Configuring System Security

You can use the Cisco Voice Provisioning Tool to provide administrators a central point of access to sensitive provisioning information (such as user passwords and other information) on multiple product systems in different locations. For this reason, you should ensure that both the connection between the administrator and the tool and the connections between the tool and the product systems are secure. If any of these connections takes place across the boundaries of a secure network, you must take additional steps to ensure that these connections are secured. This chapter explains those steps, as well as additional steps that you should take to ensure that the passwords that are used to restrict access to the tool are secure at all times.

This chapter covers the following topics:

- Configuring Browser Security, page 4-1
- Configuring Secure Communication with Product Systems, page 4-4
- Password Security, page 4-12

Configuring Browser Security

You can use the Secure Sockets Layer (SSL) to provide an authenticated, encrypted connection between the web clients that administrators use and the Cisco Voice Provisioning Tool. Without SSL in place, passwords and other potentially sensitive provisioning information may be passed in plain text across the network.

When first installing the tool, you can choose whether to enable SSL on this connection. If you need to change the configuration after installation, use one of the following sections:

- Configuring SSL for the Cisco Voice Provisioning Tool Web Application After Installation, page 4-2
- Removing SSL from the Cisco Voice Provisioning Tool Web Application After Installation, page 4-4

Configuring SSL for the Cisco Voice Provisioning Tool Web Application After Installation

To configure the Tomcat web server so that it communicates with the client web browser over a secure connection, perform the following procedure.

To Configure SSL for the Cisco Voice Provisioning Tool Web Application

Step 1 On the VPT server, verify that the PATH environment variable on the system includes the path to the bin directory of the JDK that is installed with VPT:

a. On the Windows Start menu, choose **Settings > Control Panel > System**.

b. Click the **Advanced** tab.

c. Click **Environment Variables**.

d. In the System Variables list, find and click the **Path** variable and click **Edit**.

e. If it is not already present in the path, add the full path to the bin directory of the JDK that is installed with VPT. Make sure that a semicolon (;) separates the new entry from any other entries. For example, if the JDK was installed in C:\j2sdk1.4.2_03, add the following to the end of the path: **;C:\j2sdk1.4.2_03\bin**

f. Click **OK**.

g. Close the System Properties and Control Panel windows.

Step 2 Verify that the JDK tools are available by using the path specified in Step 1:

a. On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.

b. In the command prompt window, enter **javac**. If the path is set correctly, usage information for the javac command displays.

Step 3 Add a root certificate to the keystore for the VPT server by doing the applicable steps:

- Create and add a self-signed certificate. Continue with Step 4.
- Install a certificate from a Certificate Authority. Skip to Step 5.

Step 4 If you are creating a self-signed certificate, do the following substeps:

a. Enter
keytool -genkey -alias tomcat -keyalg RSA -keystore <keystore file name>
and press **Enter**.

Note The keystore file name should include the full path to the keystore file and must not contain any spaces.

b. Follow the prompts to enter a keystore password, your name, organizational and location information, and a key password.

Note The keystore password and key password must match.

c. Close the command prompt window. Skip to Step 6.

Step 5 If you are have obtained a certificate from a Certificate Authority, do the following substeps:

a. Enter
keytool -import -alias tomcat -keyalg RSA -keystore <keystore file name> -trustcacerts -file <certificate file name>
and press **Enter**.

Note The keystore file name must not contain any spaces. The certificate file name must be an absolute path to your certificate file and should not contain any spaces.

b. Follow the prompt to enter the keystore password.

Note The keystore password must match the certificate password.

c. If the password that you entered is correct, you will be presented with the information on the certificate that you are importing and asked whether you trust the certificate. Enter **y** and press **Enter** to trust the certificate. If the password that you entered is not correct, repeat Steps a. and b.

d. Close the command prompt window.

Step 6 Browse to the <VPT installation root>\tomcat\conf directory.

Step 7 Use a text editor to open the **server.xml** file.

Step 8 Find **non-SSL Coyote HTTP/1.1 Connector**. Replace all the text that begins with **<Connector** and ends with **/>** with the following:
<Connector port="8443" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" disableUploadTimeout="true" URIEncoding="UTF-8" useBodyEncodingForURI="true" acceptCount="100" debug="0" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="<keystore file name>" keystorePass="<keystore password>" />

Note Port 8443 is the recommended port. If this port is already in use by another process, choose a different port.

Note The keystore file name and keystore password must match the values that you chose in Step 4 or Step 5.

Step 9 Save and close the **server.xml** file.

Step 10 For the changes to take effect, you must restart the VPT Tomcat service. On the Windows Start menu, choose **Programs > Administrative Tools > Services**. In the right pane, locate **VPT Tomcat**, right-click it, and click **Restart**.

Step 11 To verify the changes, open a web browser and browse to **https://<server name or IP address>:<port number>/vpt**.

Removing SSL from the Cisco Voice Provisioning Tool Web Application After Installation

To configure the Tomcat web server so that it communicates with the client web browser over a non-secure connection, perform the following procedure.

To Remove SSL from the Cisco Voice Provisioning Tool Web Application

Step 1 On the VPT server, browse to the <VPT installation root>\tomcat\conf directory.

Step 2 Use a text editor to open the **server.xml** file.

Step 3 Find **SSL Coyote HTTP/1.1 Connector**. Replace all the text that begins with **<Connector** and ends with **/>** with the following:
<Connector port="8080" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false" redirectPort="8443" acceptCount="100" debug="0" connectionTimeout="20000" URIEncoding="UTF-8" useBodyEncodingForURI="true" disableUploadTimeout="true" />

Note Port 8080 is the recommended port. If this port is already in use by another process, choose a different port.

Step 4 Save and close the **server.xml** file.

Step 5 For the changes to take effect, you must restart the VPT Tomcat service. On the Windows Start menu, choose **Programs > Administrative Tools > Services**. In the right pane, locate **VPT Tomcat**, right-click it, and click **Restart**.

Step 6 To verify the changes, open a web browser and browse to **http://<server name or IP address>:<port number>/vpt**.

Configuring Secure Communication with Product Systems

To implement security between the Cisco Voice Provisioning Tool and individual product systems, use one of the following mechanisms:

- Secure Sockets Layer (SSL) is recommended for use with Cisco Unity product systems. See the "SSL" section on page 4-4.
- IP Security (IPSec) provides a security alternative for use with Cisco CallManager systems that are separated from the VPT server by non-secure networks. See the "IPSec" section on page 4-12.

SSL

You can implement security between the Cisco Voice Provisioning Tool and individual Cisco Unity product systems by using the Secure Sockets Layer (SSL) protocol. SSL provides secure transmission of data across the network through the use of public/private key encryption.

Configuring a Product System for SSL

To configure SSL on the link between VPT and a product system, you must first configure SSL on the individual product system.

Note As of the first release of the Cisco Voice Provisioning Tool, only the Cisco Unity 4.0(5) plug-in supports SSL. For information on configuring SSL on Cisco Unity, see the *Cisco Unity Security Guide*.

If failover is in use, and SSL is configured on the primary server, it must also be configured on the secondary server for VPT to communicate with the secondary server if the primary server is unavailable.

After SSL has been configured on the product system, and a certificate has been procured or generated for the product system, do the following tasks to set up secure communication with the product system on the VPT server:

1. If you do not already have access to a copy of the server certificate(s), export a copy. See the "Exporting Certificates for Each Product System" section on page 4-5.
2. Copy certificates for each Cisco Unity product system to the VPT server. See the "Copying Certificates for Each Product System" section on page 4-7.
3. Add the product system certificate(s) to a keystore on the VPT server. See the "Entering Product System Certificates in the VPT Keystore" section on page 4-7.
4. Configure the keystore properties in the Cisco Voice Provisioning Tool. See the "Configuring Keystore Information in the Cisco Voice Provisioning Tool" section on page 4-9.
5. Configure the product system settings to use SSL in the Cisco Voice Provisioning Tool. See the "Configuring the Product Systems to use SSL in the Cisco Voice Provisioning Tool" section on page 4-9.
6. Test the product system. See the "Testing the Product System" section on page 4-10.

Exporting Certificates for Each Product System

Whether certificates were generated by using a Certificate Authority (CA) or were generated as self-signed certificates, you need to obtain a copy of the certificate to add to the VPT keystore. If self-signed certificates are used, you will need to export a copy of each server certificate (if failover is in use, you will need a copy from both the primary and secondary Cisco Unity servers). If your enterprise has a Certificate Authority, you generally will only need to obtain and add the CA root certificate to the keystore once.

Do one of the following procedures, depending on the mechanism that is used to generate the certificate(s):

- To Export a Certificate Generated by a Certificate Authority (CA), page 4-5
- To Export Self-Signed Certificates, page 4-6

To Export a Certificate Generated by a Certificate Authority (CA)

Step 1 On the CA server, on the Windows Start menu, choose **Programs > Administrative Tools > Certification Authority**.

Step 2 In the left pane of the Certification Authority window, right-click the <Root Certification Authority name> and click **Properties**.

Step 3 Click **View Certificate**.

Step 4 Click the **Details** tab.

Step 5 In the Show list, choose **All** and click **Copy to File**.

Step 6 On the Certificate Export wizard welcome window, click **Next**.

Step 7 Click **Base-64 Encoded X.509 (.CER)** and click **Next**.

Step 8 Specify a file name and a location and click **Next**.

Step 9 Verify the settings and click **Finish**.

Step 10 To close the Certificate Details dialog box, click **OK**.

Step 11 To close the Properties dialog box for the Root Certification Authority, click **OK**.

Step 12 Close the **Certification Authority** window.

To Export Self-Signed Certificates

Step 1 On the Cisco Unity server, on the Windows Start menu, choose **Programs > Administrative Tools > Internet Services Manager**. (If failover is in use, begin this procedure on the primary Cisco Unity server and repeat the procedure on the secondary server.)

Step 2 Double-click the name of the Cisco Unity server to expand it.

Step 3 Right-click **Default Web Site** and click **Properties**.

Step 4 In the Default Web Site Properties dialog box, click the **Directory Security** tab.

Step 5 Click **View Certificate**.

Step 6 Click the **Details** tab.

Step 7 In the Show list, choose **All** and click **Copy to File**.

Step 8 On the Certificate Export wizard welcome window, click **Next**.

Step 9 Click **No, Do Not Export the Private Key** and click **Next**.

Step 10 Click **Base-64 Encoded X.509 (.CER)** and click **Next**.

Step 11 Specify a file name and a location and click **Next**.

Step 12 Verify the settings and click **Finish**.

Step 13 To close the Certificate Details dialog box, click **OK**.

Step 14 To close the Properties dialog box for the Root Certification Authority, click **OK**.

Step 15 To close the Certificate window, click **OK**.

Step 16 To close the Default Web Site Properties window, click **OK**.

Step 17 Close the **Internet Information Services** window.

Step 18 If failover is in use, repeat Step 1 through Step 17 on the secondary Cisco Unity server.

Copying Certificates for Each Product System

Use the following procedure to copy certificates from each product system to the VPT server.

To Copy Certificates for Each Product System

Step 1 Copy the certificate(s) to the VPT server by doing the applicable steps:

- Recommended—By using a floppy disk. Continue with Step 2.
- For secure networks—By using a network share. Skip to Step 3.

Step 2 If you are using a floppy disk to copy the certificate, do the following substeps:

a. Insert an empty formatted floppy disk in the floppy drive of the Cisco Unity or CA server.

b. Browse to the directory that contains the certificate (.CER) file(s).

c. Copy the certificate file(s) to the floppy disk.

d. Remove the floppy disk from the Cisco Unity or CA server.

e. Insert the floppy disk in the floppy drive of a VPT server.

f. Copy the certificate file(s) on the floppy disk to a directory on the VPT server.

g. For security, delete the certificate file(s) on the floppy disk.

Step 3 If you are using a secure network share to copy the certificate(s), do the following substeps:

a. On the Cisco Unity or CA server, browse to the directory that contains the certificate.

b. Choose the certificate file, and press **Ctrl-C**.

c. Open a network share to the VPT server and log on.

d. Browse to or create a directory on the VPT server in which to store certificates.

e. To paste the certificate file, press **Ctrl-V**.

Entering Product System Certificates in the VPT Keystore

To configure VPT to communicate with product systems by using SSL, you must use the keytool application that is included as part of the Sun Microsystems Java Development Kit (JDK) when you install the Cisco Voice Provisioning Tool.

The keytool application creates a keystore (by default, the keystore is stored as a file). You can store multiple certificates in a keystore; the keystore automatically is created when you add the first certificate by using the keytool application. For more information on the keytool command, refer to the Sun Microsystems Java Development Kit documentation.

To Add Certificates to a Key Store by Using Keytool

Step 1 On the VPT server, verify that the PATH environment variable on the system includes the path to the bin directory of the JDK that is installed with VPT:

a. On the Windows Start menu, choose **Settings > Control Panel > System**.

b. Click the **Advanced** tab.

c. Click **Environment Variables**.

d. In the System Variables list, find and click the **Path** variable and click **Edit**.

e. If it is not present in the path, add the full path to the bin directory of the JDK that is installed with VPT. Make sure that a semicolon (;) separates the new entry from any other entries. For example, if the JDK was installed in C:\j2sdk1.4.2_03, add the following to the end of the path:
;C:\j2sdk1.4.2_03\bin

f. Click **OK**.

g. Close the System Properties and Control Panel windows.

Step 2 Verify that the JDK tools are available by using the path specified in Step 1:

a. On the Windows Start menu, choose **Programs > Accessories > Command Prompt**.

b. In the command prompt window, enter **javac**. If the path is set correctly, usage information for the javac command displays.

Step 3 In the command prompt window that opened in Step 2, change to the directory where the Cisco Voice Provisioning Tool is installed. For example, enter:
cd C:\Program Files\Cisco Systems\Voice Provisioning Tool
and press **Enter**.

Step 4 Enter
keytool -import -alias <Server Name> -storepass <Password> -File <Certificate File> -keystore <Keystore File>
and press **Enter**.

We recommend that you use the name of the product system or certificate authority from which the certificate was obtained for the alias. For example, if a self-signed certificate file from server c-unity1 is stored in C:\certificates\c-unity1-cert.CER, you might enter: keytool -import -alias c-unity1 -storepass pa$$w0rd! -File C:\certificates\c-unity1-cert.CER -keystore C:\VPTProdSysKeystore.

Note The -keystore parameter specifies a file that holds the keystore. If you do not specify a full path, the file is created in the directory in which you run the keytool command. You will need to know the full path to the keystore file to configure the VPT security settings in the next procedure.

Step 5 When prompted to trust the certificate, enter **yes** and press **Enter**.

Step 6 To verify that the import was successful, enter
keytool -list -keystore <Keystore File>
and press **Enter**.

Step 7 Repeat Step 4 through Step 6 for each product system certificate.

Note Ensure all product system keys are stored in the same keystore for the Cisco Voice Provisioning Tool to access them. Make sure that you use the correct syntax for the keystore value each time that you enter a new certificate.

Step 8 Close the command prompt window.

Configuring Keystore Information in the Cisco Voice Provisioning Tool

Note To configure keystore settings, your administrator account must belong to a role that has VPT Configuration Modify permissions for the VPT application. If you do not see the VPT Administration > Configuration option in the VPT navigation menu, your account does not have the applicable permissions.

To Configure Keystore Information in the Cisco Voice Provisioning Tool

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Configuration**.

The Configuration window displays.

Step 2 In the Security settings section, enter the full path of the keystore and the password that you specified in Step 4 of the "To Add Certificates to a Key Store by Using Keytool" procedure on page 4-7.

Step 3 Click **Save**.

Step 4 For the changes to take effect, you must restart the VPT Tomcat service. On the Windows Start menu, choose **Programs > Administrative Tools > Services**. In the right pane, locate **VPT Tomcat**, right-click it, and click **Restart**.

Configuring the Product Systems to use SSL in the Cisco Voice Provisioning Tool

If you have not yet added the product system to the Cisco Voice Provisioning Tool, see the "Adding a Cisco Unity Server" section on page 3-3.

If the product system is already configured in the Cisco Voice Provisioning Tool, you can change the security settings from the Manage Product Systems window, as follows:

Note To configure product system settings, your administrator account must belong to a role that has Product Systems Management Modify and View permissions for the VPT application. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Configure a Product System to use SSL

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays.

Step 2 Click the name of the product system that you want to modify.

Note As of the first release of the Cisco Voice Provisioning Tool, only product systems of type UNITY-4.0.5 support SSL.

Step 3 If the URL for the Cisco Unity Administrator changed because of the change in security settings, enter the new URL as the Product SA URL.

Step 4 Change the Unity CUAL port. Typically, the port number for SSL is 443. If failover is configured, you must also change the failover CUAL port (for the secondary Cisco Unity server).

Step 5 In the Security drop-down menu, choose **SSL**.

Step 6 Click **Save**.

Testing the Product System

After you have configured the product system and the Cisco Voice Provisioning Tool to enable SSL on a product system connection, you should test the connection to verify that the setup is working correctly.

Note To test product system connections, your administrator account must belong to a role that has Product System Connection Test permissions for the product system. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Test the Product System Connection

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays a list of configured product systems.

Step 2 Click the Test button in the Test Connection column of the product system that you want to test. If the test is successful, you should see a PASSED result for all tests.

Removing SSL from Product Systems

If SSL has been configured on a Cisco Unity product system and you want to remove it, do the following tasks:

1. Remove SSL from the product system server. Refer to the *Cisco Unity Security Guide* for instructions. If failover is in use, you must also remove SSL from the secondary Cisco Unity server.
2. Change the product system settings for the Cisco Unity server to reflect the removal of SSL. See the "Removing SSL from the Product System Configuration in the Cisco Voice Provisioning Tool" section on page 4-10.
3. Test the product system. See the "Testing the Product System" section on page 4-11.

Removing SSL from the Product System Configuration in the Cisco Voice Provisioning Tool

If you have not yet added the product system to the Cisco Voice Provisioning Tool, see the "Adding a Cisco Unity Server" section on page 3-3.

If the product system is already configured in the Cisco Voice Provisioning Tool, you can change the security settings from the Manage Product Systems window, as follows.

Note To configure product system settings, your administrator account must belong to a role that has Product Systems Management Modify and View permissions for the VPT application. If you do not see the VPT Administration > Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Remove SSL from a Product System

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays.

Step 2 Click the name of the product system that you want to modify.

Step 3 If the URL for the Cisco Unity Administrator changed because of the change in security settings, enter the new URL as the Product SA URL.

Step 4 Change the Unity CUAL port. Typically, the port number when SSL is not enabled is 80. If failover is configured, you must also change the failover CUAL port (for the secondary Cisco Unity server).

Step 5 In the Security drop-down menu, choose **No Security**.

Step 6 Click **Save**.

Testing the Product System

After you have configured the product system and the Cisco Voice Provisioning Tool to remove SSL from the product system connection, you should test the connection to verify that the setup is working correctly.

Note To test product system connections, your administrator account must belong to a role that has Product System Connection Test permissions for the product system. If you do not see the VPT Administration > Product Systems > Manage Product Systems option in the VPT navigation menu, your account does not have the applicable permissions.

To Test the Product System Connection

Step 1 In the Cisco Voice Provisioning Tool, choose **VPT Administration > Product Systems > Manage Product Systems**.

The Manage Product Systems window displays a list of configured product systems.

Step 2 Click the Test button in the Test Connection column of the product system that you want to test. If the test is successful, you should see a PASSED result for all tests.

IPSec

If the traffic between the Cisco Voice Provisioning Tool server and one or more Cisco CallManager product systems will traverse a non-secure network, you can implement IPSec to protect sensitive provisioning configuration data (such as user names, passwords, and PINs).

IPSec is a secure connection protocol that provides authentication and/or encryption at the IP layer between two hosts, or between a host and a security gateway (such as a firewall or router). For securing the connection between VPT and a Cisco CallManager server, we recommend that you implement IPSec between the VPT host and the network infrastructure for the Cisco CallManager server, rather than between the VPT host and the Cisco CallManager server.

You can enable IPSec on the VPT server by using Windows 2000 IPSec tunneling. Refer to the Microsoft Windows 2000 Help for IPSec tunneling configuration details.

For information on configuring the network infrastructure for the Cisco CallManager server, refer to the *Cisco CallManager Security Guide*.

Password Security

The Cisco Voice Provisioning Tool provides built-in features to help you ensure password security. However, because access to and use of the tool involves other network and system components, external security factors can also affect the security of the passwords that are used by and for the tool. When implementing a security policy for VPT, you should understand the mechanisms that VPT provides, as well as the actions you can take to ensure password security.

Password Security Features Provided by the Cisco Voice Provisioning Tool

The Cisco Voice Provisioning Tool provides the following password security features:

- The tool automatically validates all administrator passwords for security. All passwords require a minimum password length of 8 characters (and maximum of 80 characters). In addition, passwords must contain characters taken from at least three of the following character classes:
  - Symbols—for example, !"#$%&'()*+,-./
  - Numbers—0 to 9
  - Upper-case letters—A to Z
  - Lower-case letters—a to z
- The tool also checks all passwords for the following restrictions:
  - No character in the password can repeat more than three times consecutively.
  - The password cannot match the user name (Admin ID), either spelled forwards or backwards.
- The tool always prompts new administrators to change their passwords when they first log in to the system.
- Any time that an administrator password has been reset by another user, at the next login, the administrator will be prompted to change the new password.

- Administrators with sufficient permissions can disable other administrator accounts, which allows the administrator data to remain in the system while locking out the administrator. The change takes effect immediately (any operations already in progress by the administrator will complete, but at the next attempt to browse to another page or submit another action, the disabled administrator will be logged out of the system).

Actions You Should Take to Ensure Password Security

After installing the Cisco Voice Provisioning Tool, you should take the following actions:

- Immediately log in as superadmin and change the superadmin password (the initial password that you set during the installation process is a temporary password; the first time you log in as superadmin you will be required to change it).
- Configure SSL on the VPT website and SSL or IPSec on the product system interfaces. When administrators log in to the Cisco Voice Provisioning Tool, their credentials are sent across the network to the tool in clear text, unless SSL is configured for the VPT website. In addition, the information that administrators enter on the windows of the tool is not encrypted unless secure communications mechanisms are in use on both the VPT website and the product system connections.
- Assign unique passwords to new administrator accounts as you create them (rather than repeatedly reusing the same default password).
- Encourage administrators to log in and change their passwords as quickly as possible after creating their accounts.
- Make sure that administrators use strong passwords in templates for end-user provisioning, and that end-user access points use secure methods to transmit passwords across the network. Refer to the *Cisco CallManager Security Guide* and the *Cisco Unity Security Guide* for further details.