CHAPTER 12

Configuring Voice-Messaging Ports for Security

This chapter contains information on the following topics:

Voice-Messaging Security Overview

To configure security for Cisco Unified Communications Manager voice-messaging ports and Cisco Unity SCCP devices or Cisco Unity Connection SCCP devices, you choose a secure device security mode for the port. If you choose an authenticated voice mail port, a TLS connection opens, which authenticates the devices by using a mutual certificate exchange (each device accepts the certificate of the other device). If you choose encrypted voice mail port, the system first authenticates the devices and then sends encrypted voice streams between the devices.

- For Cisco Unity or Cisco Unity Connection 1.2 or earlier, the Cisco Unity-Unified CM TSP connects to Cisco Unified Communications Manager through the TLS port when the device security mode equals authenticated or encrypted. When the device security mode equals nonsecure, the Cisco Unity-Unified CM TSP connects to Cisco Unified Communications Manager through the SCCP port.
- Cisco Unity Connection 2.0 or later connects to Cisco Unified Communications Manager through the TLS port. When the device security mode equals nonsecure, Cisco Unity Connection connects to Cisco Unified Communications Manager through the SCCP port.

Note In this document, the use of the term “server” refers to a Cisco Unified Communications Manager server. The use of the phrase “voice-mail server” refers to a Cisco Unity server or to a Cisco Unity Connection server.

Configuration Tips for Voice-Messaging Security

Consider the following information before you configure security:

- You must run Cisco Unity 4.0(5) or later with this version of Cisco Unified Communications Manager.
- You must run Cisco Unity Connection 1.2 or later with this version of Cisco Unified Communications Manager.
- For Cisco Unity, you must perform security tasks by using the Cisco Unity Telephony Integration Manager (UTIM); for Cisco Unity Connection, you must perform security tasks by using Cisco Unity Connection Administration. For information on how to perform these tasks, refer to the applicable Cisco Unified Communications Manager integration guide for Cisco Unity or for Cisco Unity Connection.
- In addition to the procedures that are described in this chapter, you must use the certificate management feature in Cisco Unified Communications Operating System to save the Cisco Unity certificate to the trusted store. For more information on this task, refer to the *Cisco Unified Communications Operating System Administration Guide.*

  After you copy the certificate, you must restart the Cisco CallManager service on each Cisco Unified Communications Manager server in the cluster.
- If Cisco Unity certificates expire or change for any reason, use the certificate management feature in the *Cisco Unified Communications Operating System Administration Guide* 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 Unified Communications Manager.
- When configuring voice-mail server ports, you must select a device security mode.
- The setting that you specify in the Cisco Unity Telephony Integration Manager (UTIM) or in Cisco Unity Connection Administration must match the voice-messaging port device security mode that is configured in Cisco Unified Communications Manager Administration. In Cisco Unity Connection Administration you apply the device security mode to the voice-messaging port in the Voice Mail Port Configuration window (or in the Voice Mail Port Wizard).

Tip If the device security mode settings do not match, the voice-mail server ports fail to register with Cisco Unified Communications Manager, and the voice-mail server cannot accept calls on those ports.

- Changing the security profile for the port requires a reset of Cisco Unified Communications Manager devices and a restart of the voice-mail server software. If you apply a security profile in Cisco Unified Communications Manager Administration that uses a different device security mode than the previous profile, you must change the setting on the voice-mail server.
- You cannot change the Device Security Mode for existing voice-mail servers through the Voice Mail 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.

Secure Voice-Messaging Port Configuration Checklist

Use Table 12-1 as a reference when you configure security for voice-messaging ports.

Table 12-1 Configuration Checklist for Securing Voice-Messaging Ports

Configuration Steps		Related Procedures and Topics
Step 1	Verify that you installed and configured the Cisco CTL Client for Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	Verify that you configured the phones for authentication or encryption.	Phone Security Overview, page 4-1 Configuring a Phone Security Profile, page 5-1
Step 3	Use the certificate management feature in Cisco Unified Communications Operating System Administration to copy the Cisco Unity certificate to the trusted store on the Cisco Unified Communications Manager server; then restart the Cisco CallManager service. **Tip** Activate the Cisco CTL Provider service on each Cisco Unified Communications Manager server in the cluster; then restart the Cisco CallManager service on all servers.	• Configuration Tips for Voice-Messaging Security, page 12-2 • *Cisco Unified Communications Operating System Administration Guide* • *Cisco Unified Serviceability Administration Guide*
Step 4	In Cisco Unified Communications Manager Administration, configure the device security mode for the voice-messaging ports.	• Applying a Security Profile to a Single Voice-Messaging Port, page 12-3 • Applying the Security Profile in the Voice Mail Port Wizard, page 12-4
Step 5	Perform security-related configuration tasks for Cisco Unity or Cisco Unity Connection voice-messaging ports; for example, configure Cisco Unity to point to the Cisco TFTP server.	Cisco Unified Communications Manager Integration Guide for Cisco Unity or for Cisco Unity Connection
Step 6	Reset the devices in Cisco Unified Communications Manager Administration and restart the Cisco Unity software.	• Cisco Unified Communications Manager Integration Guide for Cisco Unity or for Cisco Unity Connection • Applying a Security Profile to a Single Voice-Messaging Port, page 12-3

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 12-1
- Configuration Tips for Voice-Messaging Security, page 12-2
- Secure Voice-Messaging Port Configuration Checklist, page 12-2

Procedure

Step 1 Find the voice-messaging port, as described in the *Cisco Unified Communications Manager Administration Guide*.

Step 2 After the configuration window for the port displays, locate the **Device Security Mode** setting. From the drop-down list box, choose the security mode that you want to apply to the port. The database predefines these options. The default value specifies **Not Selected**.

Step 3 Click **Save**.

Step 4 Click **Reset**.

Additional Information

See the "Related Topics" section on page 12-5.

Applying the Security Profile in the Voice Mail Port Wizard

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 12-3.

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

- Voice-Messaging Security Overview, page 12-1
- Configuration Tips for Voice-Messaging Security, page 12-2
- Secure Voice-Messaging Port Configuration Checklist, page 12-2

To apply the Device Security Mode setting in the Voice Mail Port Wizard for a new voice-mail server, perform the following procedure:

Procedure

Step 1 Cisco Unified Communications Manager Administration, choose **Voice Mail > Voice Mail Port Wizard**.

Step 2 Enter the name of the voice-mail server; click **Next**.

Step 3 Choose the number of ports that you want to add; click **Next**.

Step 4 In the Device Information window, choose a Device Security Mode from the drop-down list box. The database predefines these options. The default value specifies Not Selected.

Step 5 Configure the other device settings, as described in the *Cisco Unified Communications Manager Administration Guide*. Click **Next**.

Step 6 Continue the configuration process, as described in the *Cisco Unified Communications Manager Administration Guide*. When the Summary window displays, click **Finish**.

Additional Information

See the "Related Topics" section on page 12-5.

Where to Find More Information

Related Topics

- System Requirements, page 1-5
- Interactions and Restrictions, page 1-6
- Certificates, page 1-14
- Configuration Checklist Overview, page 1-24
- Voice-Messaging Security Overview, page 12-1
- Configuration Tips for Voice-Messaging Security, page 12-2
- Applying a Security Profile to a Single Voice-Messaging Port, page 12-3
- Applying the Security Profile in the Voice Mail Port Wizard, page 12-4

Related Cisco Documentation

- *Cisco Unified Communications Manager Integration Guide* for Cisco Unity or Cisco Unity Connection for this Cisco Unified Communications Manager release
- *Cisco Unified Communications Operating System Administration Guide*