



CHAPTER 1

Getting Started

This chapter provides information that you need to get started with the IPICS Mobile Client. It includes these topics:

- [Overview, page 1-1](#)
- [Obtaining the IPICS Mobile Client, page 1-4](#)
- [Obtaining an SSL Certificate, page 1-4](#)

Overview

The IPICS Mobile Client is an application for the Apple iPhone that allows you to use an iPhone to interact with other participants in a Cisco IP Interoperability and Collaboration System (IPICS) incident.

For information about iPhone models, iOS versions, and network configurations that support the IPICS Mobile Client, see *Cisco IPICS Compatibility Matrix*.

With the IPICS Mobile Client application, you can use an iPhone to perform a variety of activities, including:

- Access any active incident in which you are a configured participant
- Obtain up-to-date information about resources in an incident
- Access video clips, images, and journals from an incident
- Add video clips, images, and journals to an incident
- Use the push-to-talk (PTT) feature to communicate with other incident participants

Before you can use the IPICS Mobile Client, you must download it to your iPhone. You also must download an SSL certificate from the Cisco IPICS server to the iPhone. This chapter describes these procedures.

In addition, be aware of these guidelines:

- The iPhone can communicate with Cisco IPICS either via a WiFi network connection or a 3G connection over VPN (see *Cisco IPICS Compatibility Matrix* for details).

For a WiFi connection, the iPhone must be on the same wireless network as the Cisco IPICS server on which an incident that you are accessing is active. For a 3G connection over VPN, the Cisco IPICS server must be on the public Internet and be accessible by external devices, the iPhone communication with Cisco IPICS server must be handled by a router media service (RMS) or a unified media service (UMS) component, and the iPhone must have access to the 3G network of your service provider. (For supported service providers, see *Cisco IPICS Compatibility Matrix*.)

You can Configure network options on an iPhone by touching **Settings > Wi-Fi**.

- If you are using the IPICS Mobile Client on a WiFi network and have established an audio connection, you lose the audio connection if you move to a different network. For example, you lose the audio connection if you move from a WiFi network to a 3G connection over VPN.
- If you are using the IPICS Mobile Client on a 3G connection over VPN and move to a WiFi network, the IPICS Mobile Client attempts to establish audio connectivity.
- To allow audio communication, the IPICS Mobile Client must be in the same network as the RMS or UMS component that it uses, or the IPICS Mobile Client and the RMS or UMS component each must be in a network that does not block voice over IP (VoIP) communication.
- The iPhone on which you run the IPICS Mobile Client must point to a valid DNS server.
- The IPICS Mobile Client application times out and displays the Log In screen after losing connectivity to the Cisco IPICS server for a minimum of 3 minutes.
- Incoming audio has a delay of approximately 1 second.

- When you view a list of incidents or a list of resources in an incident, the information in the screen updates automatically. The update interval is defined by the Client Update Poll option in the **Administration > Options > Client** tab in the Cisco IPICS Administration Console. The default update interval is 5 seconds.
- Most communication between the IPICS Mobile Client and the Cisco IPICS server goes over Secure Socket Layer (SSL) and is encrypted and secure. Secure communication includes logging in, logging out, uploading resources, and obtaining SSL certificates. However, audio communication is not encrypted.
- If a policy that includes an alert triggers on the Cisco IPICS server, the alert appears in a pop-up screen on the iPhone if the IPICS Mobile Client is running. If you are viewing archived video when an alert triggers, the alert appears when the video stops playing. Touch OK to exit an alert pop-up screen. If you have received multiple alerts, the next one appears when you exit the pop-up screen.
- If the primary Cisco IPICS server fails while you are logged in from an IPICS Mobile Client, the IPICS Mobile Client application attempts to reconnect. If it cannot reconnect after three attempts, it displays the Log In screen.

If high availability is configured for the Cisco IPICS server, you can log back in by identifying the primary server and the system redirects you to the secondary server automatically. When fallback occurs, the IPICS Mobile Client Log In screen appears again.
- If you are using headphones with your iPhone, plug in the headphones before starting the IPICS Mobile Client.

For related information about the Cisco IPICS server and incidents, see the Cisco IPICS documentation and the Cisco Dispatch Console documentation.

Obtaining the IPICS Mobile Client

The IPICS Mobile Client is available from the Apple App Store. The application name is Incident 4.5(1). To obtain the Incident 4.5(1) application and install it on an iPhone, take either of these actions:

- Download the Apple iTunes application to your PC. Next, open iTunes, navigate to **Store > iTunes Store > App Store**, and download the Incident 4.5(1) application. Then you can sync your iPhone with iTunes. See your iPhone documentation for additional information.
- On your iPhone, launch the App Store application and download the Incident 4.5(1) application.

After you obtain the application, it appears on your iPhone as **Cisco IPICS**.

Obtaining an SSL Certificate

Before it can log in to a Cisco IPICS server, an iPhone must download an SSL certificate from that server. An iPhone requires a separate SSL certificate from each Cisco IPICS server to which it will connect.

Obtaining an SSL certificate involves downloading the certificate from the Cisco IPICS server to your iPhone. You can perform this procedure before or after you download the IPICS Mobile Client application to your iPhone.

The Cisco IPICS server from which you download an SSL certificate must have a fully qualified hostname that exists in a DNS that the iPhone can use.

For additional information about SSL certificates on a Cisco IPICS server, see the “Generating SSL Certificates for the iPhone” appendix in *Cisco IPICS Server Administration Guide*.

The following section provide instructions regarding SSL certificates:

- [Downloading an SSL Certificate to an iPhone, page 1-5](#)
- [Deleting an SSL Certificate from an iPhone, page 1-6](#)


Downloading an SSL Certificate to an iPhone

To download an SSL certificate from a Cisco IPICS server to an iPhone, perform the following steps.

This procedure requires you to provide the fully qualified hostname of the Cisco IPICS server. If you do not know this name, contact your Cisco IPICS system administrator.

If your Cisco IPICS deployment has high availability configured, you must download a certificate from both the primary and the secondary server to allow the IPICS Mobile Client to take advantage of the high availability feature.

Procedure

- Step 1** On the iPhone, touch the Safari icon to launch the Safari browser.
- Step 2** Navigate to the following URL:
- `http://host_name/`
- Replace *host_name* with the fully qualified hostname of the Cisco IPICS server from which you are downloading the certificate. For example, if the Cisco IPICS server name is *ipics1*, enter the fully qualified hostname as **ipics1.cisco.com**.
- Step 3** Touch the **Go** button.
- The Cisco IPICS Log In screen appears. You can pinch to zoom the screen.
- Step 4** Touch the certificate icon  next to the Log In button.
- If high availability is configured, two certificate icons appear. In this case, you can choose either one. When you repeat this procedure, you will choose the other one.
- An Apple installer application displays a screen that provides information about the installation.
- Step 5** Touch the **Install** button.
- Step 6** If the Install Profile screen appears, touch the **Install Now** button.
- Step 7** If you have configured a passcode for your iPhone by using **Settings > General > Passcode Lock**, enter the passcode to unlock the iPhone.
- Step 8** When you see the Profile Installed screen, touch the **Done** button.
- The certificate is now installed on the iPhone as a root certificate.

- Step 9** If high availability is configured for your Cisco IPICS server, repeat this procedure, choosing the second certificate icon in [Step 4](#).
-

Deleting an SSL Certificate from an iPhone

If you need to replace an existing SSL certificate on a Cisco IPICS server (for example, because the certificate expired), you can download a new certificate. Before doing so, you must delete the old certificate from the iPhone. To delete a certificate, follow these steps:

Procedure

- Step 1** On the iPhone, touch **Settings > General > Profiles**.
- Step 2** Touch the certificate and then touch **Remove**.
The name of an SSL certificate matches the hostname of the Cisco IPICS server from which it was downloaded.
- Step 3** In in the confirmation alert, touch **Remove**.
Now you can download the new certificate as described in the “[Downloading an SSL Certificate to an iPhone](#)” section on page 1-5.
-