Swyft Mobile for Salesforce™

Administration Guide

Last updated: June 2019

Contents

Introduction to Swyft Mobile for Salesforce

If you're already using a CRM—and especially if you're already using Salesforce.com—you know that having your sales team equipped with a mobile CRM not only offers a degree of flexibility and commodity for the individual sales rep, but it is also a proven way to boost sales, increase productivity and company revenue. This data remains highly proprietary, however, is often regulated, and IT must ensure that mobile device applications are deployed and managed with the same or similar levels of compliance as other enterprise applications.

Swyft Mobile for Salesforce (SMSF) enables sales organizations to enjoy the user experience of the standard Salesforce mobile app, while giving enterprise IT the security and necessary control to meet regulatory requirements and protect critical company information on mobile device.

Enterprise Grade Mobile Data Security Beyond the Native OS

In fact, SMSF offers enhanced security above and beyond native OS protections, including separate app level encryption and authentication that ensures constant protection of Salesforce data, even if the device PIN is compromised.

At user login, SMSF performs advanced compliance checks, including jailbreak and root detection. User access is prevented whenever out-of-compliance conditions are encountered. Business data can be shared with other business apps, but not with personal applications. Administrators can configure SMSF users to connect to the Salesforce cloud directly or through the corporate network without requiring to connect to VPN on the device. This allows IT to leverage network-based security investments already in place to secure and monitor mobile SMSF traffic.

SMSF's advanced security features beyond native include:

- App-level encryption
- App-level authentication
- App-level lock and wipe
- Data path control
- Advanced mobile DLP
- Unique app-to-app secure data sharing
- Jailbreak and compliance policies
- Integration with secure email and browser access

SMSF Installation Prerequisites

Before deploying the SMSF application you will need:

a. an active Salesforce.com account appropriate for your enterprise
b. an active Swyft Mobile for Salesforce enterprise subscription
c. BlackBerry Dynamics Servers
    - BlackBerry UEM or Good Control v.1.9.x.x or later
    - Good Proxy v.1.9.x.x or later
    - the Collaboration Edition of the BlackBerry Enterprise Mobility Suite

For complete instructions for preparing the UEM or Good Control database, please contact BlackBerry Support or visit BlackBerry UEM Product Troubleshooting and Support.

For Swyft Mobile for Salesforce Support, please contact your assigned Swyft Mobile for Salesforce technical contact. A dedicated technician is assigned for each enterprise Trial, Proof-of-Concept and Deployment.

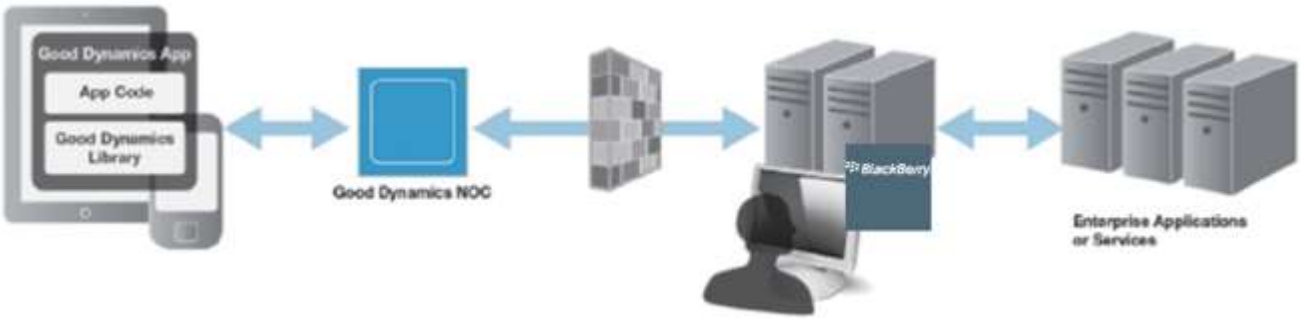
For customer service and support for the Salesforce mobile app, please contact your Salesforce representative or visit Salesforce Support Services.

For help or support with any BlackBerry products and services, contact your BlackBerry representative or visit BlackBerry Customer Support and Services.

Understanding BlackBerry Dynamics

Pictured below, the BlackBerry Dynamics platform comprises three major components:

- **BD Runtime –** the implemented APIs that enforce user authentication, secure communications, and secure storage on both sides of the enterprise firewall.
- providing a secure communications infrastructure between the BD- enabled apps on the mobile device and the **BD Network Operation Center (NOC) –** BD enterprise servers you install behind the firewall.
- **BD Enterprise Servers –** the BD server components (standalone or clustered) installed behind your enterprise firewall, namely:
    - **BlackBerry UEM [and legacy Good Control (GC)]** and its management console providing dashboard visibility and management of your enterprise's users, proprietary applications, and associated security policies; and
    - **Good Proxy (GP)**, providing secure communications between the NOC and your proprietary application servers, those also located behind the firewall.



High-Level BlackBerry Dynamics Platform Infrastructure

Deploying the SMSF App

To deploy the SMSF application, download the app from the Blackberry Marketplace, access the administration console to configure SMSF Application Policies and provision users.

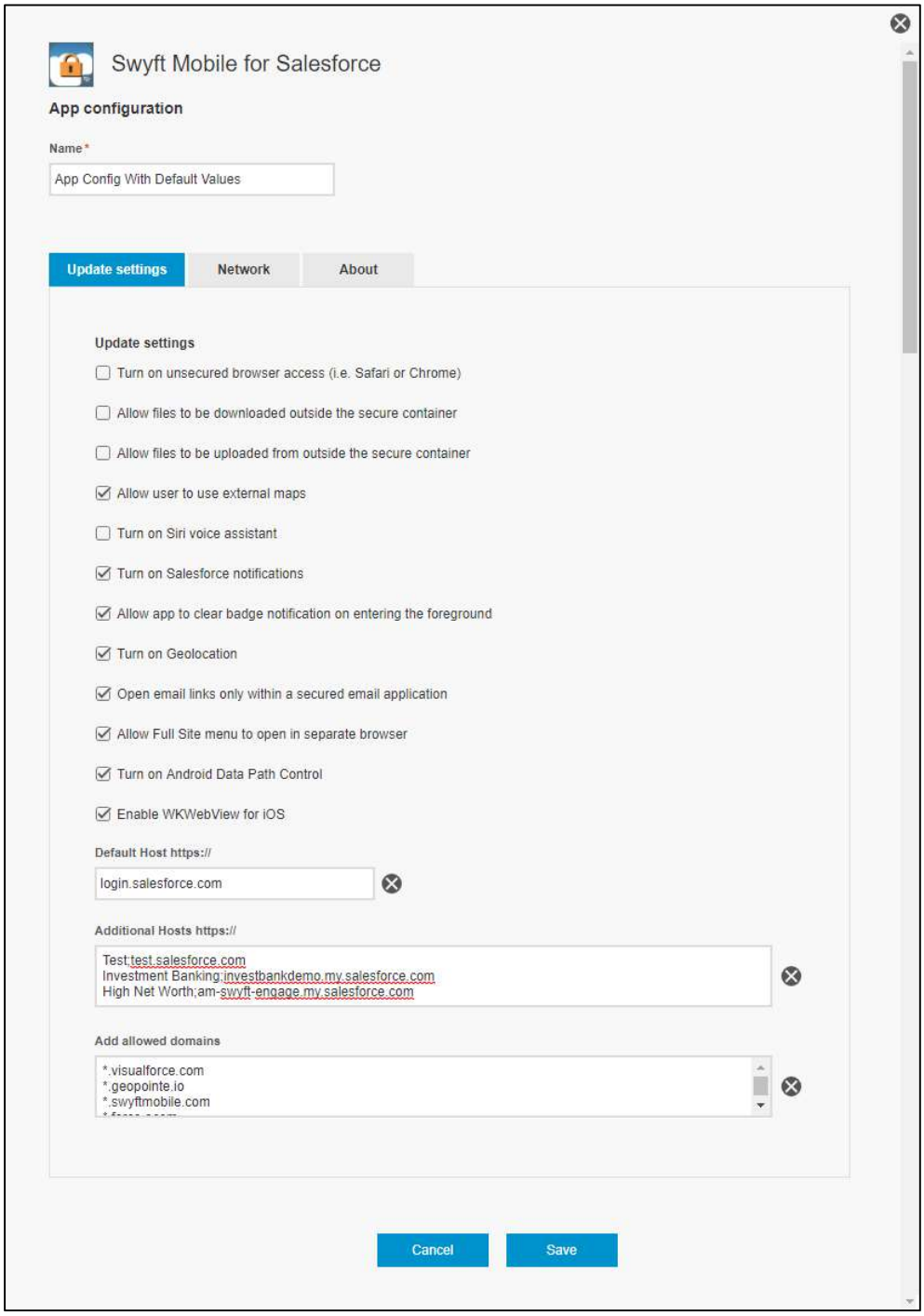
> Important: The SMSF application will not operate without the necessary BlackBerry Dynamics back-end software correctly installed and configured.

To view and manage the list of currently registered applications and deployed versions, click Manage Applications in the navigation panel on the left. The list of all applications in GC is displayed, make sure that SMSF is listed. If it is not, download it from the Blackberry Marketplace.

Configuring SMSF Policies and App Settings

To set or change SMSF application policies in UEM:

1. After opening UEM, click **Apps**, and scroll down to and select, **Swyft Mobile for Salesforce**.
2. In the application **Settings** menu, select the **App configuration** profile that you wish to edit.



SMSF Policies	Impact
Turn on unsecured browser access (i.e. Safari or Chrome)	Enables web site links in SMSF to open in an unsecured web browser on the device. If not checked, browser access will directed to BlackBerry Access.
Allow files to be downloaded outside the secure container	Allows files accessed from within inside the BlackBerry Container to be downloaded directly to the user's device
Allow files to be uploaded from outside the secure container	Allows files obtained from outside of the BlackBerry Container (files stored on the user's device) to be uploaded into the secure container
Allow user to use external maps	Enables map links within the SMSF application to open within mapping software. If not checked, map URL is blocked from within SMSF.
Turn on Siri voice assistant	Restricts the Siri voice assistant from interacting with the SMSF application (depending on which version the user is running)
Turn on Salesforce Notifications	Allow notifications from Salesforce to the SMSF app.
Alow app to clear badge notification on entering the foreground	Allows the app to hide or clear the badge notification when it enters the foreground of the user's screen
Turn on Geolocation	Allow SMSF to access mobile device location.
Open email links only within a secured email application	Enable email links within SMSF to open within BlackBerry Work. If not checked, emails will be opened outside of the container in the device's default email application.
Allow Full Site menu to open in separate browser	This allows the user to open the Salesforce full site from the application, which opens in the BlackBerry Access secure browser.
Turn on Android Data Path Control	Toggles on Data Path Control on Android. Regardless of the setting, the application always connects through BlackBerry Dynamics to access the Network Operations Center for application activation and application policy retrieval. When enabled, the application routes network traffic from the mobile device through the customer's internal network and into the Salesforce Cloud. This allows customers to enable Salesforce IP restrictions allowing access solely from the customer's network. When disabled, network traffic is encrypted over private/public WiFi or public telecommunication networks.
Enable WKWebView for iOS	This toggles on the WKWebView on the iOS operating system, as opposed to the older UIWebView. By default the UIWebView is enabled for backward compatibility, but we recommend enabling the WKWebView and testing in your Orgs to ensure there is no impact to your custom development. The WKWebView imparts increased performance in rendering content and accepting touchscreen input.

For modifying the default login URL or configuring multiple login URLs, the following is the naming convention/schema for entering URLs into the SMSF settings menu: **Label Name;URL String;Authentication Override**

Label Name is the user friendly label that appears in the Swyft Mobile for Salesforce login URLs menu accessed by pressing the gear icon (screenshot shown below). URL String refers to the URL utilized by the SMSF app to access Salesforce. Authentication Override, if applicable, can be entered as the THIRD parameter entered in a setting line to force whether "Kerberos" or "NTLM" is to be used as the authentication method.

Examples

Label Name;URL String;Authentication Override

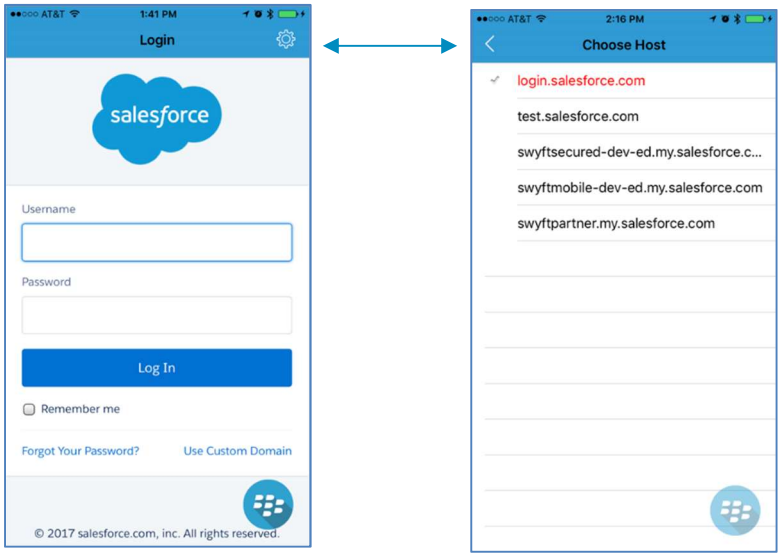
login.salesforce.com

UAT Testing Environment;test.salesforce.com

Investment Banking;invest.login.salesforce.com;Kerberos

Default host URL	Defines the default login page for Salesforce access.
Additional host URLs	Defines additional URLs that may be selected by the user for Salesforce access. One additional host is added per line. You will need to adhere to the naming conventions above.
Add allowed domains	This setting controls the behavior when a user clicks on a link in an SMSF custom tab: - Default setting is "*", meaning all domains are allowed for all links - If set to blank, then only *.salesforce.com and *force.com are allowed - Additional domains may be added, one domain per line When a user clicks a link in an embedded tab that is allowed, the link opens directly in SMSF. If the domain is not allowed by SMSF, the link is sent to BlackBerry Access if activated on the device; otherwise, the domain is blocked.

iOS users tap the gear icon on the Login screen to display a list of available Salesforce hosts:



Enabling Authentication Delegation

Delegation refers to the ability of a service to authenticate using multiple services. SMSF supports authentication delegation to and from BlackBerry Dynamics applications when configured to do so by a UEM or GC policy set.

Here, it is important to remember that policy sets apply to users, not applications. When a policy set specifies that authentication is delegated, this will apply to all applications run by end users assigned to that policy set.

To enable authentication delegation on GC:

1. Click Policy Sets in the navigator and either select an appropriate policy set or create a new one.
2. Directly below **Prevent Data Leakage**, turn on (check) **Delegate authentication to application**, then select the application to which you are delegating authentication.
3. Click **Update** to save your changes.

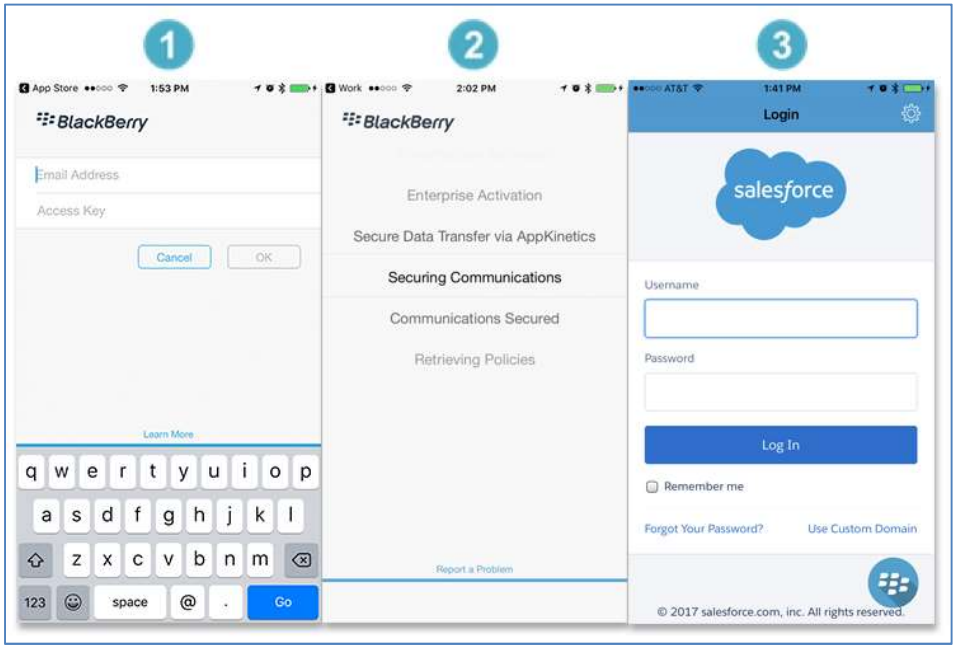
Important: The delegate must be a BlackBerry Dynamics application with the required build configuration, and the GD entitlement ID and version the delegate must be available in BlackBerry Dynamics.

Authentication delegation is backward compatible with any version of BlackBerry Dynamics that supports Enterprise SSO. The BD Runtime is coded to .sc to delegate authentication if the policy specifies BlackBerry Work as the delegate. From the client's point of view, the delegating application appears to be using the Enterprise SSO protocol.

For more complete instructions and a FAQ, please refer to BlackBerry Support.

Provisioning SMSF Clients and Easy Activation

When a user is ready to install and activate a BD application on their device, a provisioned access key must be entered when the user opens the SMSF app the first time. Via BlackBerry Dynamics, SMSF also supports a feature called Easy Activation. For more on this BD feature see the Easy Activation Feature Overview.

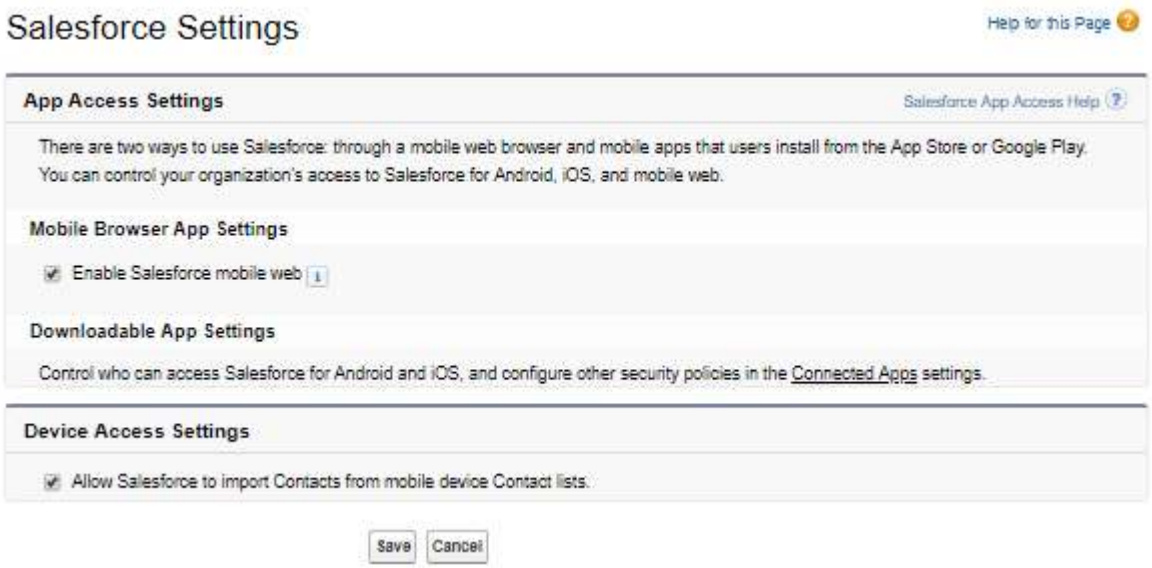


If Authentication Delegation is enabled, the Salesforce login screen is presented and access to the application is granted upon successful authentication. If your Salesforce account is configured with NTLM/Kerberos sign-on, a dialog will prompt for authentication. Enter your correct NTLM/Kerberos credentials.

Setting Salesforce to Enable Mobile Web

In order for the application to work properly, the Salesforce administrator must confirm that, in the Salesforce mobile app's menu in Setup, they've enabled mobile web.

Navigate to **Platform Tools > Mobile Apps > Salesforce > Salesforce Settings** and confirm that the **Enable Salesforce mobile web** box is checked.



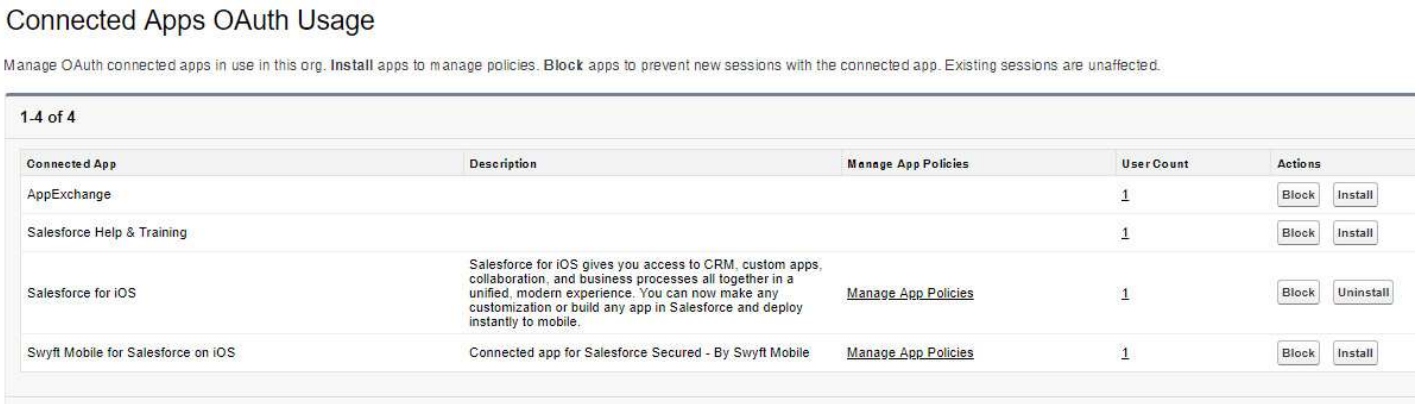
Setting up Connected App and Notifications

In order to set up Swyft Mobile for Salesforce's notifications you will need to set up Swyft Mobile for Salesforce as a Connected App within your Salesforce Org. If push notifications are NOT required for users, these steps can be ignored, and the application can be installed normally without push notifications. The connected app can be installed after the following:

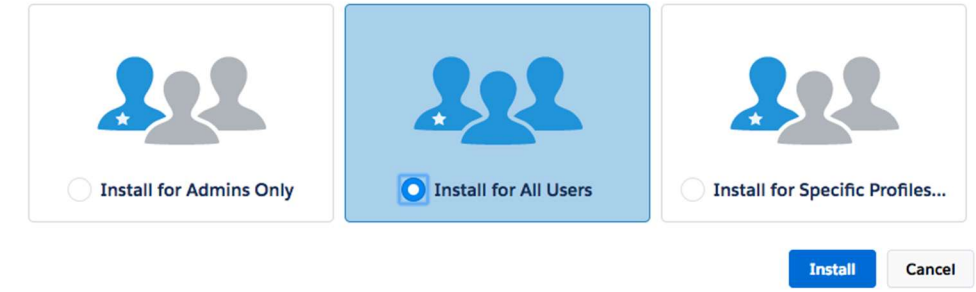
- The Swyft Mobile for Salesforce application has been deployed in your company's BlackBerry Dynamics configuration
- A policy set has been applied to a given user from UEM or GC
- The given user has been activated through their provisioned access key or Easy Activation
- The given user has signed into Salesforce using their credentials

Once a user has accessed Salesforce from the SMSF mobile app on either iOS or Android, the Swyft Mobile for Salesforce connected app package can be easily installed from within the admin's Salesforce setup menu.

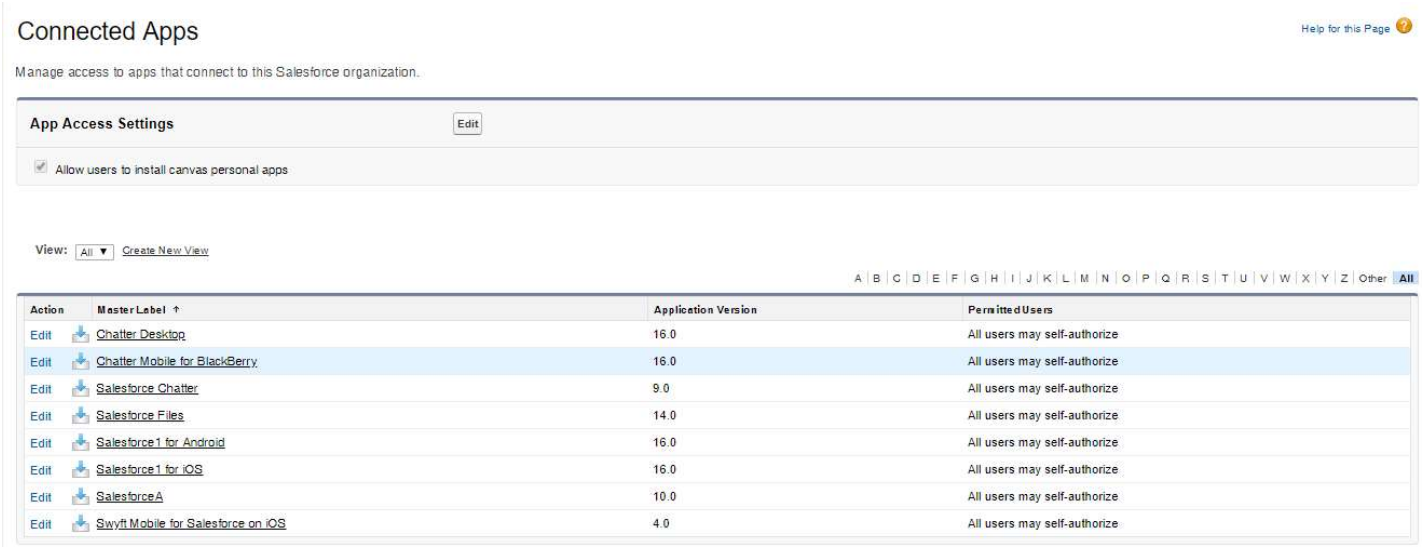
1. Navigate to the **Connected Apps OAuth Usage** menu.



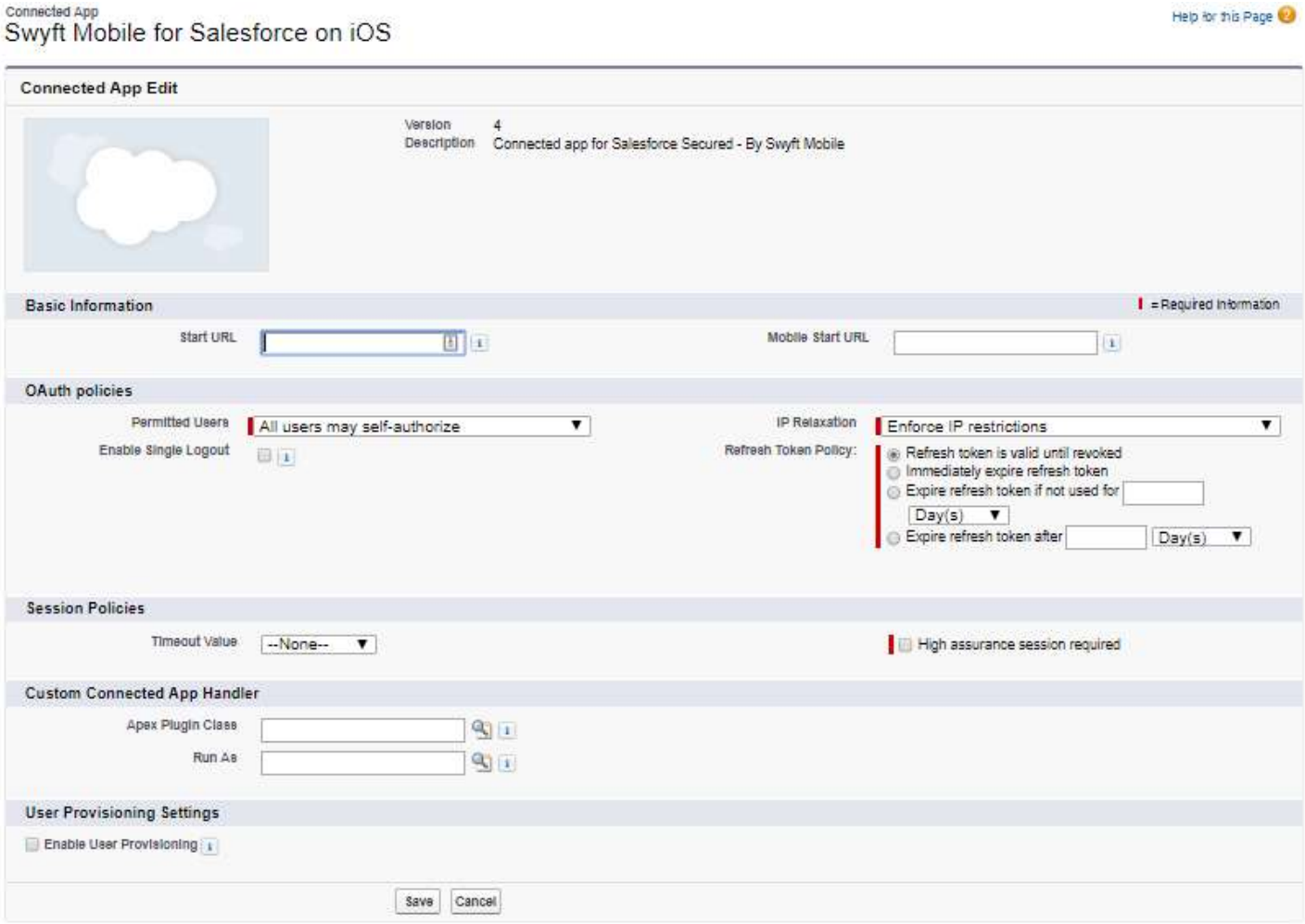
2. Select **Install** to the right of the Swyft Mobile for Salesforce connected app. Then select **Install for All Users**.



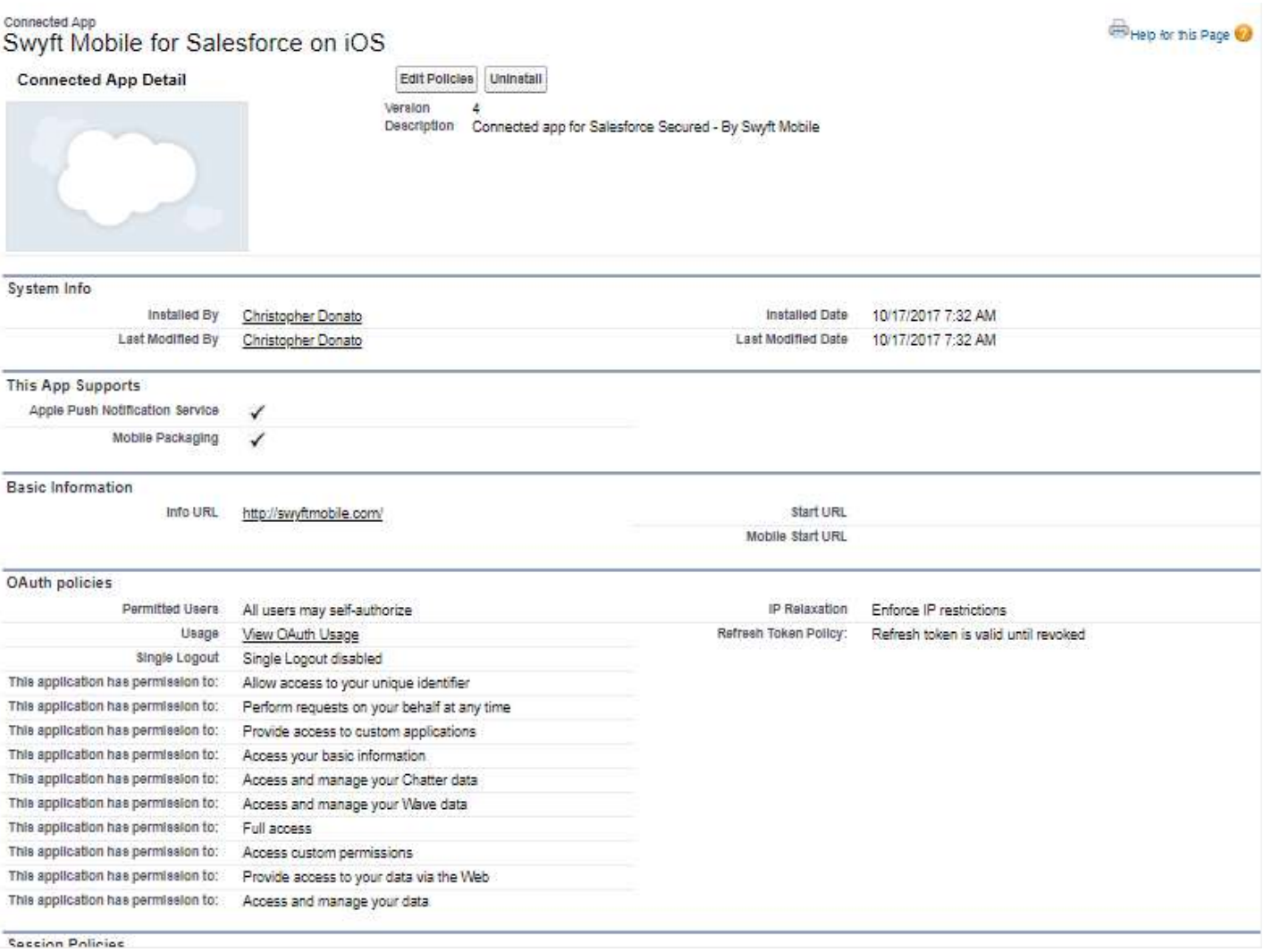
3. Navigate to the **Manage Connected Apps** menu. Then click edit on **Swyft Mobile for Salesforce**.



4. Edit the settings as appropriate in the Swyft Mobile for Salesforce policy, such as **Permitted Users**, **All users may self-authorize and IP policy**. Should you experience any problems wherein users are prompted with error messages associated IP Address issues, you have the option to **Relax IP restrictions for activated devices** from this page as well.



5. A view of all settings

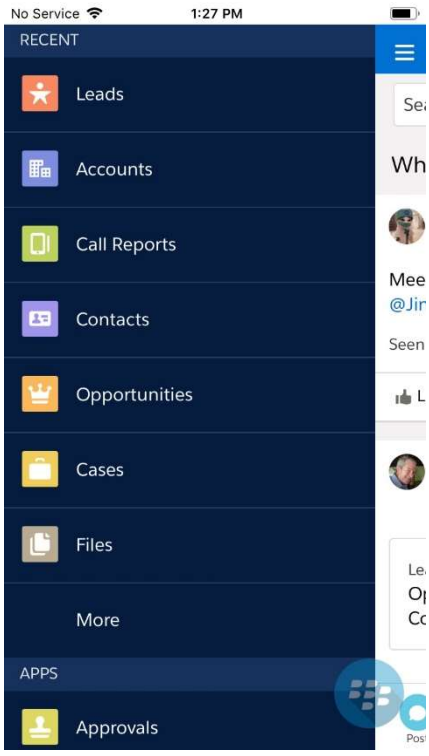


The Swyft Mobile for Salesforce app will now support standard Salesforce mobile app notifications. Additional notifications can be configured using triggers within the admin's Salesforce setup menu.

Salesforce Navigation Menu

Swyft Mobile for Salesforce inherits the configuration settings for the Salesforce Navigation Menu directly from Salesforce itself. The objects and applications that a user has access to within Swyft Mobile for Salesforce are congruent with Salesforce Mobile (Salesforce1). Users' access to Salesforce features are managed in the Salesforce Admin console in "Profiles," which can be found by searching using Quick Find. In Profiles, ensure that each user has the objects that you wish them to access Checked in the "Standard Object Permissions" and in the "Custom Object Permissions" section of the user's respective Salesforce user Profile.

The Swyft Mobile for Salesforce Navigation Menu can also be configured in Salesforce Admin in "Salesforce Navigation." In Salesforce Navigation, ensure that the items you wish your users to access are in the Selected column (it is also recommended that the Smart Search Items item is put in the Selected column as well). Please note that the "Salesforce Today" mobile navigation item will be unavailable in Swyft Mobile for Salesforce because this particular navigation item pulls in elements outside of the BlackBerry Dynamics security container.



Managing Salesforce Sessions, Timeouts, & Tokens

Upon signing into a respective Salesforce org, each user is assigned a session token that governs their access rights to their Salesforce environment and the duration of inactivity that the user has before their access times out.

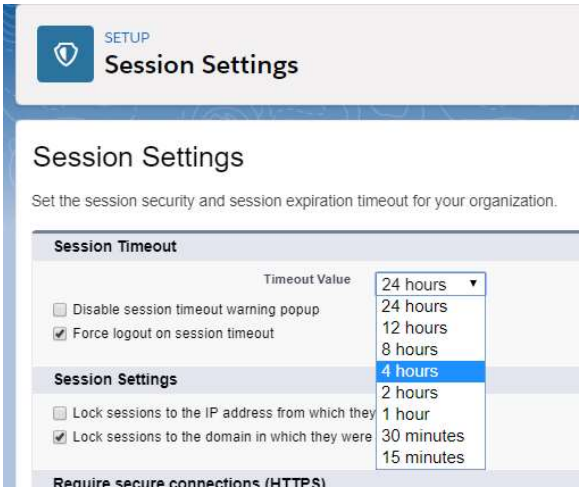
In addition to session tokens, Swyft Mobile for Salesforce also uses what's called "refresh tokens" to allow the users to access the app multiple times after their initial login without having to manually login each time.

Tokens, sessions, and timeouts are managed in the Salesforce Setup Menu for admins in the following locations:

Session Settings (manages on the org-level)

In the "Session Settings" menu in Salesforce Setup (Settings>Security>Session Settings), the "Session Timeout" section contains toggles that manage the nature of timeouts for all users across the entire Salesforce org.

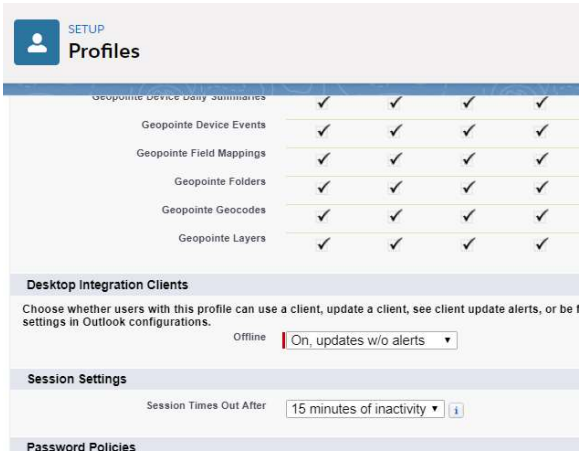
- Timeout Value
    - This dropdown field controls the time duration of inactivity before an inactive user session expires
    - This timeout will occur regardless of whether the Swyft Mobile for Salesforce application is running in the foreground or in the background on the user's device
- Disable Session Timeout Warning Popup
    - When this is toggled off, a popup box will appear on the user's screen notifying a user that their session will expire shortly, giving them the option to keep working or to let their session expire. Toggling this setting on disables to the popup.
- Force Logout on Session Timeout
    - Pushes the user back to the Salesforce login screen upon the expiration of a session
    - Do not toggle on "Disable Session Timeout Warning Popup" when using this toggle



User Profile Session Settings (manages on the user-level)

In a user profile's settings menu in Salesforce Setup (Administration>Profiles>[select a profile]), the "Session Settings" section allows you to change the length of an inactive session on a user basis.

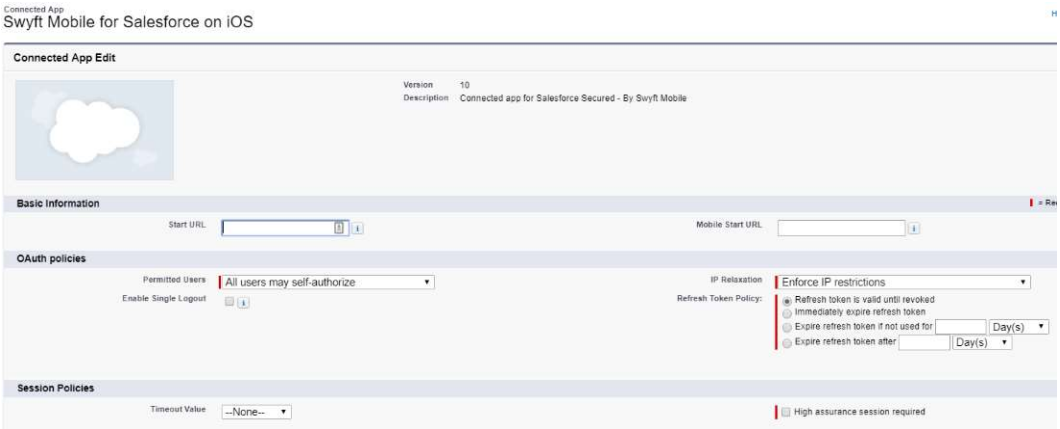
- Session Times Out After
  - This dropdown field controls the time duration of inactivity before an inactive user session expires
  - This timeout will occur regardless of whether the Swyft Mobile for Salesforce application is running in the foreground or in the background on the user's device
  - This value will override the Timeout Value assigned on the org-level in Session Settings



Connected App Refresh Tokens (manages on the org-level)

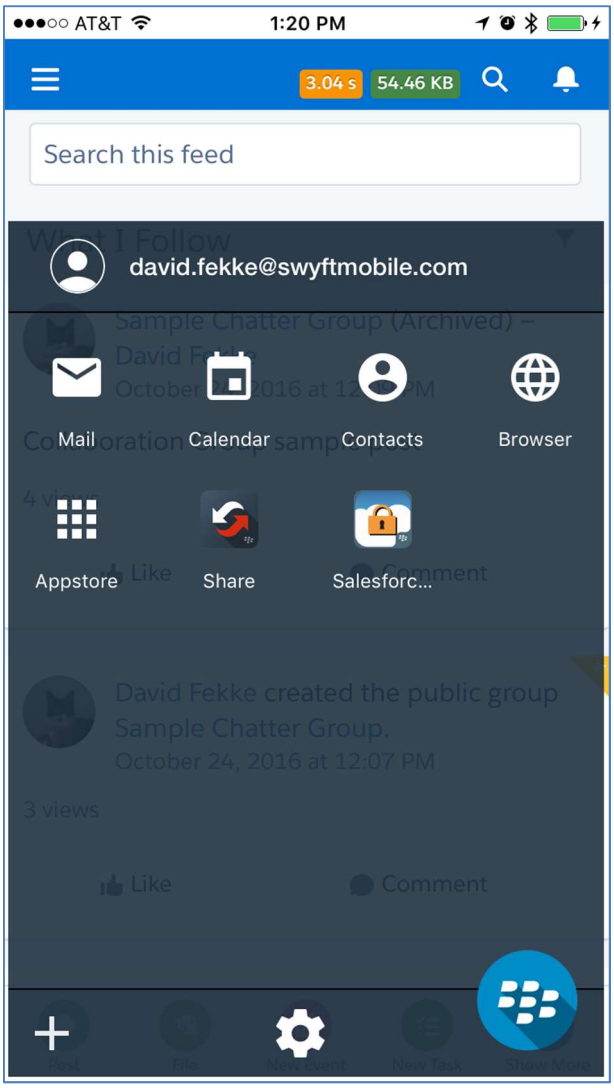
After the user's session expires or the application is closed, the user will need to either enter credentials manually or rely on a refresh token to automatically login to get back inside of their Salesforce Org.

In Swyft Mobile for Salesforce's connected app settings menu in Salesforce Setup (Platform Tools>Apps>Connected Apps>Manage Connected Apps>[Swyft Mobile for Salesforce on iOS *or* Swyft Mobile for Salesforce on Android]), the "Refresh Token Policy" field allows you to change the way in which the connected app refresh token is maintained. The refresh token can be set to expire anywhere from immediately to until manually revoked by the Salesforce administrator.



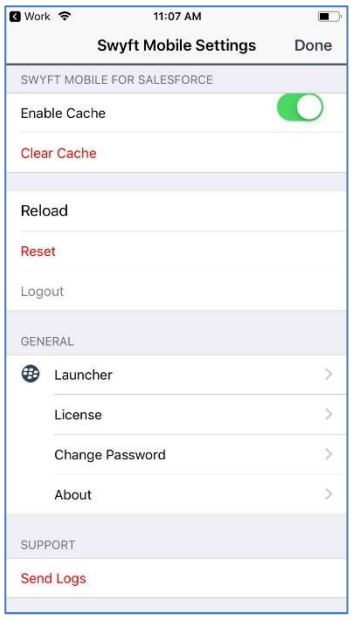
Using the BlackBerry Launcher

The Launcher can be accessed by tapping the blue BlackBerry bubble on the SMSF app screens. The Launcher allows the user to quickly switch between SMSF and any other BlackBerry Dynamics app on the device, as well as to move between Mail, Calendar, Contacts, and Chat (IM) in the BlackBerry Work app. The Launcher also gives the user access to Quick Create tools for email, contacts, and calendar events, along with access to their configurable BlackBerry application settings.



Application Settings

The user can tap the Settings icon in the BlackBerry Launcher to change available app settings:



SMSF Actions	Impact
Enable Cache	Enabling cache enhances application performance by saving static files on the mobile device, as well allowing caching for some read-only data files (e.g. recent contacts, tasks and opportunities)
Clear Cache	Removes all cached data on the mobile device, usually for troubleshooting purposes
Reload	Reloads the application content within the current view
Reset	Resets and effectively ends the current application view and creates a new connection and view
Logout	Logs out the user and displays login screen, where the user may choose a different custom host before logging into the application
Launcher	Controls opacity of the onscreen launcher button
License	Licensing information for SMSF
Change Password	Changes application password for the SMSF application (which is not the same as Salesforce desktop password)
About	Displays the version information for you application and copyright information
Send Logs	Sends diagnostic logs to your IT Administrator for troubleshooting purposes

Frequently Asked Questions

The most commonly asked questions about SMSF are answered here.

How is SMSF different than the standard Salesforce mobile app?

SMSF is different in a few ways:

- SMSF is a containerized version of the Salesforce mobile app built on the BlackBerry Dynamics Secure Mobility Platform. BlackBerry Dynamics provides app-level security controls that enables IT to protect critical customer data accessed from the Salesforce cloud or stored locally in the Salesforce app on the device and enforce the mobile security controls required to meet regulatory requirements, prevent data leakage, and confidently accelerate mobile CRM programs.
- Integrates BlackBerry Work, as all email address links only open into BlackBerry Work and all web links only open into BlackBerry Access.
- All other BlackBerry-secured apps, including ISV apps and internally built apps on BlackBerry Dynamics, can securely share data. This enables:
    - Addition of key stand-alone features lacking in the current MDM solution

        - Enforcing email links to open with contact information in BlackBerry Work
        - Enforcing web links to BlackBerry Work
        - Support of push notifications
    - Valuable integration enabling secure business workflows on the device
        - Integration with Blackberry WorkSpaces and other BlackBerry productivity tools
        - Secure app-to-app workflows with BlackBerry Inter-Container-Communication (ICC) services for dozens of productivity apps in the BlackBerry Marketplace
        - Integration with file repositories like SharePoint, Box and OneDrive
        - Document editing through Microsoft Office, PDF and .zip Support
        - Secured signature capture, printing, phone calls, instant messaging
        - Tighter integration BlackBerry contacts, emails and emails

Is the SMSF UX different than the standard Salesforce mobile app experience?

No, the user experience is essentially identical, including most functionality, customizations, AppExchange, and custom web apps that may be integrated into the Salesforce mobile app. These extensions work exactly the same in SMSF.

The only differences are:

- Email links and web links will initiate BlackBerry Work and BlackBerry Access, respectively, instead of the native email client and web browser (if BlackBerry Dynamics data leakage prevention is enabled).
- User may have to login to BlackBerry Dynamics if password timeout has expired
- There are a couple of Salesforce mobile app features that are not streamed from the cloud, but leverage the native calendar and file storage. These non-secure features are blocked by SMSF.
- SMSF supports Custom Host. This is not true SSO, but a SAML token that automatically authenticates the user.

How can I restrict a user from accessing CRM data using the native Salesforce mobile app that is in the App Store?

Your Salesforce administrator can block the native Salesforce mobile app from accessing your CRM data using the Salesforce admin console. These permissions are automatically inherited by SMSF.

Which specific security and container features are enabled?

- App-level encryption
- App-level authentication/password policies
- App-level lock and wipe
- Secure app connectivity via NOC and Proxy with no open inbound ports, DMZ, or VPN (iOS only)
- Data path control: option to use NOC or allow connection from device to SFDC cloud over carrier network (iOS only)
- Advanced mobile data loss prevention (DLP)
    - Restrict Open In to only BlackBerry-secured apps
    - Encrypt copies of documents created during Open In workflow
    - Obfuscate automatic OS screen shots
    - Prevent copy/paste between apps

    - Prevent iTunes backup of SMSF data
    - Prevent iOS 7 File Sharing to Facebook, Twitter, etc.
    - Prevent AirDrop of local SMSF data
- Unique app-to-app secure data sharing for secure workflows
- Jailbreak and compliance policies
- Integration with BlackBerry Work secure email and BlackBerry Access secure browser

Are BlackBerry Dynamics servers required?

BlackBerry Dynamics infrastructure is required, but it may be through either on-premise servers or through the BlackBerry Dynamics cloud services.

Revision History