Salesforce App and Intune

Prepared by Microsoft PM Jamie Silvestri (Jamie.Silvestri@microsoft.com)

The Salesforce App is a heavily used mobile app and many of our Intune customers are also Salesforce users. This document will address how Salesforce can work with Intune and the apps strong built in data protection policies.

Overview

Salesforce has emphasized supporting mobile configuration and data protection in their app. The following are examples of features and decisions they have made:

1. Put a strong emphasis on data protection within their application.
2. Added key configuration settings that are supported through app config settings for MDM enrolled devices (AppConfig).
3. Added controls in their admin platform to enable and disable features in their App – independent of AppConfig.
4. Support of OAuth and SAML for SSO.

Security compliance settings through MDM enabled App Config

The Salesforce app supports several configuration settings that can be passed through MDM app config channels. App config settings are supported on:

- iOS MDM enrolled device
- Android MDM enrolled device with a work profile (formerly Android for Work).

This is same requirement for all MDM vendors. While Intune/Microsoft is not a member of the AppConfig community, we do fully support any settings an application has made available through the iOS (Managed App Configuration) and Android (Managed Confgurations) platforms for pushing down configuration settings. Note: app configurations settings are not supported through MAM WE (because the device is unenrolled).

You can learn about Intune's support here:

1. Configure iOS apps with mobile app configuration policies
2. Android for Work app configuration policies

Salesforce supports the following configuration values:

1. Cert configuration
2. Custom host provisioning
3. Clipboard management

Below is an example of Salesforce configuration policy settings for iOS. The Intune admin would create a new Mobile App Configuration Policy and add this configuration.

```
<dict>
  <key>AppServiceHosts</key>
    <array>
      <string>host1</string>
      <string>host2</string>
    </array>
  <key>AppServiceHostLabels</key>
    <array>
      <string>Production</string>
      <string>Sandbox</string>
    </array>
  <key>RequireCertAuth</key>
   <true/>
  <key>ClearClipboardOnBackground</key>
  <false/>
  <key>OnlyShowAuthorizedHosts</key>
  <false/>
</dict>
```

Salesforce built in protections

Salesforce has strong data protection within their application and provides admins with options for additional constraints.

Data protection

Encryption of stored data: Salesforce provides encryption on both iOS and Android. Data kept on the device includes feeds which are stored in a database and attachments. iOS feed data is encrypted using standard iOS encryption and an AES-256 cypher. Attachments are encrypted using the platforms encryption. On iOS devices a secondary encryption is used to read the file. On the Android platform, device encryption is required.

Remote Wipe: The Salesforce admin can initiate a remote wipe of the application.

Inactivity Lock: Like the Intune PIN requirement, Salesforce allows the admin to set a requirement for an arbitrary password at launch or a defined period of inactivity.

Salesforce Connected Configurations

With version 11.0 or later Salesforce provides additional security and compliance configurations. These settings can be configured in the Salesforce site by and administrator.

- Specify which email apps can be used with Salesforce
- Disable open in functionality
- Disable print functions
- Disable external paste

Office Integration

Salesforce has worked with the office teams and built the Salesforce File Connect. Instead of adding attachments to Salesforce you link to the documents in SharePoint or OneDrive for Business using the file open APIs. This creates an environment where Office "attachments" are linked and stored in SharePoint or OneDrive for Business. Because these documents would be accessed through SharePoint or OneDrive they would be under the same DLP protections when you use those apps.

Detailed readings

- The Salesforce specific security information is captured in detail in the Salesforce Mobile Security Guide.
- Sales force mobile SDK information in the Salesforce Developer Documentation.
- SSO with Azure AD information in the Salesforce Developer Documentation.