



Setting Up Cisco Unity to Use SSL

Determining Whether to Set Up Cisco Unity to Use SSL

When subscribers log on to the Cisco Personal Communications Assistant (PCA), their credentials are sent across the network to Cisco Unity in clear text. The same is true when the Cisco Unity Administrator and the Status Monitor use the Anonymous authentication method. In addition, the information that subscribers enter on the pages of the Cisco PCA and the Cisco Unity Administrator is not encrypted, regardless of which authentication method it uses.

For increased security, we recommend that you set up Cisco Unity to use the Secure Sockets Layer (SSL) protocol, if the Cisco Unity installer has not already done so during installation.

SSL uses public-key encryption to provide a secure connection between servers and clients, and uses digital certificates to authenticate servers, or servers and clients. A digital certificate is a file containing encrypted data that attests to the identity of an organization or entity, such as a computer. Use of the SSL protocol ensures that all subscriber credentials—as well as the information that a subscriber enters on any page of the Cisco Unity Administrator or the Cisco PCA—are encrypted as the data is sent across the network. In addition, when Cisco Unity is set up to use SSL, each time that a subscriber tries to access any Cisco Unity web application, the browser will confirm that it is connected to the real Cisco Unity server—and not an entity falsely posing as such—before allowing the subscriber to log on.

To set up a web server such as Cisco Unity to use SSL, you can either obtain a digital certificate from a Certificate Authority (CA), or use Microsoft Certificate Services (available with Windows) to issue your own certificate. A CA is a trusted organization or entity that issues and manages certificates at the request of another organization or entity. Cost, certificate features, ease of setup and maintenance, and the security policies practiced by your organization are some of the issues to consider when determining whether you should purchase a certificate from a CA or issue your own.

Information on third-party CAs, Microsoft Certificate Services, and SSL is widely available on the Internet, as well as in the Microsoft Windows and IIS online documentation. Such sources can help you determine whether to use SSL and how to set up a web server to use it.

This chapter contains procedures for using Microsoft Certificate Services to issue your own certificate, and for setting up Cisco Unity to use it. See the following sections in this chapter for more information:

- [Setting Up Cisco Unity to Use SSL, page 4-2](#)
- [Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain \(Optional\), page 4-5](#)

Setting Up Cisco Unity to Use SSL

If you purchased a certificate from a CA, refer to the procedures provided by the CA to set up a web server to use it.

To use Microsoft Certificate Services to issue your own certificate and to enable Cisco Unity to use SSL, do the procedures in this section in the order listed.

Note that Microsoft Windows and IIS online documentation offer procedures similar to the ones presented in this section. The Microsoft documentation also contains procedures on how to install, configure, and use Certificate Services, and to enable a web server to use SSL in alternative ways—some of which may be more applicable to your organization than the method presented here.

To Install the Microsoft Certificate Services Component

-
- Step 1** On the server that will function as your Certificate Authority (CA) and issue certificates, on the Windows Start menu, click **Settings > Control Panel > Add/Remove Programs**.
 - Step 2** Click **Add/Remove Windows Components**.
 - Step 3** In the Windows Components dialog box, check the **Certificate Services** check box. Do not change any other items. When a warning appears about not being able to rename the computer, or join or be removed from a domain, click **Yes**.
 - Step 4** Click **Next**.
 - Step 5** Click **Stand-alone Root CA**, and click **Next**.
A stand-alone CA is a CA that does not require Active Directory.
 - Step 6** Follow the on-screen prompts to complete the installation. For information, refer to the Windows documentation.
If a message appears that Internet Information Services is running on the computer and must be stopped before proceeding, click **OK** to stop the service.
 - Step 7** In the Completing the Windows Components Wizard dialog box, click **Finish**.
 - Step 8** Close the Add/Remove Programs dialog box and the Control Panel.
-

To Create a Certificate Request

-
- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
 - Step 2** Double-click <System-name> 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** Under Secure Communications, click **Server Certificate**.
 - Step 6** On the Web Server Certificate Wizard welcome window, click **Next**.
 - Step 7** Click **Create a New Certificate**, and click **Next**.
 - Step 8** Click **Prepare the Request Now, But Send It Later**, and click **Next**.
 - Step 9** Enter a name and a bit length for the certificate.

We strongly recommend that you choose a bit length of 512. Larger bit lengths may decrease performance.

- Step 10** Click **Next**.
- Step 11** Enter the organization information, and click **Next**.
- Step 12** For the common name of the site, enter either the Cisco Unity server system name or the fully-qualified domain name.



Caution The name entered must exactly match the host portion of any URL that will access this system by using a secure connection.

- Step 13** Click **Next**.
- Step 14** Enter the geographical information, and click **Next**.
- Step 15** Specify the certificate request file name and location, and click **Next**.
Save the file to a disk or to a directory that the Certification Authority server can access.
- Step 16** Verify the request file information, and click **Next**.
- Step 17** Click **Finish** to close the Web Server Certificate Wizard.
- Step 18** Click **OK** to Close the Default Website Properties dialog box.
- Step 19** Close the Internet Information Services window.

To Submit the Certificate Request

- Step 1** On the CA server, on the Windows Start menu, click **Run**, and then run **certreq**.
- Step 2** Browse to the directory where you saved the certificate request file in [Step 15](#) of the previous procedure, and double-click it.
- Step 3** Click the CA to use, and click **OK**.

By default, when the CA processes the certificate request, it assigns a pending status for added security. This requires a person to verify the authenticity of the request and to manually issue the certificate on the virtual directories that will use it. The following two procedures guide you through the process.

To Issue the Certificate

- Step 1** On the CA server, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, double-click **Certification Authority** to expand it.
- Step 3** Double-click <Certification Authority name> to expand it.
- Step 4** Click **Pending Requests**.
- Step 5** In the right pane, right-click the request, and click **All Tasks > Issue**.
- Step 6** In the left pane, click **Issued Certificates**.

- Step 7** In the right pane, double-click the certificate to open it.
 - Step 8** Click the **Details** tab.
 - Step 9** In the Show list, choose **<All>**, and click **Copy to File**.
 - Step 10** On the Certificate Export Wizard welcome window, click **Next**.
 - Step 11** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
 - Step 12** Specify a file name and a location that the Cisco Unity server can access, and click **Next**.
 - Step 13** Verify the settings, and click **Finish**.
 - Step 14** Click **OK** to close the Certificate Details dialog box.
 - Step 15** Close the Certification Authority window.
-

To Install the Certificate

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
 - Step 2** Double-click **<System-name>** to expand it.
 - Step 3** Right-click **Default Website**, and click **Properties**.
 - Step 4** In the Properties dialog box, click the **Directory Security** tab.
 - Step 5** Under Secure Communications, click **Server Certificate**.
 - Step 6** On the Web Server Certificate Wizard welcome screen, click **Next**.
 - Step 7** Click **Process the Pending Request and Install the Certificate**, and click **Next**.
 - Step 8** Browse to the directory of the certificate (.cer) file, and double-click it.
 - Step 9** Verify the certificate information, and click **Next**.
 - Step 10** Click **Finish** to close the Web Server Certificate Wizard window.
 - Step 11** Click **OK** to close the Default Website Properties dialog box.
 - Step 12** Close the Internet Information Services window.
-

To Enable IIS to Use SSL

- Step 1** On the Cisco Unity server, on the Windows Start menu, click **Programs > Administrative Tools > Internet Services Manager**.
- Step 2** Double-click **<System-name>** to expand it.
- Step 3** Under Default Website, right-click **Web**, and click **Properties**.
- Step 4** In the Properties dialog box, click the **Directory Security** tab.
- Step 5** Under Secure Communications, click **Edit**.
- Step 6** Check the **Require Secure Channel (SSL)** check box.
- Step 7** Click **OK** to close the Secure Communications dialog box.
- Step 8** Click **OK** to close the Default Web Site Properties dialog box.

- Step 9** Under Default Website, right-click **Jakarta**, and click **Properties**.
 - Step 10** In the Properties dialog box, click the **Directory Security** tab.
 - Step 11** Under Secure Communications, click **Edit**.
 - Step 12** Check the **Require Secure Channel (SSL)** check box.
 - Step 13** Click **OK** to close the Secure Communications dialog box.
 - Step 14** Click **OK** to close the Default Web Site Properties dialog box.
 - Step 15** Close the Internet Information Services window.
-

Distributing the Root Certificate to the Trusted Root Store for All Users in the Domain (Optional)

When Cisco Unity is set up to use SSL, the Cisco Unity Administrator, Status Monitor, and Cisco PCA web applications automatically use an SSL connection every time a subscriber points the browser to their respective websites. An SSL connection means that Cisco Unity offers the digital certificate that you issued in the “[Setting Up Cisco Unity to Use SSL](#)” section as proof of its identity each time the subscriber tries to access the Cisco Unity Administrator, Status Monitor, or the Cisco PCA. Until the certificate is added to the trusted root store on the subscriber computer, the browser will display a message to alert the subscriber that the authenticity of the site cannot be verified and, therefore, its content cannot be trusted.

You can distribute the certificate to the trusted root store for all users in the domain by adding it to the Group Policy. Before doing so, discuss it with the network administrator for your organization. If this solution is not acceptable, you can tell subscribers how to add the certificate to the trusted root store on their own computers. (This can be done later when you set up subscribers to use the Cisco PCA, as described in the “[Configuring Subscriber Browsers to Use the Cisco PCA](#)” section on page 7-8 of the “[Setting Up Client Applications](#)” chapter).

Do the following two procedures in the order listed.

To Export the CA Root Certificate

- Step 1** On the CA server, on the Windows Start menu, click **Programs > Administrative Tools > Certification Authority**.
- Step 2** In the left pane of the Certification Authority window, right-click <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 screen, click **Next**.
- Step 7** Accept the default export file format **DER encoded binary X.509 (.CER)**, and click **Next**.
- Step 8** Specify a file name, and a location, and click **Next**. The location must be accessible to the Domain Admin account that will modify the group policy.
- Step 9** Verify the settings, and click **Finish**.

- Step 10** Click **OK** to close the Certificate Details dialog box.
 - Step 11** Click **OK** to close the Properties dialog box for the Root Certification Authority.
 - Step 12** Close the Certification Authority window.
-

To Add the Root Certificate to the Domain Group Policy for Trusted Root Certificate Authorities

- Step 1** Log on to Windows by using an account that is a member of the Domain Admins group.
 - Step 2** On the CA server, on the Windows Start menu, click **Run**, and then run **mmc**.
 - Step 3** On the top menu, click **Console**.
 - Step 4** Click **Add/Remove Snap-in**.
 - Step 5** On the Standalone tab, click **Add**.
 - Step 6** In the Add Standalone Snap-in dialog box, click **Group Policy**, and click **Add**.
 - Step 7** Click **Browse**.
 - Step 8** In the Browse for a Group Policy Object dialog box, click the **Domains/OUs** tab.
 - Step 9** In the Look In list, select the domain to which the Cisco Unity server belongs.
 - Step 10** In the Domains, Ous, and Linked Group Policy Objects list, click **Default Domain Policy**, and click **OK**.
 - Step 11** Click **Finish**.
 - Step 12** Close the Add Standalone Snap-in dialog box.
 - Step 13** Click **OK** to close the Add/Remove Snap-in dialog box.
 - Step 14** In the left pane of the console window, double-click **Default Domain Policy** for the Cisco Unity server domain to expand it.
 - Step 15** Click **Computer Configuration > Windows Settings > Security Settings > Public Key Policies**.
 - Step 16** Right-click **Trusted Root Certification Authorities**, and click **All Tasks > Import**.
 - Step 17** On the Certificate Import Wizard welcome screen, click **Next**.
 - Step 18** Browse to the location of the saved Root Certification Authority certificate, and double-click it.
 - Step 19** Click **Next**.
 - Step 20** Accept the default for the certificate store, and click **Next**.
 - Step 21** Verify the settings, and click **Finish**.
 - Step 22** Save the console settings.
 - Step 23** Close the console window.
-