

To adjust the fields that are shown for the payslips process:

1. In Setup, go to **Object Manager**.
2. Search for Connector Line (API name `fpay__Payroll_Line__c`).

3. Select the object and go to **Field Sets**.



The screenshot shows the Salesforce Setup interface for the 'Connector Line' object. The breadcrumb trail at the top indicates the path: **SETUP** > **OBJECT MANAGER**. The main header displays the object name 'Connector Line' next to a green icon representing a stack of papers. On the left, a sidebar menu lists various configuration options: 'Details', 'Fields & Relationships', 'Page Layouts', 'Lightning Record Pages', 'Buttons, Links, and Actions', 'Compact Layouts', 'Field Sets' (which is highlighted with a green background and a mouse cursor), 'Object Limits', and 'Record Types'. The main content area, titled 'Details', contains several fields: 'Description' (empty), 'API Name' (filled with 'fpay__Payroll_Line__c'), 'Custom' (checked with a green checkmark), 'Singular Label' (filled with 'Connector Line'), and 'Plural Label' (filled with 'Connector Lines').

SETUP > **OBJECT MANAGER**
Connector Line

Details

- Fields & Relationships
- Page Layouts
- Lightning Record Pages
- Buttons, Links, and Actions
- Compact Layouts
- Field Sets**
- Object Limits
- Record Types

Details

Description

API Name
fpay__Payroll_Line__c

Custom
✓

Singular Label
Connector Line

Plural Label
Connector Lines

4. Add items to the following field sets as required.

The field sets used by the payslips page in the mobile app are as follows.

Field Set	What it's used for
Payroll Line Summary	<p>Defines what is displayed in the summary line for a payroll item in the mobile app.</p> <p>We recommend you include the following fields in this field set:</p> <ul style="list-style-type: none"> • Pay Date: used to display the correct pay date for each payslip in the summary line. • Amount: used to include the pay amount for each payslip in the summary line. <p>Note If the Amount field is included in the field set, but the amount is not populated for a payroll line item such as a tax document, the summary line displays the label "Document". Users can open the payroll item to view and download the document.</p>
Payroll Line Details	<p>Defines the detail fields that are shown when a payroll item is expanded.</p> <p>Fields included in this field set are displayed when the pay item is expanded. Add fields that may be useful for team members to see, for example:</p> <ul style="list-style-type: none"> • Period • Type • Account Name • Account Number • Currency

Note If a field exists in both field sets, the field is only displayed once.

Distribute the app to your users

If your organization uses a custom My Domain URL for signing in, the app must be configured to use your organization's URL. To aid the deployment of the app to many users, you can distribute a setup link that automatically configures the app to use the correct URL.

The app can also be configured manually when signing in, using the **Set Login URL** button.

What is a custom domain?

Custom domains can be in the following forms:

- yourorg.cloudforce.com
- yourorg.my.salesforce.com
- fs-1234.cloudforce.com

Your organization's custom domain can be found by going to **Setup > Company Settings > My Domain**:

My Domain Settings

A My Domain showcases your company's brand and keep your data more secure by making your Salesforce org's URL customer-specific.

My Domain Details		Edit
Current My Domain URL	yourorg.cloudforce.com	
My Domain Name	yourorg	
Domain Suffix	Cloudforce (*.cloudforce.com)	
URL Stabilization	If enhanced domains are enabled, URLs are stabilized and these settings have no effect. <input checked="" type="checkbox"/> Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs <input checked="" type="checkbox"/> Include the instance name in Visualforce URLs when third-party cookies are blocked	

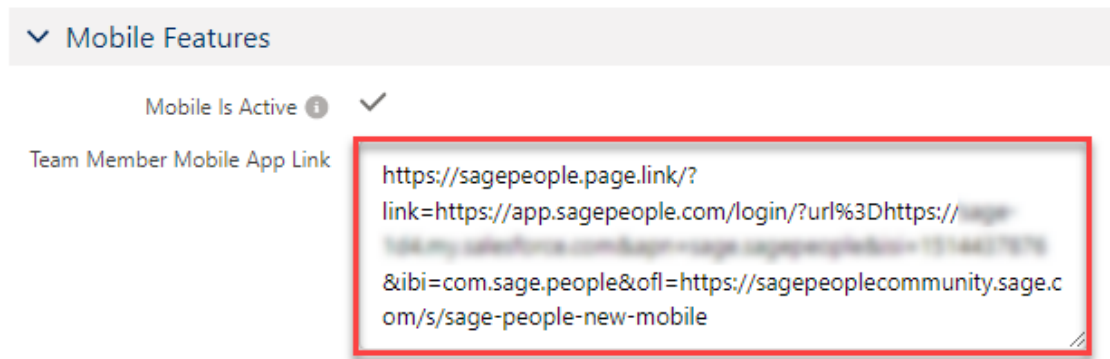
Note Using your custom domain is a requirement for accessing the app using single sign-on (SSO). If you do not use SSO in your organization, users can sign in using the standard Salesforce login URL using their Sage People credentials.

Distribute a setup link

A mobile setup link is available on the policy page in the HR Manager portal, when the **Mobile Is Active** setting is enabled for the policy. This setup link is a deep link that automatically configures the app with your organization's unique sign-in URL.

After enabling the setting, save the policy. The setup link is displayed on the Policy page under Mobile Features.

Copy the **Team Member Mobile App Link** URL that appears in the Mobile Features section:



Distribute this link to your users and instruct them to follow the link from their mobile device. The link behaves in the following ways:

- If the mobile app is not already installed, the user is taken to the Google Play store or Apple App Store as appropriate, where they can install the app. The deep link automatically configures the organization's sign-in URL for the app when installation has completed.
- If the user already has the app installed when the link is followed, the deep link will automatically configure the organization's sign-in URL for the app.
- Users accessing the link from a desktop device are taken to a webpage with instructions on how to install the app.

After the app sign-in URL has been configured using the deep link, users can follow the usual procedure for authenticating with the app using their Sage People login credentials or single sign-on details.

Tip

A set of instructions you can distribute to your end users is available here: <https://sagepeoplecommunity.sage.com/s/sage-people-new-mobile>

How to configure the sign-in URL manually

If you need to manually set up and start using the app, for example for testing purposes, follow this procedure on your device to configure the sign-in URL manually.

Your organization's custom domain can be found by going to **Setup > Company Settings > My Domain**:

My Domain Settings

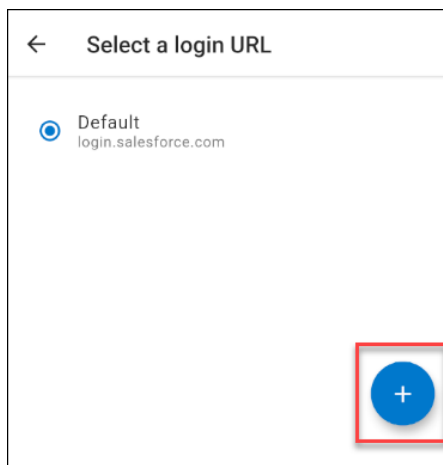
A My Domain showcases your company's brand and keep your data more secure by making your Salesforce org's URL customer-specific.

My Domain Details		Edit
Current My Domain URL	[redacted].cloudforce.com	
My Domain Name	[redacted]	
Domain Suffix	Cloudforce (*.cloudforce.com)	
URL Stabilization	If enhanced domains are enabled, URLs are stabilized and these settings have no effect. <input checked="" type="checkbox"/> Stabilize Visualforce, Experience Builder, Site.com Studio, and content file URLs <input checked="" type="checkbox"/> Include the instance name in Visualforce URLs when third-party cookies are blocked	

1. Install the app from the Google Play store or the Apple App Store.

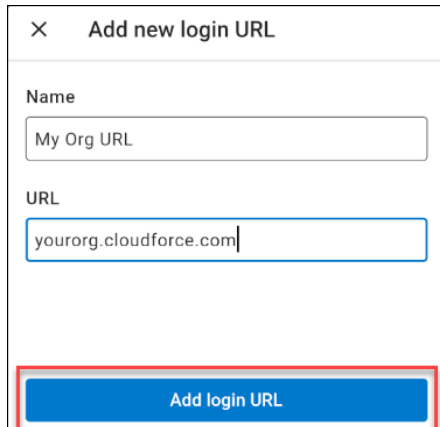


2. Open the app and tap **Set Login URL**
3. Tap the **Add +** button

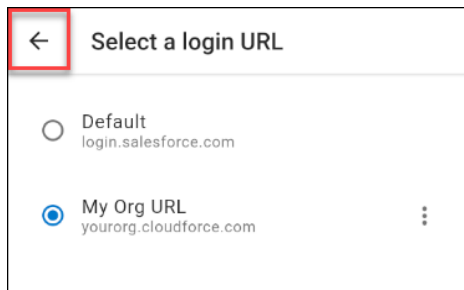


4. Enter a name for the login URL, for example "MyOrg URL".

5. Enter your organization's My Domain URL, for example: "yourorg.cloudforce.com".



6. Tap **Add Login URL**
7. Tap the **Back** arrow.



8. Tap **Login**.

You can now authenticate using your Sage People credentials or single sign-on details.

Troubleshooting

If users are having issues with the app and would like support, ensure that they have enabled analytics cookies in the **Cookie management** section. Analytics cookies enable error reporting functions that send issue details to Sage to assist with troubleshooting.

Some common issues and suggested solutions are detailed below.

Users can't sign in to the app

If users cannot access the app using single sign-on (SSO), check that SSO has been configured and tested for your organization. To use SSO, users must sign in using your organization's custom My Domain URL. See [Distribute the app to your users](#).

Ensure the user's device is configured to use network-provided system date and time, and that system time is not set manually. Single sign-on requires an accurate timestamp for successful authentication.

If users are shown an "Unable to log in" message when attempting to sign in, check the following:

- Your organization has upgraded to the minimum supported version of the HCM and Time packages.
- Mobile features are enabled in your organization's HCM package.
- Users have the **Sage People Mobile App** permission set assigned.
- The user profile has the **API Enabled** option selected.
- The **Mobile Is Active** setting is enabled in the policy.

Check the configuration steps detailed in the [Configure mobile access](#).

If users are shown the message "Error getting user session", check whether you have the **Admin approved users are pre-authorized** setting enabled in your Connected App configuration. If you have this setting enabled, you must pre-authorize users by assigning the connected app to the user's permission set or profile. See [Manage connected app settings](#).

Users cannot access time off or work details

If users are unable to book or approve time off, or access their work details, check the following settings are enabled for your WX Services:

- Active
- Show in mobile.

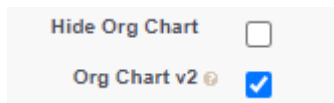
If your WX Services have a set start date and end date, ensure that the service is currently valid. If the service has a start date in the future or an end date in the past, the service will not be available in the app.

In order to view work details in the app, team members must have fields available in the Work Details View field set within the Team Member object.

The organization chart does not appear

Ensure that the **Org Chart v2** setting is enabled in the HCM package and that the org chart is not hidden:

1. In Salesforce Lightning Experience, go to **Setup > Apps > Packaging > Installed Packages**.
In Salesforce Classic, go to **Setup > Installed Packages**.
2. Find the **Human Capital Management (HCM)** package and select **Configure**.
3. Under Setup, select the **Org Chart v2** setting to enable the organization chart.
4. Ensure that the **Hide Org Chart** setting is not selected.



5. Click **Save**.

Ensure the **Hide Org Chart** setting is not enabled in your policy:

1. In Salesforce Lightning Experience, click the App Launcher and open the **Policies** item.
In Salesforce Classic, open the **Policies** tab.
2. In the Policies list, click the policy you want to edit.
3. Click **Edit**. Scroll down to the WX section, and clear the **Hide Org Chart** checkbox.
4. Click **Save**.

Incorrect values are shown in the time off graph

Incorrect values can be displayed if you have more than one default absence accrual rule for an absence type. To resolve the issue, ensure that there is a single absence accrual rule for each absence type.

1. In Salesforce Lightning Experience, click the App Launcher and open the **Absence Accrual Patterns** item.
In Salesforce Classic, click the All Tabs button and open the **Absence Accrual Patterns** tab.
2. Click the name of the absence accrual pattern you want to edit.
3. Under Absence Accrual Rules, ensure that each absence type (for example "Vacation", "Absence") has a single default rule associated with it.
4. If necessary, click **Edit**, and change the **Default** checkbox selection, then click **Save**.

	Absence Accrual Rule Name	Type	Reason	Default
1	2017.07 #45	Vacation	Annual Leave	<input checked="" type="checkbox"/>
2	2017.07 #48	Absence	Compassionate Leave	<input type="checkbox"/>
3	2017.07 #51	Absence	Jury Service	<input type="checkbox"/>
4	2017.07 #46	Absence	Maternity	<input type="checkbox"/>
5	2017.07 #47	Absence	Paternity	<input type="checkbox"/>
6	2017.07 #49	Absence	Sickness	<input checked="" type="checkbox"/>

5. Repeat this for each absence accrual pattern relevant to your app users.

Payslips are not ordered correctly

Payslips might be ordered incorrectly in the Payslips area of the app if the **Pay Date** field is not included in the Payroll Line Summary field set. If this field is not included, payslips are ordered by the date that the payroll item was created. Additionally, if this field is not included, payslips might change order in the list when a payslip entry is opened. To resolve these issues, ensure that the **Pay Date** field is added to the Payroll Line Summary field set.

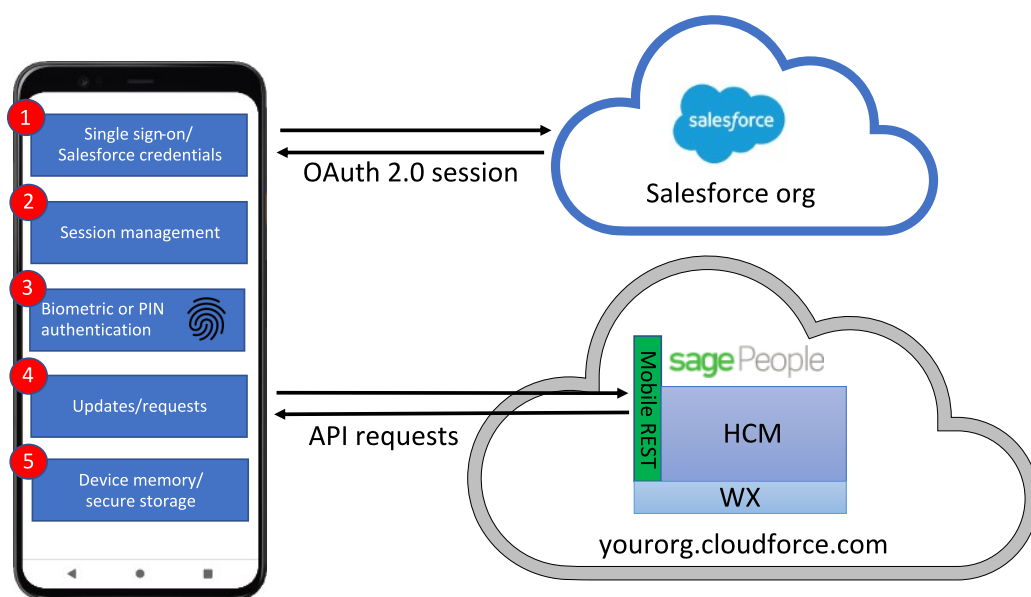
For information about adding fields to the payroll fieldsets, see [Configure payroll field sets](#).

Security

The Sage People mobile app has been designed for security. This section outlines the security features used by the app, and the secure service architecture that underpins it.

Session management

The service uses the OAuth 2.0 authorization standard to permit a connected app to access the user's Sage People information.



1. The user signs in using their single sign-on credentials or Salesforce details. The service issues an OAuth access token and refresh token to authenticate the session. These tokens are securely stored on the device.
2. Sessions are managed by Salesforce using the policies configured against the Sage People Mobile Android and Sage People Mobile iOS connected apps. You can set session policies for your organization that define requirements for the OAuth session, such as the token expiration timeout, IP address restrictions, and single sign-on.

When the access token expires, the app automatically requests a new access token using the refresh token. If the app cannot obtain a new token for any reason, the user is signed out of the app and must re-authenticate using their credentials.

3. The app times out after 2 minutes of inactivity. Access to the mobile app is secured using the device's biometric authentication or a user-defined PIN.
4. Calls to the service from the app use a dedicated mobile REST API. The API performs checks to ensure that the user has the required permissions and that requested data is enabled for mobile. The API calls WX business logic to access team member self-service features.
5. The app uses device memory to store information while the app is open. Session information, such as refresh and access tokens, is stored using the device's native encrypted storage.

If the user signs out of the app, the refresh token is expired and any sessions associated with the token are revoked.

Device security

The app uses the following methods to secure access to user information on end-user devices.

- Device authentication: the app uses the device's biometric hardware, or a user-configured PIN, for authentication. After four incorrect PIN attempts, the user is logged out of the app and must re-authenticate using their credentials.
- Inactivity timeout: the app times out after 2 minutes of inactivity. After this, the user must re-authenticate using biometric hardware or their PIN.
- App switcher image protection: mobile operating systems can take snapshots of the app screen to display when scrolling through active apps in the device app switcher. To prevent personal information being captured, the app displays a blank screen when the app is sent to the background.

Information stored on the device

Most data is stored in memory while the app is open, and not cached on the device. The app retrieves data using API requests, stores the data in memory while the app is running, and clears the data when the app is closed.

The app stores the following information:

- Encrypted session information
- The user's app preferences, including the app version and the sign-in URL
- Avatar images and organization logo (stored in cache folder)

- In-app browser cache (cookies, cached images, temp files)
- Uploaded/downloaded files are stored in the app's folders on the device.

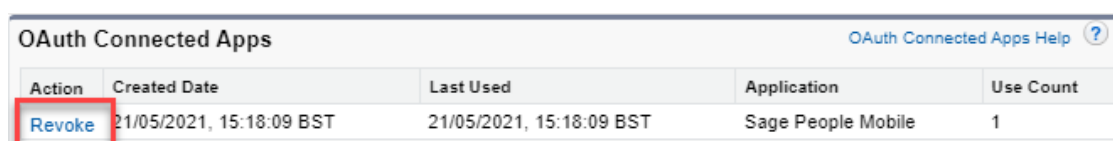
Closing the in-app browser clears the in-app browser cache and stored cookies. Signing out of the app clears all data stored by the app.

Encrypted session information

Session information such as the access token, refresh token and PIN is stored securely on the device using AES-256 encryption. The user's username and password are not stored.

Remote access revocation

System administrators can revoke active user sessions, and prevent users from signing in to the app by revoking app permissions using the **Setup** section of the HR administrator portal.



OAuth Connected Apps OAuth Connected Apps Help ?				
Action	Created Date	Last Used	Application	Use Count
Revoke	21/05/2021, 15:18:09 BST	21/05/2021, 15:18:09 BST	Sage People Mobile	1

See [How do I remotely log out a team member's device?](#) in the FAQ section.

Data integrity

To ensure data integrity, the app monitors the device's network connection and displays a message to the user in the case of a loss of internet connectivity. No user activity can be performed in the app without an active network connection. All changes and updates within the app are actioned with a single API request per change. It is not possible for information on the end user's local device to become out of sync with your Sage People organization. Because of the app's network status monitoring, it is unlikely that a significant amount of user activity (such as changing details or creating a new absence request) would be lost in the case of a loss of connectivity or a device crash.

Frequently asked questions

How do users sign in to the app?

Users must use their Sage People username and password or single sign-on details.

To access the app, the user must have the **Sage People Mobile App** permission set assigned and the user profile must have the **API Enabled** checkbox selected.

Note

Users whose profiles do not have the appropriate permissions can install the app, but see an "Unable to log in" message when attempting to sign in.

Pre-boarders, and those who have left the organization, are unable to sign in to the app.

After signing in for the first time, the user is prompted to set a security PIN that can be used to unlock the app. If configured on the device, the user can unlock the app with biometric identification.

How long does a user session last?

You can control the duration of a user session with the **Refresh Token Policy** and **Session Policies > Timeout Value** settings on the **Setup > Apps > Connected Apps > Manage Connected Apps** page. This setting defines how frequently users are required to re-authenticate with their username and password. Typically this value is set to 30 or 60 days, depending on your organization's policy. See [Configure mobile access](#).

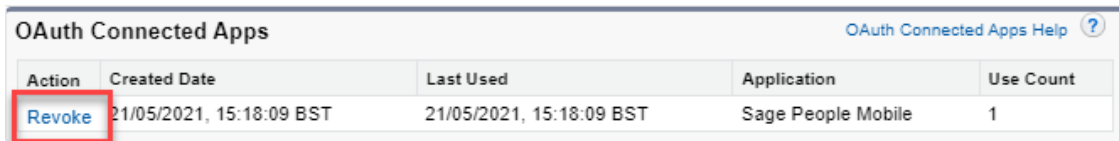
By default, the app requires PIN or biometric re-authentication after two minutes in the background.

How do I remotely log out a team member's device?

To remotely end the user's session (for example, if the team member's device is lost or compromised):

1. In Salesforce Lightning Experience, go to **Setup > Users > Users**.
In Salesforce Classic, go to **Setup > Manage Users > Users**.
2. Click the name of the user whose session you want to revoke.

3. Under **OAuth Connected Apps**, find the active Sage People Mobile session and click **Revoke**.



OAuth Connected Apps OAuth Connected Apps Help ?				
Action	Created Date	Last Used	Application	Use Count
Revoke	21/05/2021, 15:18:09 BST	21/05/2021, 15:18:09 BST	Sage People Mobile	1

The user's access and refresh tokens are removed, and the user is shown the sign-in screen when opening the app.

To prevent a user from signing in to the app, remove the Sage People Mobile App permission set for the user.

What security features does the app use?

The app employs a range of security features to keep user data secure:

- Access to the app is secured by a user-defined PIN or biometric identification.
- After four PIN entry attempts, the user is logged out and must authenticate using their username and password or single sign-on credentials.
- The app uses any multi-factor authentication requirements configured for the user's account.
- App screens are masked when the app is in the background.
- The app undergoes rigorous security testing, including regular penetration tests, and is subject to the Sage mobile certification release process.

What data does the app store on the device?

The app retrieves data using API requests, stores the data in memory while the app is running, and clears the data when the app is closed.

The app stores the following information locally on the device:

- Files uploaded to or downloaded from the app. These are stored in the app's folders on the device. These files are purged at specific times so they don't take up storage space.
- User session details are securely stored, including the Salesforce instance URL, access token, and refresh token.
- The team member's avatar image and the organization logo are stored in the app's cache folder.

- Temporary internet files used by the in-app browser (cookies, cached images, temp files).
- The user's app preferences, including the app version and the sign-in URL.

Files uploaded to or downloaded from the app are private to the app unless shared with or opened in another app. For example, viewing a PDF in Android via the app opens the file in a PDF viewer which makes a copy of the file. If removing all personally identifiable information from the device, these copies must be purged manually.

Note

The app also uses a web view to display Salesforce login and single sign-in web pages, and the self-service Sage People website. The web view uses standard web browser technology which employs caching and cookies.

How does the app secure local session information?

The app uses industry-standard encryption techniques using iOS Keychain and Android keystore technologies.

How can I delete data stored by the app?

Signing out of the app and uninstalling it clears all local data. If any downloaded files have been opened in another app (for example, downloaded PDF files) any copies of these files made by the third-party app must be manually removed.

Note

If you uninstall the app on iOS without signing out first, the Keychain entry is retained. This can be removed by reinstalling the app and opening it.

What user telemetry is sent by the app?

When analytics cookies are enabled, the following telemetry is used by Sage People to improve the app:

- Anonymous usage information is captured to help us determine the most widely used parts of the app. This enables us to focus improvements on the most popular parts of the app and to improve its usefulness.

- Anonymous crash information is captured, enabling us to identify and fix problems, drawing on as much usage information as possible. This information includes how the app has malfunctioned, and device details such as the make and model of phone.

Does the app track my activity or capture personal information?

The app does not collect or send any personally identifiable information. No activity outside of the app, such as browsing data or location information is available to the app.

For the Sage privacy notice and cookie policy, see the following links:

- US: <https://www.sage.com/en-us/legal/privacy-and-cookies>
- UK: <https://www.sage.com/en-gb/legal/privacy-and-cookies>

What device permissions does the app require?

The app requests specific device permissions that are required for it to function. For Android, app permissions are detailed in the Google Play store and can be viewed and controlled in your device settings. For iOS, app permissions can be viewed and controlled in your device settings.

What accessibility features are supported?

The app supports the following accessibility features:

- Font resizing: the app supports large font sizes, as set on the device.
- Accessible color palette: the app uses your organization's custom color – set at organization level – to generate an accessible color palette that is used throughout the app.
- Large buttons: the app uses large buttons which are designed to be easy to tap.

Why aren't empty fields displayed on the My Work Details page?

From app version 1.4.3 (December 2021), empty fields are now hidden on the My Work Details screen. This mirrors the behavior in the WX desktop interface.

Known and resolved issues

The Sage People mobile app is continuously being improved with new features and enhancements. This page lists current known issues, resolved issues, and limitations, and will be updated at each release.

Known issues

The app currently has the following known issues which will be addressed in future releases. If you encounter an issue not listed here, please report it to us by following your usual support process.

- For users on iOS 15 upgrading from a previous version of the app, images may fail to load in the WX mobile site the first time the in-app browser is opened. To work around this issue, close and reopen the in-app browser.
- When using iOS 12.4, the app content screen can briefly flicker when returning to the app from the notification screen, if the app has timed out after two minutes.

Resolved issues

The following app issues have been resolved.

Issue reference	Description	Resolved in app version	Date
SPPLDE-19017	When signing in to the app using iOS, selecting the "Forgot Your Password" link sometimes resulted in a blank screen.	1.6.0	25-Jul-2022
SPPLDEV-16191	On iOS devices, the date picker that is used to select dates for absences did not always behave as expected. The date picker has been updated to make it easier to select dates.	1.5.0	28-Jan-2022
SPPLDEV-16780	Empty fields are now hidden on the Work Details screen in the Sage People mobile app. This mirrors the behavior in the WX desktop interface.	1.4.3	6-Dec-2021

Issue reference	Description	Resolved in app version	Date
SPPLDEV-16774	Users were unable to edit their profile picture in the Sage People mobile app if there were no fields configured in the Work Details field set. Users without Work Details fields can now edit their profile picture in the app.	1.4.3	6-Dec-2021
SPPLDEV-16744	On iOS devices, files with an uppercase file extension did not open in the Sage People Mobile in-app browser. Files with uppercase extensions now open as expected.	1.4.3	6-Dec-2021

Limitations

The app currently has the following limitations:

- Booking part-day absences is not yet fully supported. When booking time off, fractional days can be manually set by entering them in the time off duration field.
- The app does not currently support users who are marked as having left the organization. An error message is shown to these users if they try to access the app.
- Rich text fields are not supported. If text fields are edited in WX with rich text formatting, the formatting is displayed as HTML in the app.
- Salesforce API limits apply to usage of the mobile app in your organization. These can limit the number of concurrent API requests that can be made, and the total number of requests per day. The app is designed to limit the number of API requests required by caching information in memory when appropriate. In practice it is not anticipated that API limits will have an impact on app usage. For more information, follow your standard Sage support process.