Using Symphony with MobileIron

February 26, 2016
Proprietary and Confidential
Do Not Distribute

Overview

Secure messaging for businesses, teams and workgroups. Increase productivity without compromising the confidentiality of your conversations. Symphony is designed to the highest security and regulatory standards – notably to satisfy the needs of leading financial institutions - and is now available for businesses of all sizes.

iOS: com.symphony.mobileiron
PlayStore: com.symphony.android

App availability

iOS: https://itunes.apple.com/us/app/symphony.com-for-mobileiron/id1138896543
PlayStore: https://play.google.com/store/apps/details?id=com.symphony.android

Device compatibility

Minimum OS Version

iOS 8+
Android 4.4

App-specific configuration

Key	**Description**	**Default if the key-value pair is not configured**
pod_domain	The domain name of your pod. (In version 1.43+ this value is unused.)	<blank>

enable_photo_picker	Set to false to prohibit attaching photos from camera roll to messages sent within the application.	true
enable_webview	Set to false to prohibit viewing non-image attachments and URLs sent within the application.	true
enable_sharing	Set to false to prohibit users from sharing image attachments to other applications through OS installed share extensions.	true
enable_crash_reporting	Set to false to prohibit the recording of crashes for later analysis.	true
enable_analytics	Set to false to prohibit recording anonymous usage statistics.	true
enable_addressbook	Set to false to prohibit using OS Address Book to invite new contacts to application.	true
enable_copy	Set to false to prohibit users from copying the contents of messages.	true
enable_network_debugging	Set to true to emit logging for debugging network-related issues.	true
disable_pin	Set to true to hide the built-in Pinched feature.	true
disable_introduction	Set to true to automatically skip the first-launch introduction screens	false
disable_sso	Set to true to prevent logging in through SSO	false

AppTunnel support

The app will need to interact with internal servers over https (port 443). These servers are the pod and the key manager.

Data loss prevention policy support (iOS SDK apps only)

The app prevents copy/paste through the "enable_copy" App-specific configuration key.

Secure file I/O support (iOS SDK apps only)

The app uses secure I/O when storing files to the disk.

AppConnect and non-AppConnect mode support (iOS SDK apps only)

The app can be used in AppConnect mode or non-AppConnect mode. There is no user-interface to switch between these modes. To switch from AppConnect to non-AppConnect, you will need to remove the device from management mode. To switch from non-AppConnect to AppConnect mode, you will have to register the device with the MobileIron servers and then quit & relaunch the application.

Configuration tasks

Use the following high-level steps to configure AppConnect for the app.

1. Enable AppConnect.
2. Configure an AppConnect global policy.
3. Configure a new AppConnect app configuration for the app.
4. Configure a new AppConnect container policy for the app.

Enable AppConnect

Before enabling AppConnect on your Core, confirm that your organization has purchased the required AppConnect licenses. Contact your MobileIron representative if you require additional details on AppConnect license purchases.

To enable AppConnect and AppTunnel functionality on the Core, navigate to the Settings page on the Core Admin Portal and check the boxes as shown below.

1. Select the option for “Enable AppConnect for third-party and in-house apps”.
2. Select the option of “Enable AppTunnel for third-party and in-house apps”.

Configure an AppConnect global policy

An AppConnect global policy configures the security settings for all AppConnect apps, including:

- Whether AppConnect is enabled for the devices that the policy is applied to

- AppConnect passcode requirements.

  Note: The AppConnect passcode is not the same as the device passcode.

- out-of-contact timeouts
- the app check-in interval

  Note: The app check-in interval is independent of the MDM check-in timer and controls, and apps cannot be forced to check-in before the interval expires. The recommended configuration for the app check-in interval is 60 minutes.

- the default end-user message for when an app is not authorized by default
- whether AppConnect apps with no AppConnect container policy are authorized by default
- data loss prevention settings

To modify an existing AppConnect global policy:

1. On the Core Admin Portal, go to Policies & Configs > Policies.
2. Select an AppConnect global policy.
3. Click Edit.
4. Edit the AppConnect global policy based on your requirements.

   See the AppConnect and AppTunnel Guide for details about each field.

Configure a new AppConnect app configuration

The AppConnect app configuration defines the app-specific parameters that are automatically pushed down to the app, as well as configurations for establishing and authenticating an AppTunnel associated with the app. See the AppConnect and AppTunnel Guide for details about each field.

Also, for more on AppTunnel configuration, see “Adding AppTunnel Support” in the AppConnect and AppTunnel Guide.

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

1. On the Core Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > App Configuration.
2. Edit the AppConnect app configuration with the Name, Description, Application, AppTunnel configuration including the identity certificate, and App-specific key-value pair configurations required for the app.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Catalog, and clicking the hyperlink to edit the app. The bundle ID resides in the Inventory field in parenthesis.

3. AppTunnel: Click on the “Add+” button and enter the AppTunnel details. The AppTunnel service for this app must be pre-configured in order to use it here.

4. App Specific Configuration: Click on the “Add+” button to enter the key-value pair information.

Configure a new AppConnect container policy

An AppConnect container policy specifies data loss protection policies for the app. The AppConnect container policy is required for an app to be authorized unless the AppConnect global policy allows apps without a container policy to be authorized. Such apps get their data loss protection policies from the AppConnect global policy.

Details about each field are in the AppConnect and AppTunnel Guide.

To configure an AppConnect container policy:

1. On the Core Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > Container Policy.
2. Enter the Name, Description, and Application.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Catalog, and clicking the hyperlink to edit the app. The bundle ID resides in the Inventory field in parenthesis.
3. Configure the data loss protection policies according to your requirements.