Using Callmy@work with MobileIron

March 2, 2016
Proprietary and Confidential
Do Not Distribute

Overview

The extreme volume of email, SMS and Social Media messages mean they are no longer ideal for important communications that require a fast response – this is an important consideration for emergency and business continuity planning.

Callmy@work now provides a dedicated communication channel, reserved for your most important business messages.

To support your Mobile First strategy, integration with MobileIron enables the Callmy@work app to be pushed to your staff's devices, configured with a security certificate and access to relevant message groups.

Via the secure Callmy@work portal, you can now post encrypted messages globally, with full control and management. There's no limit on the amount of data you can share and Callmy@work messages free to deliver. If required, each Callmy@work message can be configured to request an acknowledgement of receipt, the end users details, their location and a comment. Users also do not have the authority to forward messages and all message response remain private to your organization.

To enable you to audit if your messages are having the response you require, the Callmy@work portal provides real-time information on your how your messages are being consumed, details of responses and a complete message inventory. You can also delete messages, to instantly remove them from your end users Callmy@work App.

Callmy@work is delivered from highly resilient dual homed EU based ISO 270001 certified datacenters. The service also meets the criteria of the ISO/IEC 27001:2005 Information Security Management System (ISMS) requirements Standard.

The Callmy@work iOS Bundle is: com.callmyltd.callmyapp.appconnect and the Android Package name is: com.callmy.callmy.callmyatwork

App availability

The Callmy@work for iOS devices is available from the Apple Store:

https://itunes.apple.com/gb/app/callmy-work/id1080563130?mt=8

Callmy will make available the APK for Callmy@work for Android devices.

Device compatibility

Callmy@work requires iOS 7+ and Android 4.3+

App-specific configuration

Callmy@Work is configured using the CallmyId values. Instead of having a series of fixed keys, each Following is simply a key. For example, a customer might have two CallmyIds in their organization:

1. Executive Messages (CallmyId: exec_messages)
2. Staff Messages (CallmyId: staff_messages)

They are required to generate an RSA KeyPair for each of these Ids. The private keys are loaded into MobileIron as Certificates and can be called ex-ec_messages_cert and staff_messages_cert, for example.

If the keys are not present, there is no default value applied. They are simply not used.

The Configuration for the two CallmyIds outlined above would be:

Key	Value	Default if the key-value pair is not configured
exec_messages	exec_messages_cert	n/a
staff_messages	staff_messages_cert	n/a

AppTunnel support

AppTunnel is not used at this time.

Data loss prevention policy support (iOS SDK apps only)

No policies are applied at this time.

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

No secure file I/O is done at this time.

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

No, Callmy@Work is not a dual mode app.

Additional sections

No additional software is required.

User features

When a message is received via the Callmy@work app, the user will hear an audible alert and notification via their device. A badge is also displayed on iOS devices with the new message count. Once the app is accessed by the user, the list of current messages is displayed in chronological order. The user clicks on a message to either read or listen to the information. If required, the user may be requested to supply: their name, email address, phone number and a comment. Users may also be requested to provide their location and the app will access their current GPS coordinate.

Your Callmy@work administrator sends messages to the required groups via an on-line portal. There is no restriction on the amount of data which can be sent and each message can be sent immediately or schedule for dispatch at a required data and time. The administrator can select if users should acknowledge receipt of the message (or not) or supply details – as described above. The Callmy@work Portal, provides the administrator with real-time data on the message open rate, the number of message acknowledgements and any returned comments from users, with contact/location details.

For more information

A Callmy@work datasheet is available on request.

Configuration tasks

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

Enable AppConnect.

Configure an AppConnect global policy.

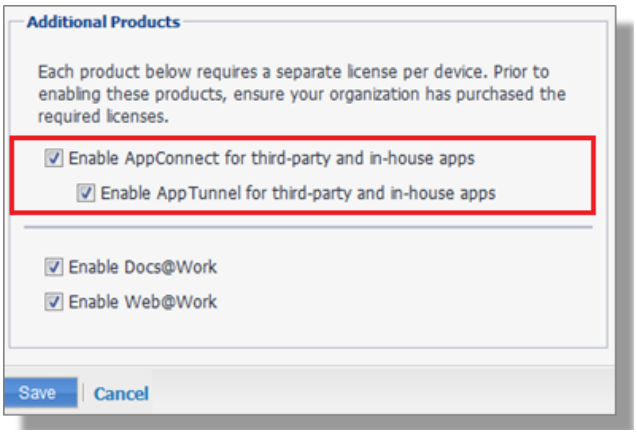
Configure a new AppConnect app configuration for the app.

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.

Create the authentication keys

In order to be authorized to follow your secure channels, you must create a cryptographic keypair. These keys are used to identify and authorize a device. One half is deployed via MobileIron and the other half is uploaded into the Callmy Portal.

This explanation will use OpenSSL (https://www.openssl.org), but you are free to use whatever tool you wish to generate an X509 public and private keys.

First, create the private key. You'll be prompted to enter a password. Be sure to use a strong password and remember the value you choose.

```
openssl genrsa -out private.key -aes256 4096
```

Next, great a certificate signing request.

```
openssl req -new -key private.key -out public.csr
```

You'll be prompted to fill in details, such as country, email address. If asked for "extra" attributes, leave those values blank.

You can now generate the private certificate

```
openssl x509 -req -days 365 -in public.csr -signkey private.key -out public.crt
```

You can change the length of validity, by using a number longer or shorter than 365 for the -days attribute.

We now have the Public certificate, signed by your private key. We will later use this certificate to secure a channel in the Callmy Portal.

To complete this section, we must now generate the Private certificate.

```
openssl pkcs12 -export -inkey private.key -in public.crt -out private.pfx
```

You will be prompted to enter the password for the private key and also to select a new password for the private.pfx file. Choose a strong password and note it down.

At this stage, you have two important files. The public.crt and the private.pfx.

Request for your Callmy@work service(s) to be updated by the Callmy Service Desk

You will need to provide details of the public key, to the Callmy service desk, with details of which Callmy@work service the key relates to. This can be done either when your Callmy@work service is first provisioned or at a later date.

The Service Desk can be contacted via: support@callmy.com

Service updates will be completed within 8 hours and your authorized contact(s) will be notified accordingly.

Add the private certificate to MobileIron

On the Core Admin Panel, go to Policies & Configs > Configurations

Choose Add New > Certificates

Under File Name, choose the private.pfx file that you created.

Under Password, use the password you chose when you created the private.pfx file.

Give this new certificate a name that identifies it as the certificate for a CallmyId e.g. "Callmy SecuredService Cert".

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.

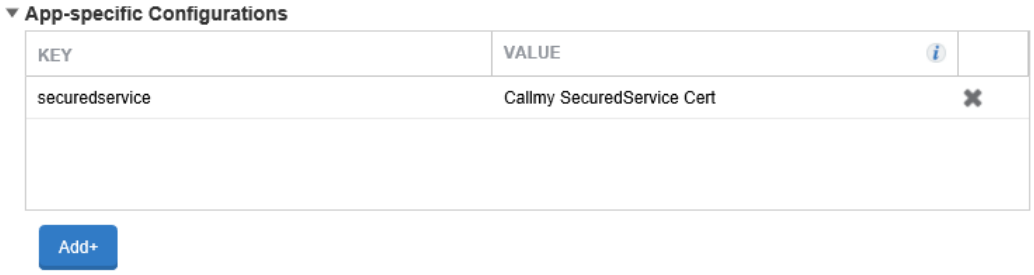
2. Edit the AppConnect app configuration with the Name, Description, Application, AppTunnel configuration including the identity certificate, and App-specific key-value pair configurations required for the app.

   For Android, select the Callmy@Work application that you have uploaded.

   For iOS, use the bundle ID, com.callmyltd.callmyapp.appconnect

3. App Specific Configuration: Click on the "Add+" button to enter the key-value pair information.

   Using the certificate, we added in the previous section, enter the appropriate CallmyId value in the Key field and choose the certificate using the dropdown in the value field. You can repeat this for as many CallmyIds that you wish to follow.



Configure a new AppConnect container policy

Callmy@Work doesn’t support any explicit container policy settings, but a container policy may be required by your MobileIron Configuration. You can, in this case, use the default settings.