



# Configuring Voice Messaging Ports for Security

This chapter contains information on the following topics:

- [Voice Messaging Security Overview, page 10-1](#)
- [Secure Voice Messaging Port Configuration Checklist, page 10-2](#)
- [Applying a Security Profile to a Single Voice Messaging Port, page 10-3](#)
- [Applying the Security Profile in the Voice Messaging Port Wizard, page 10-3](#)
- [Where to Find More Information, page 10-4](#)

## Voice Messaging Security Overview

When you configure security for Cisco CallManager voice messaging ports and Cisco Unity SCCP devices, a TLS connection (handshake) opens for authenticated devices after each device accepts the certificate of the other device; likewise, the system sends SRTP streams between devices; that is, if you configure the devices for encryption.

When the device security mode equals authenticated or encrypted, the Cisco Unity-CM TSP connects to Cisco CallManager through the Cisco CallManager TLS port. When the device security mode equals nonsecure, the Cisco Unity TSP connects to Cisco CallManager through the Cisco CallManager SCCP port.

Consider the following information before you configure security:

- In this document, the use of the term, server, refers to a server in the Cisco CallManager cluster. The use of the phrase, voice-mail server, refers to a Cisco Unity server.
- You must run Cisco Unity 4.0(5) or later with this version of Cisco CallManager.
- You must perform security tasks for Cisco Unity by using the Cisco Unity Telephony Integration Manager; for information on how to perform these tasks, refer to the *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*.
- In addition to the procedures described in this chapter, you must use the certificate management feature in the Cisco IP Telephony Platform Administration to the Cisco Unity certificate to the trusted store. For more information on this task, refer to the *Cisco IP Telephony Platform Administration Guide*.

After you copy the certificate, you must restart the Cisco CallManager service on each server in cluster.

- If Cisco Unity certificates expire or change for any reason, use the certificate management feature in the Cisco IP Telephony Platform Administration to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and voice messaging does not work because it cannot register to Cisco CallManager.
- The setting that you specify in the Cisco Unity Telephony Integration Manager must match the voice messaging port device security mode that is configured in Cisco CallManager Administration. In Cisco CallManager Administration, you apply the device security mode to the voice messaging port when you apply a SCCP phone security profile to the port.

**Tip**

If the device security mode settings do not match for Cisco CallManager and Cisco Unity, the Cisco Unity ports fail to register with Cisco CallManager, and Cisco Unity cannot accept calls on those ports.

- Changing the security profile for the port requires a reset of Cisco CallManager devices and a restart of the Cisco Unity software. If you apply a security profile in Cisco CallManager Administration that uses a different device security mode than the previous profile, you must change the setting in Cisco Unity.
- When you apply a security profile to the port, Cisco CallManager ignores the Certificate Authority Proxy Function (CAPF) settings that exist for the profile because voice messaging ports do not support these settings. Choose a profile based on the device security mode, not the CAPF settings.
- For information on settings that you configure in the SCCP phone security profile, see the “[Configuring a Phone Security Profile](#)” section on page 5-1.

## Secure Voice Messaging Port Configuration Checklist

Use [Table 10-1](#) as a reference when you configure security for voice messaging ports.

**Table 10-1 Configuration Checklist for Securing Voice Messaging Ports**

Configuration Steps		Related Procedures and Topics
<b>Step 1</b>	Verify that you installed and configured the Cisco CTL Client for secure mode.	<a href="#">Configuring the Cisco CTL Client, page 3-1</a>
<b>Step 2</b>	Verify that you configured the phones for authentication or encryption.	<a href="#">Phone Security Overview, page 4-1</a>
<b>Step 3</b>	Use the certificate management feature in the Cisco IP Telephony Platform Administration to copy the Cisco Unity certificate to the trusted store on each server in the cluster; then, restart the Cisco CallManager service on each server.	<ul style="list-style-type: none"> <li>• <a href="#">Voice Messaging Security Overview, page 10-1</a></li> <li>• <i>Cisco IP Telephony Platform Administration Guide</i></li> <li>• <i>Cisco CallManager Serviceability Administration Guide</i></li> </ul>
<b>Step 4</b>	In Cisco CallManager Administration, configure the security profile for the voice messaging ports; apply the profile to the port.	<ul style="list-style-type: none"> <li>• <a href="#">Applying a Security Profile to a Single Voice Messaging Port, page 10-3</a></li> <li>• <a href="#">Applying the Security Profile in the Voice Messaging Port Wizard, page 10-3</a></li> </ul>

Table 10-1 Configuration Checklist for Securing Voice Messaging Ports (continued)

Configuration Steps		Related Procedures and Topics
<b>Step 5</b>	Perform security-related configuration tasks for Cisco Unity voice messaging ports; for example, configure Cisco Unity to point to the Cisco TFTP server.	<i>Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x</i>
<b>Step 6</b>	Reset the devices in Cisco CallManager Administration and restart the Cisco Unity software.	<ul style="list-style-type: none"> <li><i>Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x</i></li> <li><a href="#">Applying a Security Profile to a Single Voice Messaging Port, page 10-3</a></li> </ul>

## Applying a Security Profile to a Single Voice Messaging Port

To apply a security profile to a single voice messaging port, perform the following procedure. This procedure assumes that you added the device to the database and installed a certificate in the phone, if a certificate does not already exist. After you apply a security profile for the first time or if you change the security profile, you must reset the device.

Before you apply a security profile, review the following sections:

- [Voice Messaging Security Overview, page 10-1](#)
- [Secure Voice Messaging Port Configuration Checklist, page 10-2](#)

### Procedure

- 
- Step 1** Find the voice messaging port, as described in the *Cisco CallManager Administration Guide*.
- Step 2** After the configuration window for the port displays, locate the **SCCP Phone Security Profile** setting. From the drop-down list box, choose the profile that you want to apply to the port.
- Step 3** Click **Save**.
- Step 4** Click **Reset**.
- 

### Additional Information

See the “[Related Topics](#)” section on page 10-4.

## Applying the Security Profile in the Voice Messaging Port Wizard

You cannot change the SCCP Phone Security Profile for existing voice messaging servers through the Voice Messaging Port Wizard. If you add ports to an existing voice-mail server, the device security mode that is currently configured for the profile automatically applies to the new ports.

To change the security setting for an existing voice-mail server, see the “[Applying a Security Profile to a Single Voice Messaging Port](#)” section on page 10-3.

Before you apply a security profile, review the following sections:

- [Voice Messaging Security Overview, page 10-1](#)
- [Secure Voice Messaging Port Configuration Checklist, page 10-2](#)

To apply the SCCP Phone Security Profile setting in the Voice Messaging Port Wizard for a new voice-mail server, perform the following procedure:

#### Procedure

- 
- Step 1** In Cisco CallManager Administration, choose **Voice Messaging > Voice Messaging Port Wizard**.
- Step 2** To add ports to a new voice-mail server, click the radio button that applies; click **Next**.
- Step 3** Enter the name of the voice-mail server; click **Next**.
- Step 4** Choose the number of ports that you want to add; click **Next**.
- Step 5** In the Device Information window, choose the profile that you want to apply from the SCCP Phone Security Profile drop-down list box. Configure the other device settings, as described in the *Cisco CallManager Administration Guide*. Click **Next**.
- Step 6** Continue the configuration process, as described in the *Cisco CallManager Administration Guide*. When the Summary window displays, click **Finish**.
- 

#### Additional Information

See the “[Related Topics](#)” section on page 10-4.

## Where to Find More Information

#### Related Topics

- [System Requirements, page 1-4](#)
- [Interactions and Restrictions, page 1-5](#)
- [Certificate Types, page 1-12](#)
- [Configuration Checklist Overview, page 1-19](#)
- [Voice Messaging Security Overview, page 10-1](#)
- [Applying a Security Profile to a Single Voice Messaging Port, page 10-3](#)
- [Applying the Security Profile in the Voice Messaging Port Wizard, page 10-3](#)

#### Related Cisco Documentation

- *Cisco CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco IP Telephony Platform Administration Guide*