CHAPTER 3

Configuring Security for Cisco Visual Voicemail

Revised: March 2, 2010

- Configuration of Security for Visual Voicemail, page 3-1
- Adding the Security Service Parameter to the Visual Voicemail Service, page 3-2
- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2
- How to Obtain a Certificate for Visual Voicemail on Cisco Unity Connection, page 3-5
- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

Configuration of Security for Visual Voicemail

If you configure security for Visual Voicemail, the traffic between phones and the voicemail servers is secure. Visual Voicemail uses the HTTPS protocol instead of HTTP for traffic between phones and the voicemail servers.

Note When you configure security for Visual Voicemail, you use the Cisco CTL Client plug-in. The purpose of running the Cisco CTL Client plug-in is to sign the CTL file. This process does not configure secure messaging for your Cisco Unified Communications Manager, or change your Cisco Unified Communications Manager to secure mode or mixed mode.

Related Topics

- Visual Voicemail Security and Complex Configurations, page 3-1

Visual Voicemail Security and Complex Configurations

Your Cisco Unified Communications system might contain the following elements for failover, clustering, or to ensure that the system can be scaled:

- Multiple voicemail servers
- Multiple Cisco Unified Communications Manager servers

If your system contains these elements, you must repeat some of the installation steps described in this chapter. You must repeat steps on different servers. For example, you might need to configure a service parameter on multiple Cisco Unified Communications Manager servers.

Related Topics

- Configuration of Security for Visual Voicemail, page 3-1
- Configuring Cisco Visual Voicemail on Complex Systems with Failover, Clusters, and Multiple Servers

Adding the Security Service Parameter to the Visual Voicemail Service

Ensure that you added the use_secure_https_connection parameter to the Visual Voicemail service when you created the Visual Voicemail service.

If you did not add this parameter, you must delete the Visual Voicemail service, recreate the service, then add the use_secure_https_connection parameter to the Visual Voicemail service.

Related Topics

- Service Parameters for Visual Voicemail, page 2-10
- Adding the Visual Voicemail Service, page 2-11
- Updating Visual Voicemail Service Parameters, page 7-2

What to Do Next

- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2
- How to Obtain a Certificate for Visual Voicemail on Cisco Unity Connection, page 3-5

How to Obtain a Certificate for Visual Voicemail on Cisco Unity

- Creating a Certificate Request for the Cisco Unity Server, page 3-2
- Submitting the Certificate Request to a Certificate Authority, page 3-3
- Installing the Certificate on the Cisco Unity Server, page 3-4
- Downloading the IIS Certificate from Cisco Unity, page 3-4

Creating a Certificate Request for the Cisco Unity Server

Procedure

Step 1 Start Internet Information Services Manager.

Step 2 Select the Cisco Unity server in the left pane.

Step 3 Select **Web Sites**.

Step 4 Right-click **Default Web Site**, then select **Properties**.

Step 5 Select the **Directory Security** tab.

Step 6 Select **Security Certificate**.

This starts a wizard that you can use to create the certificate request.

Step 7 Select **Create a new certificate**, then select **Next**.

Step 8 Select **Prepare the request now, but send it later**, then select **Next**.

Step 9 Type a name for the certificate, then select **Next**.

For example, type the hostname as the name of the certificate.

Step 10 Enter information about your organization, then select **Next**.

Step 11 Enter the fully-qualified domain name of the Cisco Unity server in the Common name field, then select **Next**.

Step 12 Enter your geographical information, then select **Next**.

Step 13 Enter a filename for the certificate request, then select **Next**.

Step 14 Check the details of your certificate request on the Request File Summary screen, then select **Next**.

Step 15 Select **Finish**.

Related Topics

- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2

What to Do Next

- Submitting the Certificate Request to a Certificate Authority, page 3-3

Submitting the Certificate Request to a Certificate Authority

Procedure

Step 1 Begin the process to submit a certificate on your certificate authority web site.

Step 2 Copy the contents of the certificate request text file.

Step 3 Paste the contents into the appropriate field on your certificate authority web site.

Step 4 Submit your request.

Step 5 Locate the certificate request on your certificate authority web site.

Step 6 If the certificate has been issued, download the certificate to a folder on your Cisco Unity server.

Related Topics

- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2

What to Do Next

- Installing the Certificate on the Cisco Unity Server, page 3-4

Installing the Certificate on the Cisco Unity Server

Procedure

Step 1 Start Internet Information Services Manager.

Step 2 Select the Cisco Unity server in the left pane.

Step 3 Select **Web Sites**.

Step 4 Right-click **Default Web Site**, then select **Properties**.

Step 5 Select the **Directory Security** tab.

Step 6 Select **Security Certificate**.

This starts a wizard that you can use to install the certificate.

Step 7 Select **Process the pending request and install the certificate**, then select **Next**.

Step 8 Enter the location of the certificate file, then select **Next**.

Step 9 Enter **443** as SSL port, then select **Next**.

Step 10 Check the details of your certificate on the Certificate Summary screen, then select **Next**.

Step 11 Select **Finish**.

Related Topics

- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2

What to Do Next

- Downloading the IIS Certificate from Cisco Unity, page 3-4

Downloading the IIS Certificate from Cisco Unity

Procedure

Step 1 Start a browser on the Cisco Unity server.

Step 2 Use the HTTPS protocol to access the URL of the Cisco Unity server.

You can access the URL structured as follows:

https://<*localhost*>

For example, access:

https://unityserver/

Step 3 Select **View Certificate** on the security dialog box.

Step 4 Select the **Details** tab.

Step 5 Select **Copy to File**.

Step 6 Select **DER encoded binary X.509 (.CER)**, then select **Next**.

Step 7 Enter a filename for the certificate, then select **Next**.

Step 8 Verify the details of your certificate on the Completing the Certificate Export Wizard screen, then select **Finish**.

Related Topics

- How to Obtain a Certificate for Visual Voicemail on Cisco Unity, page 3-2

What to Do Next

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

How to Obtain a Certificate for Visual Voicemail on Cisco Unity Connection

- Downloading the Tomcat Certificate from Cisco Unity Connection, page 3-5

Downloading the Tomcat Certificate from Cisco Unity Connection

Procedure

Step 1 Select **Security > Certificate Management** in Cisco Unified Operating System Administration.

Step 2 Find the Tomcat certificate.

Step 3 Select the **tomcat.der** link.

Step 4 Select **Download**, then save the tomcat.der file to your computer.

What to Do Next

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

How to Add Certificates to Cisco Unified Communications Manager and Your Phones

To ensure that the traffic between the Visual Voicemail application and the voicemail server is encrypted, you must do the following:

1. Upload the certificate to your Cisco Unified Communications Manager.
2. Sign the Certificate Trust List (CTL) file on the Cisco Unified Communications Manager.
3. Restart the Cisco Unified Communications Manager and TFTP servers to update the trust list on the phones in your system.

The phones trust the certificates in the CTL file, so the phones can make secure connections to the server specified in the certificate.

Related Topics

- Uploading Certificates to Cisco Unified Communications Manager, page 3-6
- Checking the Certificate on Cisco Unified Communications Manager, page 3-6
- Signing the CTL File on Cisco Unified Communications Manager, page 3-7
- Restarting the Cisco Unified Communications Manager and TFTP Servers, page 3-9
- Checking That the CTL File Is On Phones in Your System, page 3-9

Uploading Certificates to Cisco Unified Communications Manager

Procedure

Step 1 Select **Security > Certificate Management** in Cisco Unified Operating System Administration.

Step 2 Select **Upload Certificate**.

Step 3 Select **Phone-trust** from the Certificate Name list box.

Step 4 Enter a description for the certificate in the **Description** field.

For example, enter **Unity Connection Tomcat Certificate** or **Unity IIS Certificate**.

Step 5 Enter the path to the certificate you downloaded in the Upload File field.

Step 6 Select **Upload File**.

Step 7 Select **Close**.

Related Topics

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

What to Do Next

- Checking the Certificate on Cisco Unified Communications Manager, page 3-6

Checking the Certificate on Cisco Unified Communications Manager

Procedure

Step 1 Select **Security > Certificate Management** in Cisco Unified Operating System Administration.

Step 2 Select **Find** to display a list of all security certificates.

Step 3 Locate the certificate that you uploaded. The certificate has the following values:

Field	Value
Certificate Name	Phone-trust
Certificate Type	trust-certs
.PEM File	<*hostname-of-Cisco Unity-or-Cisco Unity Connection-system*>.pem
.DER File	<*hostname-of-Cisco Unity-or-Cisco Unity Connection-system*>.der
Description	Trust certificate

Related Topics

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

What to Do Next

- Signing the CTL File on Cisco Unified Communications Manager, page 3-7

Signing the CTL File on Cisco Unified Communications Manager

Before You Begin

You must sign the CTL file. To do this, you need at least one security eToken. If this is the first time that the CTL file is being signed, you need two security eTokens.

The purpose of running the Cisco CTL Client plug-in is to sign the CTL file. This process does not configure secure messaging for your Cisco Unified Communications Manager, or change your Cisco Unified Communications Manager to secure mode or mixed mode.

The CTL file is signed so that the IP phone trusts the voicemail server certificate in the CTL file, and allows the phone to establish secure HTTPS connections to the voicemail server

Note Even if the phones in your system already had a CTL installed, you must sign the modified CTL file after you upload the certificate to the Cisco Unified Communications Manager.

For more information about the Cisco CTL Client plug-in, see the *Cisco Unified Communications Manager Security Guide* at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Procedure

Step 1 Select **Application > Plugins** in Cisco Unified Communications Manager Administration.

Step 2 Select **Find**.

Step 3 Download the **Cisco CTL Client** plug-in to your computer.

Step 4 Run the Cisco CTL Client installer application.

Step 5 Start the Cisco CTL Client application.

Step 6 Enter the details of the publisher server on the **Cisco Unified Communications Manager Server** tab, then select **Next**.

Field	Value
Hostname or IP Address	Enter the IP address of the Cisco Unified Communications Manager publisher server to which you uploaded the certificate in Uploading Certificates to Cisco Unified Communications Manager, page 3-6.
Port	Enter the port of the Cisco Unified Communications Manager publisher server to which you uploaded the certificate. The default value is 2444. You do not need to change this value.
Username	Enter the administrator username for the Cisco Unified Communications Manager Administration application.
Password	Enter the administrator password for the Cisco Unified Communications Manager Administration application.

Step 7 Select **Update CTL File** on the Cluster Security Mode tab, then select **Next**.

A message box prompts you to insert a security token.

Step 8 Insert a security eToken into your computer, then select **OK** on the message box.

Select **Add** or **Next** on the Security Token Information tab.

Step 9 Check that the CTL file is listed on the CTL Entries tab.

Verify that the hostname or address that you entered in Step 6 is present in the Subject column of one of the entries.

Step 10 Select **Finish**.

If this is the first time that the CTL file is being signed, you are prompted to sign with two eTokens, as follows:

1. Select **OK** on the prompt message box.
2. Select **Add Tokens** on the CTL Entries tab.
3. Select **OK** on the prompt message box.
4. Remove the first eToken from your computer.
5. Insert the second security eToken into your computer.
6. Select **Add** on the Security Token Information tab.
7. Select **Finish**.

Step 11 Enter the password for the eToken in the Log On: eToken dialog box.

The default password for the eToken is provided with the eToken.

Step 12 Select **OK**.

Step 13 Select **Done** on the dialog box that shows the location of the CTL file.

Related Topics

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

What to Do Next

- Restarting the Cisco Unified Communications Manager and TFTP Servers, page 3-9

Restarting the Cisco Unified Communications Manager and TFTP Servers

After you sign the CTL file, restart the Cisco Unified Communications Manager services and Cisco TFTP services in Cisco Unified Serviceability. Restart the TFTP and Cisco Unified Communications Manager services on all nodes in the cluster that run these services.

Related Topics

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

What to Do Next

- Checking That the CTL File Is On Phones in Your System, page 3-9

Checking That the CTL File Is On Phones in Your System

Procedure

Step 1 Press the Settings button on any phone in your network.

Step 2 Select **Security Configuration**.

Step 3 Select **Trust List**.

Step 4 Check that the value of one of the Application Server entries is the hostname of your Cisco Unity or Cisco Unity Connection server.

Related Topics

- How to Add Certificates to Cisco Unified Communications Manager and Your Phones, page 3-5

What to Do Next

- Installing Cisco Visual Voicemail on Phones