Swyft Mobile for Saleforce$^{\text{TM}}$

Installation Checklist

Last updated: June 2018

Installation Checklist

Be sure to refer to this checklist to ensure that Swyft Mobile for Salesforce is set up properly. This checklist is also ideal for troubleshooting.

1. Deploy Swyft Mobile for Salesforce through BlackBerry Dynamics
    - □ Swyft Mobile for Salesforce or its trial has been installed from the BlackBerry Marketplace at https://apps.good.com/#/apps/519278971
    - □ The "Swyft Mobile for Salesforce" app is registered and appears within BlackBerry UEM or Good Control on your list of applications in *Manage Applications*
2. Configure *App Specific Policies* and settings in Good Control or UEM for Swyft Mobile for Salesforce
    - □ Under a user's policy set, navigate to *App Specific Policies*, and edit settings for Swyft Mobile for Salesforce to comply with your individual business needs
    - □ When setting up additional host domains or allowed (whitelisted) domains for the Swyft Mobile for Salesforce application, be sure that the URLs that you add do NOT have the "https://" or http://" prefix in the address
    - □ The changes to your policy settings have been applied to Good Control or UEM (note that, by default, updates to UEM policy settings take 24 hours to deploy to end-users)
3. Mobile access to Salesforce has been enabled in the Salesforce Setup menu
    - □ The toggle for *Enable Salesforce mobile web* is turned on. This is found (through the Lightning interface) by navigating to *Platform Tools* > *Apps* > *Mobile Apps* > *Salesforce* > *Salesforce Settings*
4. A user has been provisioned and has successfully downloaded and activated their application through BlackBerry Dynamics using one of these two options:
    - Easy Activation
        - □ A user is able to activate the Swyft Mobile for Salesforce application using another previously installed BlackBerry Dynamics application, like BlackBerry Work or BlackBerry UEM Client. The Authentication Delegation menu in UEM or Good Control can be used to assign applications which are able to delegate authentication for Easy Activation
    - Provisioned by Access Key
        - □ A user has accessed Swyft Mobile for Salesforce using an Access Key provisioned in BlackBerry UEM or Good Control
5. A user has logged into your Salesforce environment through one of two methods:
    - Standard login
        - □ The user has entered a Salesforce.com username and password and gained access to the Salesforce environment
    - Single sign-on (SSO) login
        - □ The user has accessed a Salesforce org using a username or password for a SSO service, which is configured as the login host in Swyft Mobile

6. Swyft Mobile for Salesforce connected app has been installed and configured in Salesforce, enabling push notifications
    - □ From the *Connected Apps OAuth Usage* menu in Salesforce Setup (found in *Platform Tools > Apps > Connected Apps* from Lighting), “Swyft Mobile for Salesforce on iOS” and/or “Swyft Mobile for Salesforce on Android” has been installed. The connected apps will be available for install in this menu after a user has been provisioned and logs into the application
    - □ The “Install for All Users” option was selected when the Swyft Mobile for Salesforce connected apps were installed
    - □ If users are having trouble accessing Salesforce within the application and are receiving error messages associated pertaining to their IP Address, the “Relax IP restrictions for activated devices” option can be set from the Swyft Mobile for Salesforce app menu from the *Manage Connected Apps* menu in Salesforce Setup
7. Deploy your team
    - □ Once you’ve completed these steps, you can provision and enable Swyft Mobile for Salesforce access to additional users across your team