Oracle Field Service Cloud
Using Android and iOS Mobile Applications
## Contents

**Preface**  
| i |

**1 Using Oracle Field Service Cloud Mobile Application**  
| Overview | 1 |

**2 Install the Mobile Application**  
| Install Field Service Cloud Mobile for Android | 3 |
| Install Field Service Cloud Mobile for iOS | 3 |

**3 Configure the Mobile Application**  
| Configure Your Instance of Oracle Field Service Cloud Mobile | 5 |
| Simplified Login | 5 |
| Single Sign-On on the Mobile Application | 7 |
| Biometric ID Authentication | 8 |
| Face ID Authentication | 13 |
| Activate or Deactivate Coordinate Gathering | 16 |
| Conditions for Gathering Coordinates | 17 |
| Mobile Application Specifics | 17 |

**4 About Disabling Route Activation**  
| Overview of the Disable Route Activation Feature | 19 |
| Route Activation Messages | 19 |
| How to Enable Location Services in Android and iOS Devices? | 20 |
| Enable or Disable Route Activation | 22 |

**5 Use the Mobile Application**  
| Search Inventory with Barcode Scanner | 23 |
| Change the Name of Your Mobile Instance | 24 |
| Create Shortcuts to Mobile Instances | 24 |
| Troubleshoot Your Mobile Application | 26 |
Preface

This preface introduces information sources that can help you use the application and this guide.

Using Oracle Applications

To find guides for Oracle Applications, go to the Oracle Help Center.

Documentation Accessibility

For information about Oracle’s commitment to accessibility, visit the Oracle Accessibility Program website. Videos included in this guide are provided as a media alternative for text-based topics also available in this guide.

Contacting Oracle

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides. Please take one of the following surveys:

- For web-based user guide, Web-based User Guide Survey
- For tutorial feedback, Tutorial Survey
1 Using Oracle Field Service Cloud Mobile Application

Overview

The Oracle Field Service Cloud Mobile for Android application uses a native implementation of Oracle Field Service Cloud Mobility in the application. This application is enhanced to improve the collection of resource geocoordinates using their mobile device in near real-time. The Mobility option of the application is configured in the same way as Oracle Field Service Cloud Mobility.

You can use the mobile application to find the location and track the travel patterns of a mobile resource. The mobile application is available on Google Play services.

This section discusses how to download, install and run the mobile application on devices.

In case you use Mobile Device Management (MDM) software, you should modify the instructions in accordance with MDM software.

Your mobile device must satisfy the following criteria to run the Oracle Field Service Cloud Mobile application:

- The mobile application must support Android 6.0 or later
  
  ✍️ Note:
  
  - For the most recent Browser Support Policy, see Oracle Field Service Cloud Browser Support Policy

- Location services are available and enabled in High Accuracy mode (use GPS, WLAN and mobile network to determine location)

Security Notes

- Information Access — Oracle Field Service Cloud Mobile doesn't change customer or user sensitive information storage against existing secure storage which is implemented in Oracle Field Service Cloud.

- Authentication — The feature does not require any additional user authentication against authentication which is implemented in Oracle Field Service Cloud.

- Communication
  
  - The application uses https protocol for any communication out of device
  
  - Does not support self-signed certificates
  
  - Obtains access token using secured Oracle Field Service Cloud API

- Device Security
  
  - The application does not manage or control any security related device options and does not require any specific options
It is responsibility of client to set reasonable secure options of the device: set password for unlock device, encrypt device, disable any developer mode options, and so on.

It is responsibility of client to verify any security tools for compatibility with the application.

Hardware Notes

WiFi-only devices: Oracle Field Service Cloud
2 Install the Mobile Application

Install Field Service Cloud Mobile for Android

You can install Oracle Field Service Cloud Mobile Application from the Google Play Store.

Ensure that you are using an Android device with active internet connection and access to Google Play Store.

1. From your Android mobile device, open Google Play Store.
2. Search for Oracle Field Service Cloud Mobile and select it.
3. Click Install.

Now, you have downloaded and installed the Oracle Field Service Cloud Mobile App on your device.

You can use the procedure described above or you can download the mobile application directly from the following link:


Install Field Service Cloud Mobile for iOS

You can install Oracle Field Service Cloud Mobile Application from the Apple App Store.

Ensure that you are using an iOS device with active internet connection and access to Apple App Store.

1. From your iOS mobile device, open Apple App Store.
2. Search for Oracle Field Service Cloud Mobile and select it.
3. Click Install.

Now, you have downloaded and installed the Oracle Field Service Cloud Mobile App on your iOS device.

You can use the procedure described below or you can download the mobile application directly from the following link:

Chapter 3
Configure the Mobile Application

Configure Your Instance of Oracle Field Service Cloud Mobile

You should download and install the Oracle Field Service Cloud Mobile application from the Google Play Store.

To configure Oracle Field Service Cloud Mobile Instance:

1. Open the Oracle Field Service Cloud Mobile application.
2. Read and accept End User License Agreement.
3. Specify the Oracle Field Service Cloud Mobility instance to be connected.
4. In the instance name field (for example, sunrise or sunrise.test), enter the name of the instance you want to switch and then select OK.

▶ Note: You can use this approach only to configure application installed using MDM.

▶ Note: Do not include the 'etadirect.com' domain in the instance name field.

5. Enter login (username) and password.
You can also create shortcuts for the Oracle Field Service Cloud Mobile instances. Using the shortcut, you can open the Oracle Field Service Cloud Mobile and load the instances automatically.

To use this option, you need to create and download an XML file to the device. A sample XML file is explained below:

```xml
<?xml version="1.0" ?>
<instance>
  <name>Demo</name>
  <url>http://demo.etadirect.com/m</url>
</instance>
```

In the above sample,
- <instance> — root node
- <name> — child of <instance>, contains the Name of the shortcut to be displayed.
- <url> — child of <instance>, contains the URL of the Mobility instance.

Simplified Login

The field resources use the same instance most of the times to login to the installed application.

To reduce this effort of using the same series of steps to login to a particular instance every time, you can use the Mobile Device Management (MDM) option.
How to configure MDM?

A MDM system must be properly configured before using it to populate your instance details. It should also allow IT service to distribute the installed application to the end user’s devices. For more information, you should refer to MDM documentation. If you need specific MDM information, please contact your IT department.

Note: You can use this approach only to configure application installed using MDM.

Each platform (Android and iOS) allows the following set of configuration parameters:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Purpose</th>
<th>Type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance.url_X</td>
<td>URL of the instance</td>
<td>String</td>
<td>X can be any number from 1 to 5</td>
</tr>
<tr>
<td>instance.name_X</td>
<td>Instance friendly name</td>
<td>String</td>
<td>X can be any number from 1 to 5</td>
</tr>
</tbody>
</table>

To configure one access point, you need to set the fields as follows:

instance.url_1, instance.name_1

If only one access point is passed in Managed Configuration, it will be shown as plain text in the Instance name. In case of multiple access points, a drop down list will have all the instances.

How to use MDM?

In general, the field resource needs to provide the instance name and other details to access a particular instance. The MDM makes it easy by populating the last used instance for field resources. The user just needs to select and access the instance.

If there is more than one instance that the resource uses frequently, all such instances are listed under the Instance name drop down. You can select the required instance and access it.
Offline

If the field resource used a particular instance at least once, the instance availability check is done and if the device is online, the offline data is updated. When the device is offline, the field resource can continue to work by entering the PIN.

Single Sign-On on the Mobile Application

Similar to the OFSC, you can also use the Single Sign On technology in the installed application.

SP Initiated Login

Using the SP initiated login is same as described in the ‘Configure Oracle Field Service Cloud Instance’ section.
IdP Initiated Login

You need to follow the same procedure described in ‘Configure Oracle Field Service Cloud Instance’ section with a minor change. In step 4, you need to enter the url path to the IDP provider starting with https://. For example, https://sso.oracle.com/login.

Biometric ID Authentication

You can use fingerprint authentication or biometric id to login to the installed application.

Important: To use this feature, the mobile application must be installed on devices working on Android versions (7.0 or later) or iOS versions (10.0 or later). Also, the devices must have fingerprint scanners when Basic and / or LDAP authentication is used. This feature is not available for SSO users using either SAML or OpenId Connect.

For field technicians, it may be difficult to enter the password on their device when logging in every time. So, using the ‘Enable Touch ID’ (for iOS) or ‘Enable Fingerprint ID’ (for Android) option from the login screen makes it possible to access the installed application without having the need to enter the username and password during each login. The mobile application uses built-in operating system storage to store user credentials, which is secure.

How to configure this feature?

You need to follow the steps below to configure this feature:

1. From the hamburger menu, click Configuration.
2. Under Displays section, select Display.
3. Under General settings, select ‘Remember user name on Login screen or use Biometrics ID’.
4. Click Save.

You need to logout from the current instance and login again to use this feature.

In case you do not want to use fingerprint authentication, though the option is present in your mobile device, do not select the ‘Remember user name on Login screen or use Biometrics ID’ in Configuration section.

Disable Fingerprint Authentication

You can disable the fingerprint authentication on your device from the login screen. You need to clear the ‘Enable Touch ID’ or ‘Enable Fingerprint ID’ selection. For future logins, you cannot use this feature unless you select the ‘Enable Touch ID’ or ‘Enable Fingerprint ID’ option.

Use Biometric ID for Android Devices

You can use biometric id to login to your mobile application installed on Android platform.

To use biometric id option for Android devices, follow the steps described below:

1. Double-click and launch the installed mobile application.
2. Enter the instance name and click Next.
3. Enter username and password and select the ‘Enable Fingerprint ID’ option.
4. Click Sign In.

A Fingerprint dialog box to save and protect password is displayed.
If you want to save password, you need to put your finger on the device scanner and your username and password will be saved to your device operating system storage.

**Fingerprint Authentication**

**Confirm using your fingerprint**

Note: In case you have saved password using fingerprint id and changed or deactivated password from another application, an error message appears on the screen. You need to map new password with your fingerprint from the login screen again.

### Use Biometric ID for iOS Devices

You can use biometric id to login to your mobile application installed on iOS platform.

To use the biometric id option for iOS devices, follow the steps described below:

1. Double-click and launch the installed mobile application.
2. Enter the instance name and click Next.
3. Enter username and password and select the ‘Enable Touch ID’ option.
4. Click Sign In.

A Fingerprint dialog box to save and protect password is displayed.

If you want to save password, you need to put your finger on the device scanner and your username and password will be saved to your device operating system storage.
Note: In case you have saved password using fingerprint id and changed or deactivated password from another application (like browser—based Mobility or another mobile device), an error message appears on the screen. You need to map new password with your fingerprint from the login screen again.

Offline Mode Re-Authentication

You can authenticate again to log into the same session if your session goes offline.

If your session is offline because of connectivity issues or not being active for long time, you can re-authenticate using fingerprint id to log into the same session again.

You will be directed to the ‘Restore Session’, from where you can use fingerprint id to log into the installed application. If you do not want to use the fingerprint id authentication, click Cancel on the fingerprint id window on the Restore Session screen.

Android devices
iOS devices
Note: The fingerprint authentication appears on Restore Session screen only if you have mapped your credentials for fingerprint id authentication. Otherwise, you need to login by entering your password in the Restore Session window. This is applicable to mobile application installed on Android and iOS devices.

Passcode Login for iOS Devices

If you are using mobile application on a device working on iOS platform, and if the fingerprint authentication fails, you can use passcode to login to the installed application.

Sometimes you might not be able to login to the installed application because your finger print is not recognized after multiple attempts. In such case, you will have the opportunity to use passcode to login to the installed application.

Note: This option is not available for Android devices.
Face ID Authentication

Face ID Authentication for iOS Devices

You can use Face ID authentication on iOS devices to log in to the Installed Application.

To use the Face ID authentication on your iOS device, you must have installed the application in any of the following devices:

iPhone Models

- iPhone XS Max
- iPhone XS
- iPhone XR
- iPhone X

iPad Models

- iPad Pro 12.9-inch (3rd generation)
- iPad Pro 11-inch

How the Face ID Authentication Works?

On the Login screen, you will have the option to **Enable Face ID**.

If you select the option and confirm the permissions to use this feature, Face ID starts detecting your face.
If your face recognition fails, an appropriate message displays. You may cancel the process or try again.
After successful face recognition, you can log into the Installed Application. Your mobile device’s storage saves your password and the Face ID authentication protects it.

**Note:** You can view the buttons and messages displayed on Biometric ID screen translated and localized to all the supporting languages. This feature is available in both Android and iOS platforms depending on your OFSC Settings.

**Configure Face ID Authentication**

If you want to use the Face ID Authentication to login to the Installed Application, you must configure it.
To configure the Face ID, follow these steps:

1. Select Configuration from the Display screen.
2. Select the **Remember username on Login screen or use Biometrics ID** option.
3. Click **Save**.

Enable or Disable Face ID Authentication

You can enable or disable the Face ID Authentication from your Installed Application.

Enable or Disable Face ID Authentication

To enable the Face ID Authentication, follow these steps:

1. Select the **Remember username on Login screen or use Biometrics ID** option present on the Display screen.
2. Select the **Enable Face ID** option on the login screen.

**Note:** To disable the Face ID Authentication, clear the **Remember username on Login screen or use Biometrics ID** selection on Display screen.

Canceling Face ID Authentication

You can save the password using Face ID authentication and still not use it for future logins.

You can cancel the Face ID authentication by not showing the face in front of mobile device’s camera. In such a case, your Face ID authentication fails and you must authenticate your face again or Cancel the Face ID authentication.

Offline Re-Authentication Using Face ID

Sometimes, the Installed Application may periodically require you to log in again.

You must re-authenticate to login to the Installed Application. This could happen even if you are online or offline. If you have enabled the Face ID authentication, you can use it for re-authentication.

Activate or Deactivate Coordinate Gathering

You should download Oracle Field Service Cloud Mobile application using Google Play. The application is installed on the device and first run passed.

To activate or deactivate Coordinate Gathering:

1. Open the Oracle Field Service Cloud Mobile application.
   The application opens the Oracle Field Service Cloud instance that you specified previously.
2. Select **Activate Route**.
   The application starts collecting GPS coordinates.
3. Switch to another Android application and then switch to the Oracle Field Service Cloud mobile instance.
You will notice that the application continues to obtain GPS coordinates.

4. Select **Deactivate Route**.
   The application stops collecting GPS coordinates.

**Conditions for Gathering Coordinates**

This section discusses the conditions followed when the mobile application collects coordinates of mobile resources.

Once the route of the resource is activated, the Oracle Field Service Cloud Installed Application starts collecting coordinates.

Following conditions are true:

- Coordinates are collected only if the mobile resource is logged into the Oracle Field Service Cloud Installed Application and the route is activated.
- Coordinates are collected continuously regardless of whether Oracle Field Service Cloud application started, stopped, or the mobile device is locked.
- Coordinates are provided continuously when internet connection is active.
- Coordinates gathering is stopped when the mobile resource logs out from Oracle Field Service Cloud Installed Application or when the route of the mobile resource is deactivated.

**Important:** In case, the mobile resource does not deactivate the route, coordinates gathering is automatically terminated within two hours after working hours.

**Mobile Application Specifics**

Using Field Service Cloud Properties

When using File Property with GUI type ‘Image’, the camera opens automatically and there is no possibility to select an existing image from the gallery. If you want to select an image from the gallery, the File Property with GUI type must be set as ‘File’ and not as ‘Image’.

Saving Username

You cannot save passwords in the Mobile Application because of security reasons. However, you can save the username in Mobile Application.

To save the username, you need to access Display Settings from the Configuration section of your Mobile Application. You need to select the ‘Remember User Name on Login Screen’ option. Selecting this option saves your user name and populates it automatically, when you use the same device and browser to log into the application. This feature is available only for users who have the Internal and LDAP login policies, and not for users who have the SAML or OpenID Connect policies. If your authentication fails, your user name doesn’t get populated when you try to login to the mobile application next time.
4 About Disabling Route Activation

Overview of the Disable Route Activation Feature

You can prevent a resource from activating their Route if they are not sharing their location (GPS) data.

You can configure this option using the Disable route activation if geolocation is not enabled on device option in the User Type – Permissions under Enable GPS Telemetry.

Route Activation Messages

If the Route Activation feature is enabled and the user is not sharing their location, a warning message will appear instead of the Route Activation screen.

Accessing using the web browser

<table>
<thead>
<tr>
<th>Platform</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>To activate route in iOS</td>
<td>Route Activation requires your location. Please enable location access</td>
</tr>
<tr>
<td></td>
<td>in your iOS settings. To enable location services, go to Device Settings-Privacy-Location Services.</td>
</tr>
<tr>
<td></td>
<td>Route Activation requires your location. Please enable location sharing on your device. Once enabled, refresh the browser page and “allow” location access when requested.</td>
</tr>
<tr>
<td>To reactivate route in iOS</td>
<td>Route Reactivation requires your location. Please enable location access in your iOS settings. To enable location services, go to Device Settings-Privacy-Location Services</td>
</tr>
<tr>
<td></td>
<td>Route Reactivation requires your location. Please enable location sharing on your device. Once enabled, refresh the browser page and “allow” location access when requested.</td>
</tr>
</tbody>
</table>
Accessing using the Installed Applications:

For Android (Installed Application)

- 'Enable now' button will appear, tapping on it takes you to the Location services settings screen where you can enable the location services quickly.

For iOS (Installed Application)

- Extra message will be added to the warning text instructing you about how to enable location services: 'To enable Location services, please go to Device Settings - Privacy - Location Services'.

‘Cancel’ button simply navigates you back.

How to Enable Location Services in Android and iOS Devices?

If you have installed the mobile application on Android or iOS devices, you will get a notification to activate the route.

For Android devices:
For iOS devices:
Enable or Disable Route Activation

You can enable or disable Route Activation depending on your user type.

Follow these steps to enable or disable route activation:

1. From the **Configuration** page, select the desired user type from the **User Types** option.
2. Select **Enable GPS Telemetry** option present under the **Permissions** section.
   
   Within that option, **Disable route activation if geolocation is not enabled on device** must be visible and not selected. If you select this option, the Activate/Reactivate Route options will not work on the OFSC application and you have to enable the location services on the mobile device.
5 Use the Mobile Application

Search Inventory with Barcode Scanner

You can use the Barcode Scanner button to search for inventory in the Oracle Field Service Cloud Mobile application.

**Note:** The Barcode Scanner button is available in the inventory search screen when using Oracle Field Service Cloud Mobile – the iOS and Android applications. The button is not available when using the browser-based Oracle Field Service Cloud Mobile application unless a plug-in is developed and configured.

In general, parts and equipment have barcodes printed on their package. The new Barcode Scanner button added to the Search field helps you to find a part or equipment without the need to type any text and tap the Search button. This feature allows the Barcode Scanner to scan the barcode and Search is run without the need to tap the button and populate the result.

The following figure shows the inventory search screen with the Barcode Scanner option:

To use the Barcode Scanner:

1. From the Resource Info screen, click any activity. The Activity details screen appears.
2. Click the Search button present on the screen. The Search by keyword text box with the barcode scanner appears on the screen.
3. Click the Barcode scanner button and place the mobile in front of the printed barcode on any of the packages. The barcode information is captured and the search is run.

All the relative inventory items will appear on the screen. You can select the required part or equipment and continue with your activity.

<table>
<thead>
<tr>
<th>Barcode Type</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR_CODE</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>DATA MATRIX</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>
Table: Barcode Types

<table>
<thead>
<tr>
<th>Barcode Type</th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPC_A</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>UPC_E</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>EAN_8</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>EAN 13</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>CODE_39</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>CODE_93</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>CODE_128</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>CODABAR</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>ITF</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>RSS14</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>PDF417</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>RSS_EXPANDED</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Change the Name of Your Mobile Instance

You can change/update the Oracle Field Service Cloud Mobile instance name. For example: Moving from a TEST name to a PROD name.

To change the Oracle Field Service Cloud Mobile Instance:

1. Open the Oracle Field Service Cloud Mobile application.
2. Navigate to the OFSC Mobility Instance page.
3. In the instance name field, enter the name of the instance you want to switch and then select OK.

Create Shortcuts to Mobile Instances

You can create shortcuts to open the Oracle Field Service Cloud Mobile app and load the desired Mobility instance automatically.

This option is supported in OFSC Mobile for Android only.

In order to create the shortcut, you must create and download the XML file on the device. The XML file contains the following content nodes:

- `<instance>` — *required*, root node
- `<name>` — *required*, child of `<instance>`, contains the Name of the shortcut to be displayed
- `<url>` — *required*, child of `<instance>`, contains the complete URL of the desired Mobility Instance

Example:
After downloading the XML file, launch it and select the OFSC Mobile app (Field Service) option. The Field Service option appears as shown below:

When OFSC app opens, it loads the Mobility instance specified the in the <url> node.

In addition, it creates the shortcut on the Mobile screen. When you click the shortcut button, the configured Mobility instance opens.
Troubleshoot Your Mobile Application

This section lists a set of troubleshooting steps for Oracle Field Service Cloud Mobile application.

1. Activity and Inventory is not updated in my instance
   - Check to see if the instances are the same (Mobile and Manage).

2. Coordinates were not gathered
   - Verify if the resource is logged in and their route is active
   - If using a Mobile Device Management (MDM) solution, ensure that the geolocation services are available.

3. Requirements when using MDM software
   - The application must not prevent a user from starting or launching of a web application.
   - Following Android permissions MUST NOT be blocked:
     - precise location (GPS and network based)
     - full network access
     - view network connections
     - run at startup
# Revision History

This document will continue to evolve as existing sections change and new information is added.

<table>
<thead>
<tr>
<th>Date</th>
<th>What’s Changed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2019</td>
<td>• Face ID Authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• About Disabling Route Activation</td>
<td></td>
</tr>
<tr>
<td>May 2019</td>
<td>• Biometric ID Authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Updated MDM information in Simplified Login section</td>
<td></td>
</tr>
<tr>
<td>February 2019</td>
<td>• Minor updates</td>
<td></td>
</tr>
<tr>
<td>August 2018</td>
<td>• About Conditions for Gathering Coordinates</td>
<td></td>
</tr>
<tr>
<td>February 2018</td>
<td>• Added new information related to iOS application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Added information related to Android application from Using Smart Location guide.</td>
<td></td>
</tr>
</tbody>
</table>