Field Service Mobile Security Guide

Salesforce, Winter '22

@salesforcedocs

Last updated: July 21, 2021

CONTENTS

FIELD SERVICE MOBILE SECURITY

Protect and safely store data that is gathered from the Field Service mobile app (Android and iOS).

The Field Service App is built with the Salesforce Mobile SDK. The Salesforce Mobile SDK provides a set of low-level services that include security and authentication to applications that are built using this framework.

For information about data protection regulations and Service Cloud, see Data Protection and Privacy.

EDITIONS

Available in: Salesforce Classic and Lightning Experience

The Field Service core features, managed package, and mobile app are available in **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions. Work orders are also available in **Professional** Edition.

Field Service mobile users need the **Field Service Mobile** user license to access the app.

Local Encryption at Rest

Encryption boosts the security of your customers' data and helps you comply with privacy policies, regulatory requirements, and contractual obligations. Shield Platform Encryption and Field Audit Trail are supported for the following fields on work orders, work order line items, and service appointments:

- `Description`
- `Subject`
- `Address` (`Street` and `City` only)

To encrypt these fields, add them to your Encryption Policy in Setup. The Subject and Address fields support both probabilistic and deterministic encryption, while the Description field supports only probabilistic encryption. If Field Audit Trail is enabled, you can set field history data retention policies for the fields whose data you want to retain.

Important:

- Encryption is not supported for the Latitude and Longitude fields, which could be used to pinpoint an address.
- When you encrypt a field, existing values aren't encrypted. Contact Salesforce for help with encrypting existing data.

Table 1: Offline Data

Salesforce App	Field Service App
Offline data is stored using Core Data, and encrypted using NSFileProtectionCompleteUntilFirstUserAuthentication. This authentication dictates how passcodes are exposed internally to access the offline data. The passcode for the offline data is removed from the local keychain when Salesforce is closed or running in the background. Salesforce offline data is only accessible when the app is open and in the foreground.	Data is stored using the Sqlcipher provider for Sqlite3. Cached data is purged based on a least-recently-used cache policy.

Table 2: Files and Attachments

Salesforce App	Field Service App
Files and attachments are stored on the device's file system in a double-encrypted format. The device's hardware encryption encrypts the files while the device is locked. In addition, Salesforce encrypts using an AES algorithm (128-bit block size and 256-bit key size). When the file is viewed, there's a temporary unencrypted copy kept on the file system (removed when the 'viewing' operation is complete).	Files are stored in an iOS sandboxed directory and are also encrypted by application encryption. While viewing, files are temporarily unencrypted in another sandbox directory, but are erased when the app is in the background or when the viewer is dismissed. Also, the temp directory is cleaned when the application is launched.

Table 3: Chatter Feed Data

Salesforce App	Field Service App
Feed data is stored using Core Data, and encrypted using NSFileProtectionCompleteUntilFirstUserAuthentication. This authentication dictates how passcodes are exposed internally to access the feed data. The passcode for the feed data is removed from the local keychain when Salesforce is closed or running in the background. Salesforce feed data is only accessible when the app is open and in the foreground. Also, the feed data storage is time-based. The feed cache purges items older than one week, unless the remainder of feed items is fewer than 25 items. Also feeds that have more than 500 items have their excess items removed.	All Chatter feed data is stored with the Sqlcipher provider for Sqlite3. Cached data is purged based on a least-recently-used cache policy. In addition, Feed functionality is provided by a shared component, which makes the experience on iOS and Android the same.

Server-Side Encryption at Rest

Salesforce provides encryption abilities for data at rest on the Salesforce servers. The Platform Encryption feature allows customers to create policies at the field-level to encrypt sensitive data. This feature supports custom objects, and a subset of standard fields on standard objects. As of the time of this writing, encryption is supported for some fields on the following standard objects: Account, Contact, Opportunity, Lead, Case, and Case Comment.

Custom fields on these or other objects can be encrypted assuming that they use data types that can be encrypted.

Encrypting Data in Transit

Data transmitted to and from the Salesforce server is protected using SSL. Authentication, access controls, and digital signatures are protected using SHA-256.

User Authentication

Salesforce App	Field Service App
the Salesforce mobile app supports certificate-based login, whereby the customer can push a unique certificate to the device using Mobile Device Management (MDM). The certificate can authenticate the user to Salesforce. Alternatively, Salesforce's Lightning Login feature has multifactor authentication from the Salesforce Authenticator app. The factors are: • What you have: The mobile device • What you are: If fingerprint biometrics is enabled on the device • What you know: if the device is enabled for PIN-based login. Lightning Login is only enabled on devices that have either PIN or fingerprint enabled.	Certificate-based authentication is a function of the Identity Provider. Files are stored in the application directory and are encrypted using application encryption. The files are decrypted while viewing and deleted after the view operation is complete. The directory is cleared when the user logs out.

Trusted IP Ranges

Logins to the Field Service mobile app can be restricted to specific trusted IP ranges, which is also true for the Salesforce mobile app. You can implement this using a Virtual Private Network (VPN) solution on mobile devices. After logging in to VPN, users can log in to the app. Afterwards, the user can log in to Salesforce.

Device Identification

Salesforce is piloting a new feature to track device fingerprints accessing the Salesforce services. The feature supports the ability to see who logged in with a particular device and to revoke access to specific devices.

Handling Sensitive Data

To prevent leakage of sensitive data, Salesforce apps support four settings to limit data exfiltration on a mobile device.

- **DISABLE_EXTERNAL_PASTE** : Allows users to copy-and-paste data *within the app*, but prevents users from pasting data copied from the app to other apps or OS features.

  Note: This feature does not work on Samsung phones (and other manufacturers of Android phones) where a custom clipboard implementation is used.

- **FORCE_EMAIL_CLIENT_TO** : If a user taps on an email action within the app, the user is directed to the email app specified in the attribute value.
- **SHOW_OPEN_IN** : Prevents users from opening files in applications outside of the app.
- **SHOW_PRINT** : Used to disable printing from within the app.

The following table shows the level of support for these features in the Field Service mobile app as well as the Salesforce mobile app.

Setting	Supported on Field Service Mobile	Supported on Salesforce Mobile
DISABLE_EXTERNAL_PASTE	✅ (Default: FALSE)	✅
FORCE_EMAIL_CLIENT_TO	❌	✅
SHOW_OPEN_IN	✅ (Default: TRUE)	✅
SHOW_PRINT	❌	✅

The Field Service Mobile app settings are non-restrictive by default. To change a setting from the default value, go to Setup. Enter *Connected Apps* in the Quick Find box, select **Manage Connected Apps**, then click the name of the Field Service connected app. Update the attribute from the Custom Attributes section on the connected app page.

Mobile Device Management

Salesforce provides an extra level of security compliance with the most popular Mobile Device Management (MDM) suites. Both Android and iOS, with an MDM, give you enhanced functionality for distribution and control over your users' devices. The enhanced security functions, when you combine Salesforce with an MDM, include certificate-based authentication and automatic custom host provisioning.

MDM	Supported on Field Service Mobile	Supported on Salesforce Mobile
RequireCertAuth	✅	✅
AppServiceHosts	✅	✅
AppServiceHostLabels	✅	✅
OnlyShowAuthorizedHosts		
ClearClipboardOnBackground	✅	✅