. ɐı ›pic with navigation

You are here: Mobile SDK > Mobile SDK for iOS > Integrating with EMM providers > Integrating with MobileIron

Integrating MicroStrategy Mobile with MobileIron

You can use the MobileIron platform to add an extra layer of security to iPhones and iPads that are running MicroStrategy Mobile. Instructions for integrating MicroStrategy Mobile with MobileIron are provided below:

- Prerequisites
- Setting up the MobileIron Core Admin Portal environment
- Deploying MicroStrategy Mobile with MobileIron support

You can choose the combination of security policies and configuration that you want MobileIron to apply on your device. These policies and configurations can help the enterprise to manage the devices and data. There are three kinds of security policies available on MobileIron to help administrators prevent data leakage.

- Copy and Paste. This policy is used to allow/disallow users to copy/paste content from/to an app managed by MobileIron. When you disallow this policy, no data can be copied from or pasted to the app.
- Print. This policy is used to allow/disallow users to print content from an app managed by MobileIron. When you disallow this policy, no data can be printed in the app.
- Open in. This policy is used to allow/disallow users to open files in some specific apps managed by the MobileIron Core Admin Portal. The administrator can choose to allow users to open files in all apps, apps that are managed by MobileIron, or apps in a white list. The Open In policy manages all app interaction and data loss prevention features, such as applying URLs, opening files in third-party apps, and so on.

The level of security you choose for each option is determined by the stringency of the security requirements in your environment versus the need for less restrictive data transfer.

The following MicroStrategy features are not currently supported by the MicroStrategy Mobile app integrated with MobileIron.

- Collaboration
- Usher Integration
- Certificate Server
- Confidential Project

Prerequisites

The following are required to deploy the MicroStrategy Mobile application with MobileIron support.

- You must use an Apple Mac, running Xcode® 6.x with iOS SDK 8.x.
- Your organization must be enrolled in the iOS Developer Enterprise Program. For information about this program, visit the iOS Developer web site.
- You must create a wildcard App ID for your application, using the iOS Provisioning Portal. A wildcard App ID is of the form `[BundleSeedID].*`, where:
    - `BundleSeedID` is an alphanumeric code that is generated by Apple when you create the App ID.
    - The asterisk (*) is a placeholder for the Bundle Identifier of the App ID. The Bundle Identifier is used by iOS to identify the application on your device. To integrate with MobileIron, you accept the default value—`com.microstrategy.iPad` for an iPad app or `com.microstrategy.MSTRMobile` for an iPhone app.
- You must have a location on your network that users can access through their web browsers, using either HTTP or HTTPS protocol. The distributable archive of the application must be saved to this location.
- Depending on how you plan to provide users with the URL to the manifest file for the application, you may need to create a web page on your network where users can access the URL.

Setting up the MobileIron Core Admin Portal environment

To set up your MobileIron Core Admin Portal environment so users can install the MicroStrategy Mobile application with MobileIron support on their mobile devices, perform the administrative tasks listed below. For a detailed explanation of how to perform these tasks, refer to the MobileIron Core Admin Portal Admin Guide.

1. Register yourself on the official MobileIron web site.
2. Install your MobileIron Core Admin Portal.
3. Log in to the MobileIron Core Admin Portal and add MicroStrategy to the MobileIron managed apps.
4. Create your security policy set and security configurations for MicroStrategy Mobile, depending on your requirements.
5. Add the users in your organization who are allowed to use MicroStrategy Mobile.

6. Register the devices of the added users so that they can be notified to install the MobileIron app on their devices.

7. Create Labels on the MobileIron Core Admin Portal. A Label is a combination of security policies and configurations. Then apply these Labels to the users who share the same set of policies.

8. If you want to use the App Tunnel feature from MobileIron, you can configure the Sentry on the MobileIron Core Admin Portal. App Tunnel is a secure way for enterprise apps to access data behind the enterprise firewall. Once App Tunel and Sentry are configured, all access to the enterprise server goes through the Sentry and is protected by MobileIron.

Deploying MicroStrategy Mobile with MobileIron support

Use Xcode to configure and build your MicroStrategy Mobile application, and then use the iOS Enterprise Deployment process to install the application on your users' devices.

Once you have met the prerequisites and set up your MobileIron environment, do the following:

1. Download and install the MicroStrategy Mobile SDK integrated with MobileIron

2. Configure the MicroStrategy Mobile application

3. Create a distributable archive of the application

4. Upload and distribute the application

Note: For a list of supported iPhone and iPad devices and operating systems, see the MicroStrategy Readmes.

A detailed description of each step is provided below.

Note: The third-party products discussed below are manufactured by vendors independent of MicroStrategy, and the information provided is subject to change. For detailed instructions to perform the following tasks, refer to the iOS Developer Library.

1. Download and install the MicroStrategy Mobile SDK integrated with MobileIron

a. On a Mac computer, go to the MicroStrategy Download site and download the latest DMG file for the MicroStrategy Mobile SDK Secured by MobileIron. This includes the MicroStrategy Mobile Xcode project and a MobiileIron integration framework called the `MSIAppConnect.framework`. You must have a username and password to access the download site.

   Note: The latest Mobile SDK may or may not be the same version as the version of Intelligence Server you are using.

b. Double-click the downloaded DMG file.

c. Click **Agree** to accept the terms of the license agreement. This opens the disk image.

d. Copy all the folders to your local drive.

e. Eject the disk image.

2. **Configure the MicroStrategy Mobile application**

Make sure that you have created and installed the distribution certificate for MicroStrategy Mobile on your Mac and created and downloaded the distribution provisioning profile. Use the Keychain Access utility on your Mac and the iOS Provisioning Portal to create these files.

a. In the `MicroStrategyMobile` folder copied from the disk image on your Mac, double-click `MicroStrategyMobile.xcodeproj`. The MicroStrategy Mobile project opens in Xcode.

b. Choose either the **MicroStrategyMobileIPhone_AppConnect** or **MicroStrategyMobileIPad_AppConnect** scheme, depending on the type of device you are creating the application for.

c. Open the appropriate property list file—`Info_IPhone.plist` for iPhone or `Info_IPad.plist` for iPad.

d. Accept the default **Bundle Identifier** property—`com.microstrategy.iPad` for an iPad app or `com.microstrategy.MSTRMobile` for an iPhone app.

e. For the scheme you selected, make sure that your distribution provisioning profile is selected under Code Signing in the Build Settings section.

f. Add the `MSIAppConnect.framework` into the target that you want to build.

3. **Create a distributable archive of the application**

With the project still open in Xcode, do the following:

a. From the **Build** menu, select **Build and Archive**. An archived version of the application is built, with an `.ipa` extension.

b. Open Xcode’s Organizer window, select the archived application, and click **Share Application**. The Share Archived Application dialog box opens.

c. Click **Distribute for Enterprise**. The archive is built, and you are prompted to enter information for the application’s manifest file, which devices use to download the application.

d. In the **URL** field, enter the web address for the network location where users can download the application, in the format `http://`*`YourNetworkLocation`*`/`.

e. Close Xcode.

4. Upload and distribute the application

a. Copy the following files to the network location where users can download the application:

- The application archive (for example, `MicroStrategyMobile.ipa`).
- The manifest file (for example, `manifest.plist`).

b. To distribute the application, provide users with a URL to the manifest file, using the following syntax:

```
itms-services://?
```

You can provide this URL in an email or on a web page that users can connect to.