Quick Start Guide - Symphony for MobileIron

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: Request the apk file from Symphony

Device compatibility

Minimum OS Version

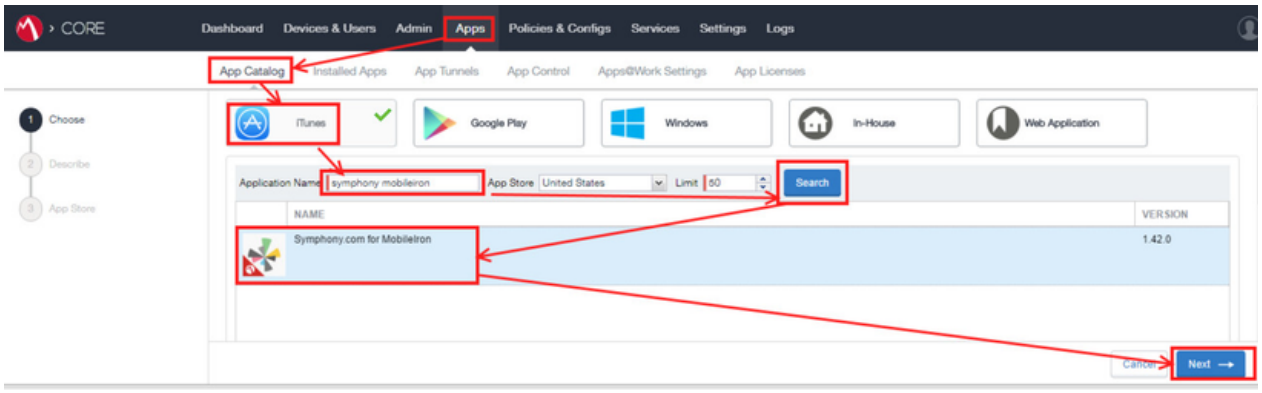
iOS 8+
Android 5.0

Administrator - Configuring the MobileIron server for the Symphony for MobileIron App

1. Add Symphony to your App Catalog

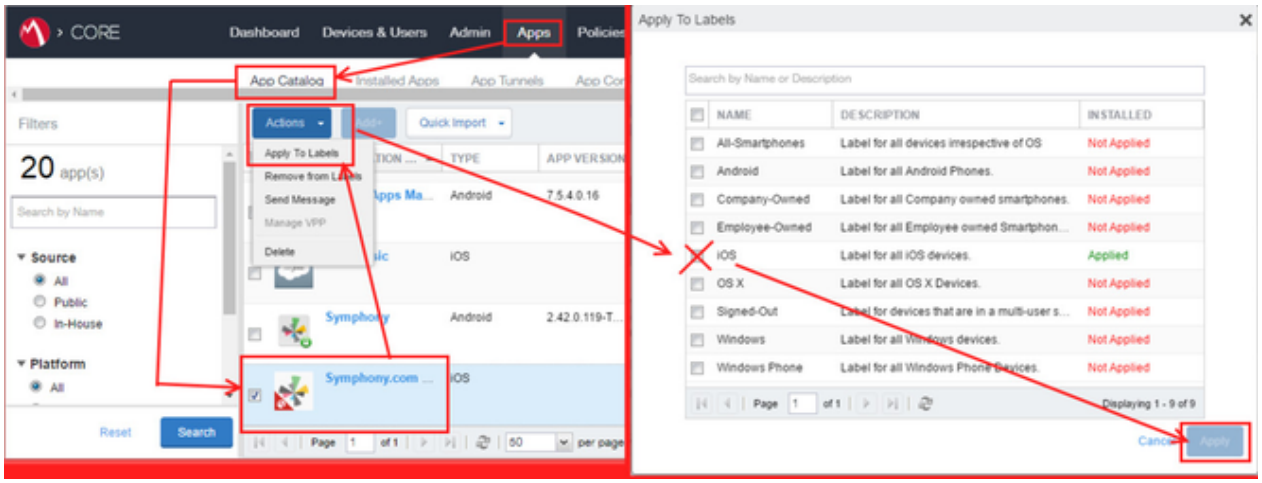
    Apps -> App Catalog -> Add+ -> iTunes -> "Symphony.com for MobileIron"

    Next button -> (see summary) -> Next Button This is a Free App
    Feature this App in the Apps@Work catalog (optional)



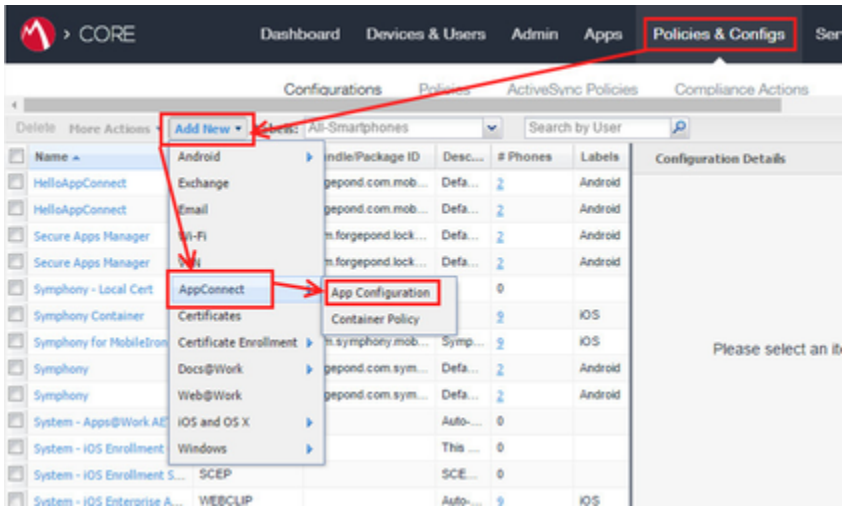
2. Apply Labels to App

Apps -> App Catalog -> Checkmark "Symphony.com for MobileIron"
Actions -> Apply To Labels -> "iOS" (check all labels you'd like to apply) -> Apply Button
Note: At this point you should see at least one "Label" in the Labels column for "Symphony.com for MobileIron"

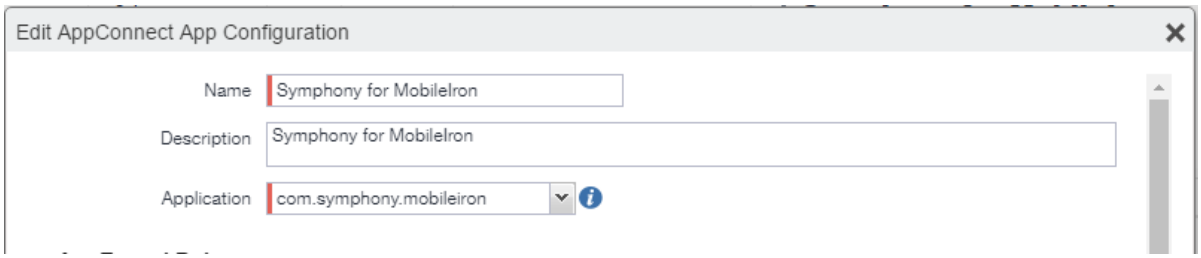


3. Associate app configuration (AppConfig)

a. Policies & Config -> Add New -> AppConnect -> App Configuration

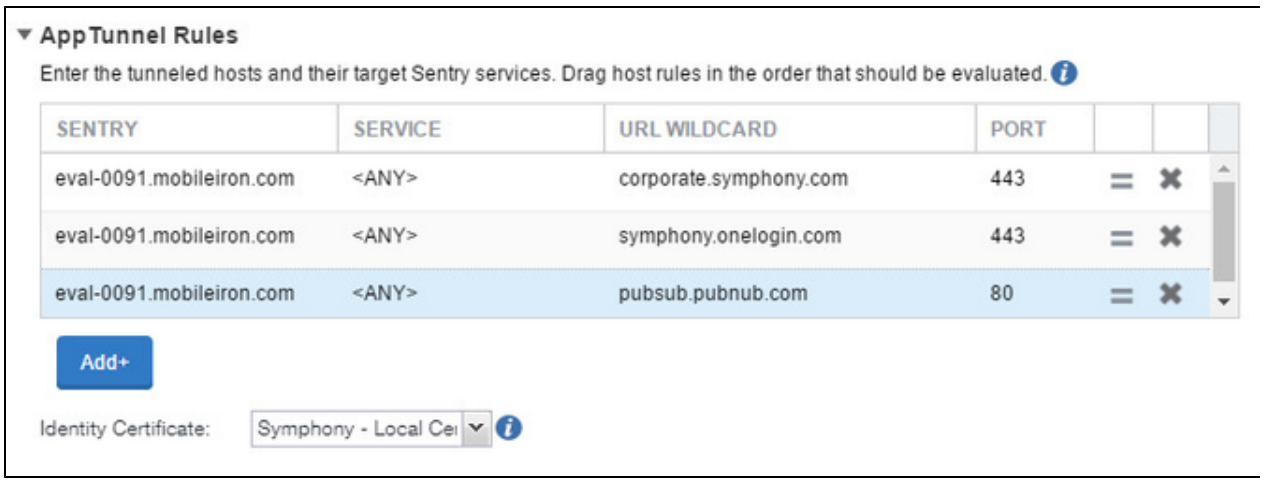


- For Name enter "Symphony for MobileIron"
- For Application type in the bundle identifier "com.symphony.mobileiron"

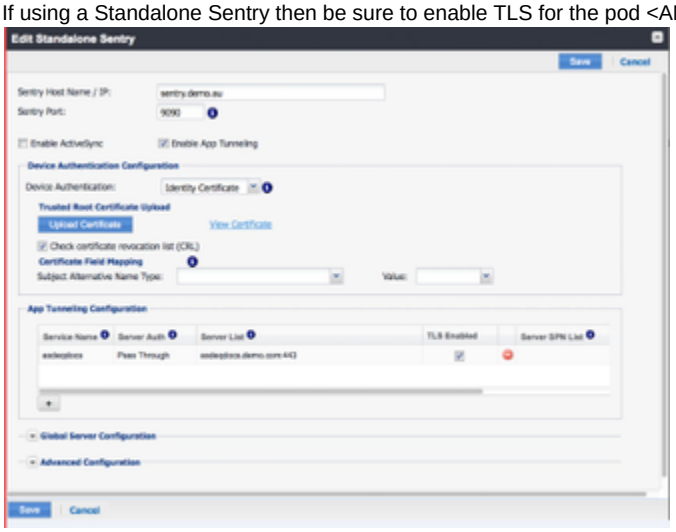


b. For AppTunnel Rules Add+ an entry to the list for the following URLs in this order:

- **Pod** URL such as "mycompany.symphony.com", port 443
- If using **SSO** signon then enter SSO URL and port other wise skip
- If **Key Manager** is in the pod then skip this otherwise enter the Key Manager URL such as mykeymanager.company.com, port 8443
- Enter the URL "pubsub.pubnub.com", port 443 to receive **Apple Push Notifications** for the app
- Enter the URL "*.pndsn.com", port 443 to receive **Apple Push Notifications** for the app
- Enter the URL my.symphony.com, port 443 for pod lookup access based on email



- If using a Standalone Sentry then be sure to enable TLS for the pod <ANY> service will already have TLS enabled:



c. Select your App Identity certificate and Add+ the following App-specific configurations:

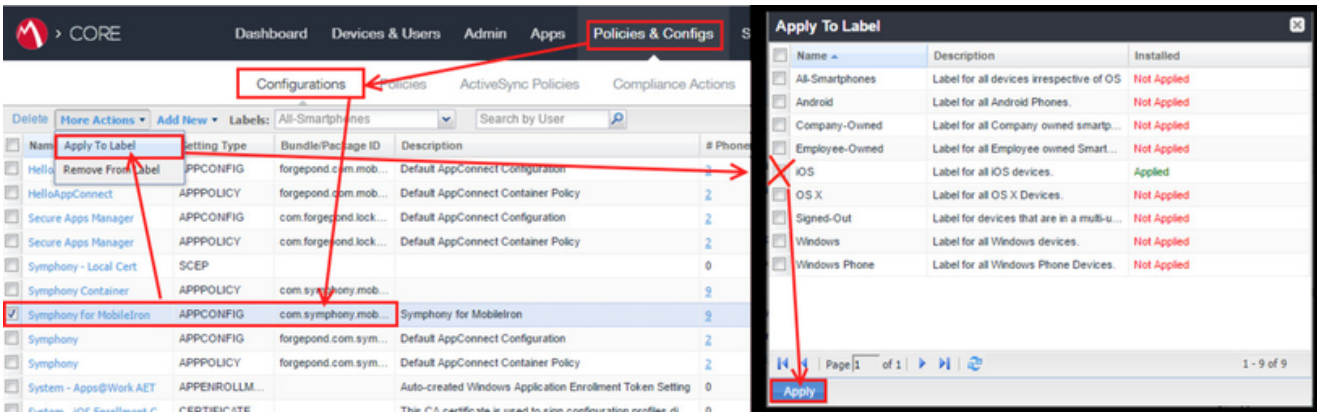
Configuration Key	Description	Value	Type	Supported in iOS	Supported in 'Android for Work'

sso_url **(Supported in R44+ for iOS, and R45+ for Android)**	Set to a string value that points to the SSO URL for your pod, for example "https://MyCompany.symphony.com/login/sso/initsso". App will no longer prompt for email and instead take you directly to the sso signon page	lookup pod by users email domain	String	Y	Y
enable_photopicker	Set to false to prohibit attaching photos from camera roll to messages sent within the application.	true |false	String	Y	Y
enable_webview	Set to false to prohibit viewing non- image attachments and URLs sent within the application.	true |false	String	Y	Y
enable_sharing	Set to false to prohibit users from sharing image attachments to other applications through OS installed share extensions.	true |false	String	Y	Y
enable_crash_reporting	Set to false to prohibit the recording of crashes for later analysis.	true |false	String	Y	Y
enable_analytics	Set to false to prohibit recording anonymous usage statistics.	true |false	String	Y	Y
enable_addressbook	Set to false to prohibit using OS Address Book to invite new contacts to application.	true |false	String	Y	Y
enable_copy	Set to false to prohibit users from copying the contents of messages.	true |false	String	Y	Y
enable_network_debugging	Set to true to emit logging for debugging network-related issues.	true |false	String	Y	Y
disable_pin	Set to true to hide the built-in Pinched feature.	true |false	String	Y	Y
disable_introduction	Set to true to automatically skip the first-launch introduction screens	true |false	String	Y	Y
enable_feedback	Set to true to allow user to send feedback (as an email) to support@symphony.com	true	Boolean	Y	Y
pod_domain (53 onwards iOS only)	The domain name of your pod such as mycompany.symphony.com OR symphony.mycompany.com	<blank> (manual user entry)	String	Y	Y
refresh_token_period (53 onwards)	Mobile Refresh Token (This value will determine how often the mobile app will refresh the session token)	<blank> (manual user entry)	String (value)	Y	Y

d. Save AppConfig Settings. If you changed the AppConfig settings then existing users that had downloaded the previous config may need to uninstall and reinstall the Symphony for MobileIron app.

4. Associate Label with App Configuration

Policies & Config -> Configurationws select AppConfig we created in the previous step
Drop down "More Actions" -> Apply To Label -> Select "iOS" Label Click Apply



5. If you change the AppConfig your users may need to uninstall and reinstall the Symphony app

7. Add your users and devices if not already configured

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.
    a. 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.
    a. 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.

--

Users - Steps to get Symphony for MobileIron on your device

1. Your administrator will have had to invite you to use your device on the MobileIron managed network.
2. On your mobile device, visit the MobileIron server (you will need to get this URL from your MobileIron administrator as mentioned in #1).
3. Download Mobile@Work
4. Sign in to Mobile@Work with credentials you've received from your administrator.
5. Follow the prompts to install the Profile from MobileIron
6. Install Symphony for MobileIron from https://itunes.apple.com/us/app/symphony.com-for-mobileiron/id1138896543?mt=8 (it is important that you install the Symphony app AFTER Mobile@Work is set up. If done out of order then uninstall Symphony and reinstall.)
7. Launch Symphony for MobileIron
8. This switches back and forth to Mobile@Work where data is exchanged. This can take 60 seconds for the first time.
9. When the device switches back to Symphony, you should be able to sign in to Symphony through SSO or Username/Password.

--

MobileIron Customer Case Study

"The solution was done with App Connect/App Tunneling - we did use a VPN setup.

So we have a dedicated Sentry for App Tunneling, so we wanted to point Symphony to connect in via that path rather than the VPN. It is on that internal Sentry where we opened up the firewall access to the keymanager. The Sentry you use for the tunneling must have that access opened.

By far the single biggest challenge we initially had was that we did not set up a specific App Config in Mobile Iron, where you specifically link the com.symphony.mobileiron app to use the Sentry we have dedicated for tunneling. That what tripped me up for a while until we added that and then it all started to fall into place. Once we had the Symphony APPCONFIG (routes it to the Sentry) and an APPPOLICY (for securing open-in controls) established, we could then see the devices connecting through the Sentry logs, and that allowed us to then pursue any remaining firewall changes needed.

The initial step to add the secure Symphony for Mobile Iron app to our app catalog on the Core was straightforward enough, as was adding/editing existing general security policies to include the new labels so that devices inherited the correct polices.

The other Mobile Iron I can add is to be sure and remove the devices/users from any default policies where App Connect may be disabled, as that is the default."

--

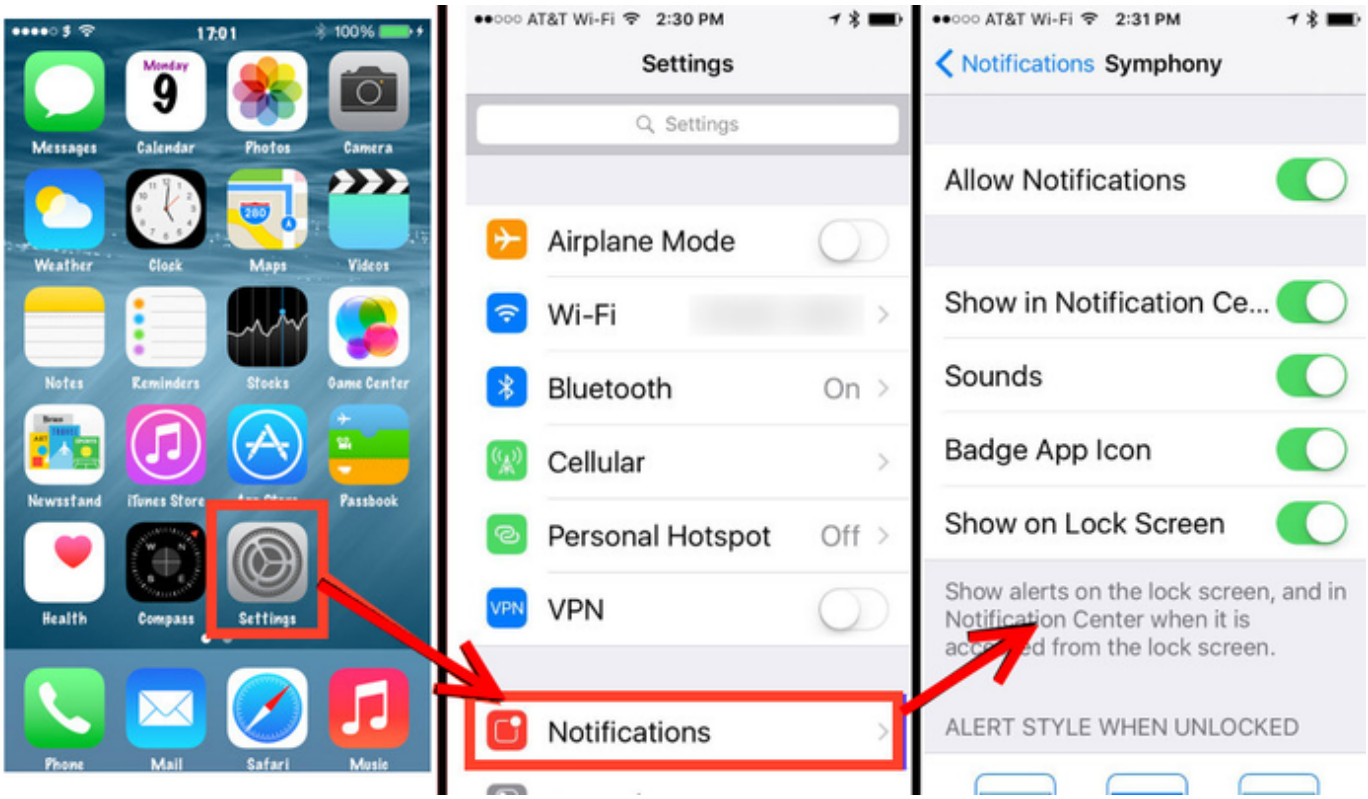
Frequently Asked Questions

Q. I am using the Symphony for MobileIron app and nobody at my company gets Apple/Google Push Notifications. Whats up?

A. Your Symphony pod must be updated to reflect that you are using the MobileIron version of the Symphony app instead of the standard version. Ask Symphony support or your Solutions Architect to update your "pubnub keys" to the MobileIron app version of the keys. This will require a restart of your pod so it will need to be scheduled for after hours or the weekend.

Q. I am using the Symphony for MobileIron app and my coworker gets Apple/Google Push Notifications but I don't. Whats up?

A. Your device notification settings must be updated to "Allow Notifications" as shown here for iOS. Go to Settings > Notifications> Symphony App > Allow Notifications and other notification related settings.


17:01
100%
Messages
Calendar
Monday
9
Photos
Camera
Weather
Clock
Maps
Videos
Notes
Reminders
Stocks
Game Center
Newsstand
iTunes Store
Passbook
Health
Compass
Settings
Phone
Mail
Safari
Music
AT&T Wi-Fi 2:30 PM
Settings
Settings
Airplane Mode
Wi-Fi
Bluetooth
On
Cellular
Personal Hotspot
Off
VPN
VPN
Notifications
AT&T Wi-Fi 2:31 PM
Notifications
Symphony
Allow Notifications
Show in Notification Ce...
Sounds
Badge App Icon
Show on Lock Screen
Show alerts on the lock screen, and in Notification Center when it is
from the lock screen.
ALERT STYLE WHEN UNLOCKED