*Using Salesforce1 with MobileIron*

December, 2015
Proprietary and Confidential
Do Not Distribute

## **Overview**

Salesforce1 is a brand new way to experience Salesforce from any device and brings all your Chatter, CRM, custom apps, and business processes together in a unified, modern experience for any Salesforce user. With the power of the Salesforce1 Platform, you can now customize and build any app and instantly deploy that functionality through the Salesforce1 app on iOS and Android.

The Salesforce1 client application communicates across the wireless network to provide a mobile experience for the broad set of Salesforce functionality. The client application or browser on the handheld device pulls feed data on demand to the device. This architecture provides a very high quality of service and a productive working experience for the end user.

Salesforce1 provides a sandboxed environment for a user to access Salesforce data from a mobile device, while an org administrator can manage user access, even if the mobile device belongs to the user.

IOS Bundle ID: com.salesforce.chatter ( when released )

## **App availability**

This app will be available in the Apple Store.

Salesforce1 app version 8.0 supports the EMM management functionality. The current release date for this version of the app is Late February.

If you are interested in trying out the app please contact your salesforce representative.

## **Device compatibility**

iOS : minimum supported version 7.0

## **App-specific configuration**

The following needs to be configured on your MobileIron Admin Console:

|  |  |  |
| --- | --- | --- |
| **Key** | **Description** | **Default if the key-value pair is not configured** |
| AppServiceHosts  | Data Type: String, String Array  | Login hosts. First value in the array is the default host. **iOS:** Doesn't require https:// in the host URL.  |
| AppServiceHostLabels  | Data Type: String, String Array  | Labels for the hosts. The number of AppServiceHostLabels entries must match the number of AppServiceHosts entries.  |
| ClearClipboardOnBackground  | Data Type: Boolean  | If true, the contents of the iOS clipboard are cleared when the mobile app is backgrounded. This prevents the user from accidentally copying and pasting sensitive data outside of the application.  |
| RequireCertAuth  | Data Type: Boolean  | If true, the certificate-based authentication flow initiates. **iOS:** Redirects the user to Safari for all authentication requests.  |

## **AppTunnel support**

If Salesforce1 is implemented to redirect authentication to a IdP such as SAML server that is deployed within the company firewall the app can use iOS per-app VPN technology to securely tunnel traffic.

Overview: <https://www.mobileiron.com/en/products/tunnel>

### **App Deployment**

### Enable MobileIron’s IOS Enterprise AppStore WebClip to be available to the registered device

 MobileIron Core Admin Portal -> Policied&Configs -> Configurations -> Select “iOS Enterprise AppStore” -> Assign “iOS” label to this WEBCLIP

### If the app is available in AppStore import the app into MobileIron Server.

MobileIron Core Admin Portal -> Apps -> App Catalog -> App Store -> Search for the app -> Import

NOTE: As mentioned Salesforce1 app is still not in production hence you would have to upload the ipa file manually using “Add in-house” app

### Assign a label

Select the imported app in the above step -> Actions -> Apply Label.

### **App Configuration**

The app configuration defines the app-specific parameters that are automatically pushed down to the app.

Use the following steps to configure the app-specific configuration:

On the Core Admin Portal, go to Policies & Configs -> Configurations -> Add New > iOS and OS X > Managed App Config.

Edit Managed App Configuration with the Name, Description, BundleId and select the external file (PLIST), that contains the App-specific key-value pair configurations required for the app.

**Note:** You can find the bundle ID for iOS apps by going to Apps > App Catalog, and clicking the hyperlink to edit the app. The bundle ID resides in the inventory field in parenthesis.

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

 <key>AppServiceHosts</key>

 <string>salesforceservername.com</string>

 <key>ClearClipboardOnBackground</key>

 <true/>

</dict>

</plist>

### **per-app VPN Configuration**

Configuration Details: <https://community.mobileiron.com/docs/DOC-3683>

### **Data Loss Prevention**

To prevent sensitive data from leaking outside the app the following controls are provided. In case of an app crash, the data will still remain on the clipboard (iOS only)

1. Copy/Paste – By using the salesforce provided key “ClearClipboardOnBackground”
2. Open-In – By using native OS capability.

MobileIron Core Admin Portal -> Policies&Configs -> Configurations -> Add New -> iOS and OS X -> Restrictions

* All documents from managed apps to unmanaged apps
* All documents from unmanaged to managed apps
1. Other MDM Security Controls

MobileIron Core Admin Portal -> Apps -> AppsCatalog-> Salesforce1 -> Edit

* Prevent backup of app data
* Remove app when MDM profile is removed
* Remove app when device is quarantined or signed out



### **Single Sign-On**

Salesforce1 app supports single sign-on by using iOS native safari capability to redirect the cert authentication to the SAML IDP server.

Supported solution

* Certificate based authentication to SAML IDP server
* Kerberos based authentication to SAML IDP server

The key “RequireCertAuth” is required.