Release Notes

3.4.1 | July 2015 | 3725-82878-016B2

# Polycom® RealPresence® Mobile for Apple® iOS

6001 America Center Drive
San Jose, CA 95002
USA



# Contents

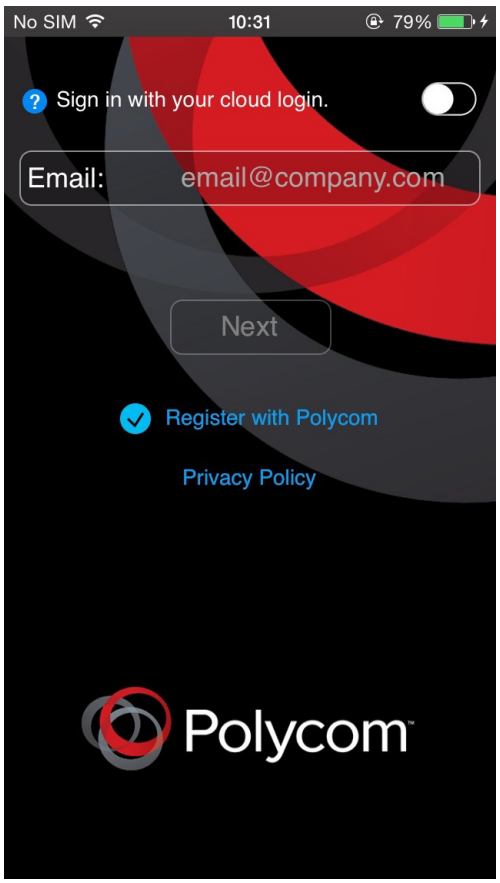
# What’s New in RealPresence Mobile 3.4.1

Polycom announces the 3.4.1 release of the Polycom® RealPresence® Mobile software. This release includes one new feature—support for Cloud Service deployments.

## Support for Cloud Services

In Cloud Service environments, the RealPresence Mobile client connections are enabled, authenticated, provisioned, and monitored by a service provider system.

Once the RealPresence Mobile app is provisioned by a provisioning server, users can sign in with their email address (see illustration).



# What's New in RealPresence Mobile 3.4

Polycom RealPresence Mobile 3.4 includes these new features:

- Profile Photo and Virtual Business Card Feature
- Mid-string Search of Favorites
- Support for Polycom NoiseBlock™
- In-call Toolbar User Interface Enhancement
- Support for 64-bit iOS Platform

**Get the latest product information from Polycom Support**
To view the latest Polycom product documentation, visit Polycom Support web site.

## Profile Photo and Virtual Business Card Feature

During a call, RealPresence Mobile can display the speaker's profile information—a virtual business card—as part of the speaker's video. The virtual business card can include the following profile information:

- Name
- Title
- Work Location

RealPresence Mobile can also be configured to display the profile photo of the speaker, along with the virtual business card, when the speaker is on video mute.

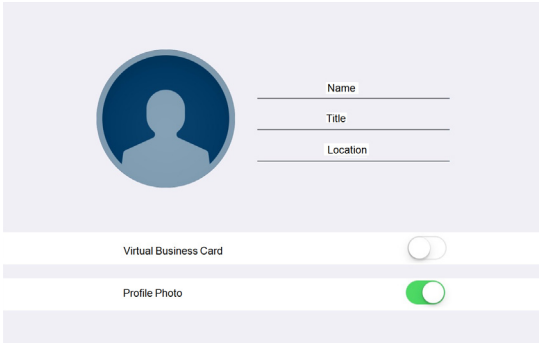
The following constraints apply to this feature:

- This feature is not supported in SVC multipoint conferences.
- In standalone mode, the profile information displayed is provided by the user; in managed mode the profile information is provided by the provisioning system.
- The profile photo must be at least 240 x 240

### To enter profile information, a profile photo, and enable a virtual business card:

1 Tap **Settings** and then **Profile**.

The **Virtual Business Card** page appears. In managed mode, the profile information is pre-populated.



2 When not in managed mode, enter the profile information to display on your virtual business card.
3 Tap the photo area and choose either Take a photo or Choose a photo.
4 Follow the prompts to complete the process and include the photo.
5 Enable both **Virtual Business Card** and **Profile Photo**.
6 Tap **Done**.

## Mid-string Search of Favorites

In standalone mode, RealPresence Mobile users can search for local contacts in their Favorites list by typing in any string of characters from the contact's name.

In managed mode, this kind of mid-string search for local and LDAP contacts is enabled when the provisioning RealPresence Resource Manager system is configured to allow mid-string searches. This feature is not available for searches of the corporate Active Directory, because in those instances the RealPresence Resource Manager system uses the standard Active Directory search functionality.

## Support for Polycom NoiseBlock™

When enabled, Polycom NoiseBlock specifies whether the system mutes audio from the microphone when keyboard tapping sounds or other extraneous noises are detected, but no one is talking. NoiseBlock unmutes the system when speech is detected regardless of the presence of background noise.

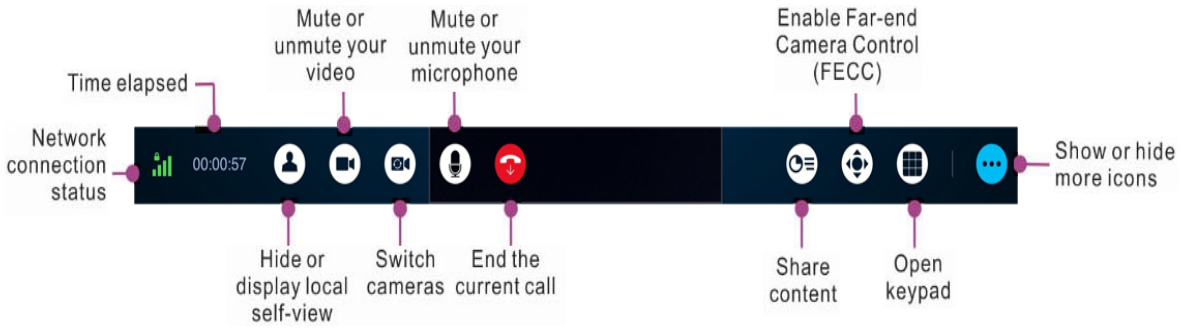
### To enable NoiseBlock:

1 Tap **Settings** and then **Advanced**.
2 Enable **NoiseBlock**.

## In-call Toolbar User Interface Enhancement

RealPresence Mobile 3.4 has a newly designed in-call toolbar. The illustration below is an example in-call toolbar on an iPad.

**iPad in-call toolbar**



## Support for 64-bit iOS Platform

RealPresence Mobile 3.4 adds support for 64-bit iOS platforms. This includes all Apple A7, A8, and A8X products.

# Release History

The following table shows the release history of the Polycom RealPresence Mobile application.

| Version | Release Date | Features |
|---|---|---|
| 3.4 | June 2015 | Profile Photo and Virtual Business Card Feature<br>Mid-string Search of Favorites<br>Support for Polycom NoiseBlock™<br>In-call Toolbar User Interface Enhancement<br>Support for 64-bit iOS Platform |
| 3.3 | January 2015 | Support for BroadSoft Device Management as Provisioning Server<br>User Interface Improvements<br>Standalone mode provides more features. See System Capabilities and Constraints for a complete list of feature capabilities.<br>Support for high video resolution (720p) on powerful mobile devices such as iPad Air and iPad Mini 2, for AVC point to point calls, AVC multi-points calls, and SVC point to point calls.<br>Support for the SDP Size Adjustment Feature<br>Devices Support Changes<br>• Drop support for iOS 6<br>• Add support for iOS 8<br>• Add support for iPad Air 2 and iPad Mini 3<br>• Add support for iPhone 6 and iPhone 6 Plus |
| 3.2.1 | July 2014 | The **Roster** display button is not shown in CloudAXIS 1.5 and earlier versions.<br>Fixed an OpenSSL security vulnerability (CVE-2014-0224).Fixed two issues.See Resolved Issues for details. |
| 3.2 | June 2014 | Support for CloudAXIS HTTPs tunneling<br>Support for roster display in a CloudAXIS meeting<br>Support for log collector<br>Support for Czech<br>Support for iPad Air and iPad Mini with Retina display |

# Hardware and Software Requirements

The following hardware and software requirements were determined based on test scenarios. Your system's actual performance may vary based on software or hardware configurations.

| | |
|---|---|
| Apple | • **iPad** iPad Air 2, iPad Air, iPad with Retina display, iPad 2, iPad Mini 3, iPad Mini with Retina display, and iPad Mini.<br>• **iPhone** iPhone 6, iPhone 6 Plus, iPhone 5S, iPhone 5C, iPhone 5, and iPhone 4S. |
| iOS Requirements | iOS 7.0 or later |
| System Requirements | Syncing with iTunes® on a Mac or PC requires:<br>• iTunes: 10.2 or later<br>• Mac: OSx 10.2 or later<br>• PC: Windows XP SP3 or later |
| Network Requirements | • Wireless Local Area Network (WLAN), 802.11 a/b/g/n recommended<br>• 3G or 4G network |
| Optional Peripheral Devices | • 3.5 mm headset<br>• Stereo Bluetooth headset |

### To view your iOS system version:

» From your device, tap **Settings > General > About > Version**.

# Products Tested with this Release

Polycom RealPresence Mobile systems are tested extensively with a wide range of products. The following table does not provide a complete inventory of compatible equipment, but indicates the products that have been tested for compatibility with this release.

**Upgrade your Polycom products**

You are encouraged to upgrade all your Polycom systems with the latest software before contacting Polycom support to ensure that the issue has not already been addressed by vendor software updates. Go to the Polycom support website to find the current Polycom Supported Products matrix.

## Polycom CMA System and RealPresence Resource Manager System

The RealPresence Mobile application can register to the Polycom CMA Server and Polycom RealPresence Resource Manager server. Some management features have limitations relative to other Polycom endpoints. For example, software updates of RealPresence Mobile are not supported and the QOS monitoring is limited.

| Type | Product | Version |
|---|---|---|
| Gatekeeper, Gateways, External MCU, Bridges, Call Managers | Polycom Distributed Media Application™ (DMA®) 7000 | 6.2.0, 6.3.0 |
| | Polycom Converged Management Application™ (CMA®) 4000/5000 | 6.2.5 |
| | Polycom RealPresence Resource Manager | 8.3, 8.4 |
| | Polycom RMX® 4000/2000 | 8.5, 8.6 |
| | Polycom RMX® 1500 | 8.6 |
| | Polycom RealPresence® Collaboration Server 1800 | 8.5, 8.6 |
| | Polycom RMX® 1000C | 2.5.1 |
| | Polycom RSS™ 4000 | 8.5.1 |
| | Polycom RealPresence Capture Server | 1.8, 2.0 |
| | Broadsoft SIP r19 Server | r19 |
| | Polycom RealPresence CloudAXIS™ Suite | 1.6, 1.7 |
| NAT/Firewall/Border Controller | ACME Packet Net-Net 3820 | Firmware SCX6.3.0 MR-5 Patch 2 |
| | Polycom VBP® 5300-ST | 11.2.19 |
| | Polycom VBP-E | 11.2.19 |
| | Polycom RealPresence® Access Director™ | 4.1, 4.2 |
| Endpoints | Polycom HDX® Series | 3.1.4, 3.1.5 |
| | Polycom RealPresence Mobile | 3.3, 3.4 (iOS)<br>3.3, 3.4 (Android) |
| | Polycom VVX® | 5.0.1 |
| | Polycom CMA® Desktop | 5.2.6 |
| | Polycom Telepresence m100 | 1.0.7 |
| | Polycom RealPresence Desktop | 3.3, 3.4 (Windows) |
| | | 3.3, 3.4 (Mac) |
| | Polycom RealPresence Group Series | 4.2, 4.3 |

| Type | Product | Version |
|---|---|---|
| Other | Polycom People+Content IP | 1.3 (PC only) |
| | Broadsoft environment | r19 |

# Install and Uninstall RealPresence Mobile

This section explains how to install and uninstall RealPresence Mobile.

### To install the RealPresence Mobile application:

1. Go to the Apple Store, search for **Polycom** or **video conferencing** to find the RealPresence Mobile application.
2. Tap **Free** and then **INSTALL APP.**

**Consume one more license after upgrade**

RealPresence Mobile will consume one more license after upgrading from 3.0 or earlier version to version 3.1 or later versions.To release the old license, you must remove the old license manually or set the license reclaim cycle to be a small value (for example five minutes) on RealPresence Resource Manager.

### To uninstall the RealPresence Mobile application:

1. Go to the device's application list.
2. Tap and hold **Video** until it begins to jiggle.
3. Tap and then tap **Delete.** Your user data is deleted when you uninstall this application.

# System Capabilities and Constraints

The following protocols, resolutions, algorithms, and ports are supported for RealPresence Mobile.

## Capabilities

| Call Rate | Video Capability |
|---|---|
| 1 Mbps | 720p |
| 512 kbps<br>384 kbps<br>256 kbps | 480x270 |
| 128 kbps | 240x135 |
| 64 kbps | Audio only |

## Protocols

The following table lists the protocols supported in this version of the RealPresence Mobile application.

| Protocol | Description |
|---|---|
| DNS | Domain Name System |
| H.235 | Security and Encryption |
| H.239 | Token Management |
| H.323 | Signaling |
| H.460 | Firewall/NAT Traversal |
| LDAP, H.350 | Directory Services |
| NTLMv2 | Authentication |
| Polycom LPR™ | Lost Packet Recovery |
| SIP | Session Initiation Protocol |

## Resolutions

The following table lists the resolutions supported in this version of the RealPresence Mobile application.

| Resolution and Frame Rate | Source |
|---|---|
| Up to 720p, 15 fps | People video sent from camera |
| Up to 720p, 30 fps | People video received from far end |
| Up to 720p (1280x720), 5 fps | Content received from far end |
| Up to XGA (1024x768) / 5fps | Content showing from the tablet |

**Video capability**

Actual transmitted video resolution is determined by several factors, such as camera capability, computer performance, network conditions, the far-end system's capabilities, and whether content is being received.

HD/720p 30 fps is the maximum video receiving capability. The actual resolution is based on the negotiation with the far end.

## Algorithms

The following table lists the algorithms supported in this version of the RealPresence Mobile application.

| Algorithm Type | Description |
|---|---|
| Audio | G.722.1 Annex C<br>G.711u<br>G.711a<br>Siren LPR<br>Acoustic Echo Cancellation (AEC)<br>Automatic Gain Control (AGC)<br>Scalable Audio Coding (SAC) |
| Video | Polycom Lost Packet Recovery™ (LPR™)<br>H.264 SVC<br>H.264 AVC<br>H.264 high profile<br>H.263 and H.263+ (for content only)<br>**Note:** H.261 is not supported. |
| Encryption | AES-128 media encryption<br>TLS for SIP calls |

## Inbound and Outbound Ports

The following table lists the inbound and outbound ports supported in this version of the RealPresence Mobile application.

| Port | Function |
|---|---|
| 1720 (TCP) | H.323 Call Signaling (H.225) |
| 1719 (UDP) | H.323 Registration, Admission, and Status (RAS) |
| 3230 - 3250 (TCP) | H.323 Call Control (H.245) |
| 3230 - 3250 (UDP) | Media (RTP/RTCP) |
| 3238 (UDP and TCP) | BFCP |
| 5060 (UPD and TCP) | SIP |

| Port | Function |
|---|---|
| 443 (TCP) | Provisioning, Monitoring, Help Files, HTTPS |
| 389 (TCP) | LDAP |
| 5060 (UDP and TCP) | SIP |
| 5061 (TCP) | SIP TLS signaling |

| Port | Function |
|---|---|
| 1720 (TCP) | H.323 Signaling (H.225) |
| 1719 (UDP) | H.323 Registration, Admission, and Status (RAS) |
| 3230 - 3250 (TCP) | H.323 Control (H.245) |
| 3230 - 3250 (UDP) | Media (RTP/RTCP) |
| 3238 (UDP and TCP) | BFCP |

# Known Issues

The following table lists the known issues for this release. If a workaround is available, it is noted in the table.

| Issue ID | Description | Workaround |
|---|---|---|
| SWEP-7515 | When RealPresence Mobile is configured in standalone mode and SIP calls are enabled, the UI shows TLS is shown as the transport protocol in error. | None |

# Resolved Issues

The following table lists the resolved issues for this release.

| Issue ID | Description |
|---|---|
| SWEP-7203 | AGC may lower the microphone volume when the user speaks loudly, but doesn't readjust when the user speaks softly. |
| SWEP-6684 | Sometimes camera can't be started in the call and UI is dead and it can't be touched. |
| SWEP-6835 | RealPresence Mobile SIP URI dialing into our RPAD--> RMX and it Crashed |

# Interoperability Issues

You may encounter the following issues when using RealPresence Mobile with other products or on specific operating systems.

**Interoperability Issues**

| Limitation Type | Description | Solution |
|---|---|---|
| Limitations Related to Operation System or Devices | On some iPads with poor CPU performance, when RealPresence Mobile send PDF content, the video may freeze on far ends every three seconds. | None. |
| | Audio may stop in the first few seconds when plugging in an earphone in a call on iPhone 6. | None.<br>This is a device issue. |

**Interoperability Issues**

| Limitation Type | Description | Solution |
|---|---|---|
| Limitations Related to Other Polycom Products | If you create a Continuous Presence (CP) only conference call on Polycom RMX 4000/2000 system and Polycom RealPresence Collaboration Server 800s version 8.1 with default content settings (**Content Settings: HiResGraphics** and **Content Protocol: H.264 HD**), the RealPresence Mobile application cannot send or receive content if call rate is set as 384 kbps or below. | • Change the RMX **Content Settings** to **Graphics**, and **Content Protocol** to **H.263 & H.264 Auto Selection**.<br>• Set the call rate on RealPresence Mobile to above 384 kbps. |
| | Polycom VSX® Visual Concert™ cannot display 1024x576 content sent by RealPresence Mobile, whether or not they call each other directly. | Double-click the content to show the content in full screen, then RealPresence Mobile will send 1024x768 content, and the Polycom VSX Visual Concert can display correctly. |
| | RealPresence Mobile may consume more than one license on RealPresence Resource Manager if you install and uninstall RealPresence Mobile several times. | Configure the reclaim period on RealPresence Resource Manager to a small value (for example five minutes). |
| | RealPresence Mobile supports only using English user names and password to sign in Polycom CMA server and RealPresence Resource Manager, or to register to a gatekeeper or an SIP server. | Use English user name and password. |
| | In a motion mode conference, RealPresence Mobile receives video with a long delay because the video is 60 fps. | Set a conference with sharpness mode on MCU. |
| | RealPresence Mobile in internet may fail to call Telepresence m100 in intranet. | Let Telepresence m100 call RealPresence Mobile. |
| | You may hear a short audio glitch on RealPresence Mobile when dialing in an SIP AVC encrypted conference created on the RMX 4000 with NGB. | None. |

# Enterprise Scalable Video Coding (SVC) Solution

The Enterprise Scalable Video Coding (SVC) solution is an alternative to the AVC mode that has traditionally been supported. Differences between the two modes are listed in the following table.

| SVC Mode | AVC Mode |
|---|---|
| Each participant in the conference call is received by the client as a separate video stream. | The composite video image is determined by the bridge based on administrator configuration. |
| A Caller ID is indicated by text in the appropriate window, on display throughout the call. | Caller ID information is displayed intermittently. |
| Double-clicking or tapping on a participant's video, content video, or local preview expands that video to full screen. Double-clicking or tapping again reverts the display to the composite image.<br>Pinch controls enable you to zoom in and out on a participant's video or content video. | Layout may typically be controlled by dialing **, and then selecting a format. |

The SVC solution provides the following features:

- For video send and receive, support up to 720p on high performance devices under 1 Mbps call rate.
- For video send, support 7.5/15 fps
- For video receive, support 7.5/15/30 fps
- Support auto layouts of 1x1, 1+1 through 1+5.

  The maximum layout of 1+5 comprises 4 remote participants plus 1 content-sharing frame, and 1 local preview frame.
- Support for AVC content.
- Support for Scalable Audio Coding (SAC) with at least two quality layers.
- Ability to mix up to three different audio streams from the MCU.
- Ability to combine up to four different SVC video streams (call rate at 512kbps and above) from the MCUs.
- Support for SVC dial-out from DMA.

Using SVC conference calls has following limitations:

- Does not support recording.
- Far-end Camera Control (FECC)
- In a SIP call, when networks using UDP experience 10 percent packet loss, the screen layout on received devices can be incorrect.
- Does not support H.323 call
- In a poor network connection, sometimes a participant disconnects automatically from an SVC call. This can result in a frozen video stream of the participant. The RMX system will clear the frozen stream in 30 minutes.
- Do not use 128 kbps if you share content in a SVC call, otherwise people's video will freeze while sending or receiving content.

# Access Media Statistics

To access media statistics, click . The following table shows the meaning of each value.

| Value | Description |
|---|---|
| Call Type | SIP or H.323 call type. |
| Call Encryption | Indicates whether your call is encrypted. |
| Far Site Name | Name of the far site. |
| Far Site System | Type of video conferencing system at the far end and the software version. |
| Call Speed | Negotiated speed (bandwidth) for the call, which is usually the combined video and audio speeds in the call. |
| Video Protocol | ITU-C video algorithm and annexes used in the current call. The video protocol used depends on the capabilities of the system at the far end as well as on your system's configuration. |
| Video Format | Picture size currently in use. |
| Audio Protocol | Audio algorithm and annexes used in the current call. The audio protocol used depends on the capabilities of the system at the far end as well as on your system’s configuration. |
| Audio Rate | Bandwidth specified for the audio portion of the call. The proportion of the audio rate to the video rate depends on the protocol used. |
| Video Rate | Bandwidth specified for the video portion of the call. The proportion of the video rate to the audio rate depends on the protocol used. |
| Video Rate Used | Actual bandwidth being used for the video portion of the call. This is a real-time measurement, which normally fluctuates. |
| Video Frame Rate | Rate your system uses to update the picture seen at the far end. The system can send up to 15 fps. If the camera picks up large, continuous, or frequent motions, the software takes longer to assemble the data into video frames, and the frame rate drops. Changes in lighting also reduce the frame rate. |
| Video Packets Loss Percentage | Total video packet loss as a percentage of the total number of video packets transmitted by your system and those transmitted by the far end. |
| Video Jitter | Percentage of variation in the video transmission rate. |
| Audio Packet Lost | Number of audio data packets lost during the call, including transmitted packets and incoming packets. Packet loss indicates congestion or other problems on the network. |
| Audio Packets Loss Percentage | Total audio packet loss as a percentage of the total number of audio packets transmitted by your system and those transmitted by the far end. |
| Audio Jitter | Percentage of variation in the audio transmission rate. |
| Content Protocol | Format used for the recording, compression, and distribution of the content. |
| Content Format | Display resolution of the content. |
| Content Rate | Rate your system uses in content transmission. |

| Value | Description |
|---|---|
| Content Rate Used | Actual bandwidth being used for the content transmission. |
| Content Frame Rate | Rate your system uses in content frame transmission. |
| Content Packets Lost | Number of content data packets lost during the call, including transmitted packets and incoming packets. Packet loss indicates congestion or other problems on the network. |
| Content Packets Loss Percentage | Total audio packet loss as a percentage of the total number of content packets transmitted by your system and those transmitted by the far end. |

# Prepare Your Device for Mutual Transport Layer Security

You can establish secure communications using Mutual Transport Layer Security (MTLS) with provisioning servers such as Polycom DMA or RealPresence Resource Manager systems.

To establish MTLS connections, the client and server need to hold certificates issued from the same Certificate Authority (CA) and the root certificate of this CA.

To import certificates into your iPad, you need to generate a Certificate Request (CSR) first by using a computer that has installed the OpenSSL tool. This is an iOS limitation.

The following example uses Mac as the example.

### To generate and import your certificate:

1. Open the Terminal from your Mac computer.
2. Generate the private key *client.key*. For example:
   ```
   Mike-MacBook-Pro:~ root# openssl genrsa  -out client.key 1024
   ```
3. Generate the certificate request *client.csr*. For example:
   ```
   Mike-MacBook-Pro:~ root# openssl req -new -key client.key -out client.csr
   ```
   You are about to be asked to enter information that will be incorporated into your certificate request.

   What you are about to enter is what is called a Distinguished Name or a DN.

   There are quite a few fields but you can leave some blank
   ```
   For som-----
   Country Name (2 letter code) [GB]:cn                 ---CSR info.
   State or Province Name (full name) [Berkshire]:bj  ---CSR info.
   Locality Name (eg, city) [Newbury]:bj      ---CSR info.
   Organization Name (eg, company) [My Company Ltd]:plcm  ---CSR info.
   Organizational Unit Name (eg, section) []:caqa   ---CSR info.
   Common Name (eg, your name or your server's hostname) []:caqa  ---CSR info.
   E-mail Address []:pp@pp.com  ---CSR info.
   ```

4 Enter the following extra attributes to be sent with your certificate request. Write down the challenge password. You will need it later in the procedure

```
A challenge password []:1234            -----see [Note1]
An optional company name []:poly
```

5 Submit the certificate request to your CA:

**a** View the content of the file *client.csr* using the following command, then select and copy its content (from ---BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST---):

```
Mike-MacBook-Pro:~ root# cat client.csr
```

**b** Go to your CA's web interface http://<CA's IP address>/certsrv/, and click **Request a certificate**.

**c** Click **Advanced certificate request**.

**d** Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

**e** Paste the content of the file **client.csr** to the **Saved Request** text field, and click **Submit**.

**f** Click **Base 64 encoded** and click **Download certificate.**

The file is saved as *certnew.cer* by default in the folder **Downloads**.

6 Move the generated **certnew.cer** file to your current directory.

7 Convert the file *ccertnew.cer* to a .p12 file by using the OpenSSL tool. For example:

```
Mike-MacBook-Pro:~ root#openssl pkcs12 -export -in certnew.cer -inkey
client.key -out client.p12 -name testp12
Enter Export Password:

Verifying - Enter Export Password:
```

The export password should be the same as the challenge password you set in step 3.

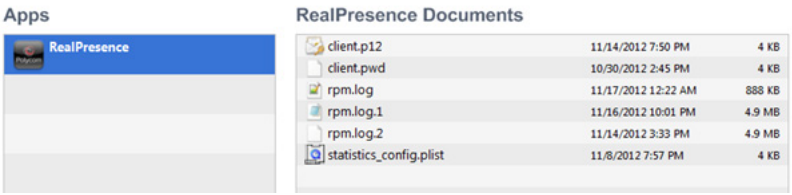
8 Encrypt the challenge password you set in Step 3:

**a** Go to Convert Strings.

**b** Enter the challenge password in the text field, and click **Base64 Encode!**.

**c** Copy the encoded text from the following text field, and save it as a .pwd file, for example, *client.pwd*.

9 Add both *client.p12* and *client.pwd* to your iPad using iTunes.




## To import the root certificate of your CA into your iPad:

1 Go to your CA's web address http://<MCA's IP address>/certsrv/, click **Download a CA certificate, certificate chain, or CR**L.

2 Select **Base 64**, and click **Download CA Certificate.**

3 Send the certificate to your iPad as an e-mail attachment.

4 On your iPad, open the attached certificate from your e-mail, and then click **Install**.

5 When prompted to install the profile, tap **Install Now**, and then tap **Done**.

The certificate is now installed on your iPad. You can find it from your iPad **Settings > General > Profile > Configuration Profiles**.

**Hold CA root certificate and system's certificates on servers**

To establish MTLS connection with servers such as Polycom DMA or RealPresence Resource Manager systems, the Polycom DMA or RealPresence Resource Manager system should also hold the CA root certificate and the system's certificates.