Secure Sockets Layer (SSL) secures information shared in a web conference by encrypting the data for travel across the network.

Contents

Restrictions

- Self-signed certificates are not supported, starting with Cisco Unified MeetingPlace Release 6.0.
- Cisco Unified MeetingPlace Web Conferencing must be installed before you configure SSL.
- If you are using SSL on an external web server, make sure that the hostname on the SSL certificate resolves to the external web server IP address.
- If you are using SSL on a system with a segmented DNS, make sure that the hostname on the SSL certificate differs from the segmented DNS name. To change either the Home Page hostname or the Web Conferencing hostname, see Configuring the Web Server.
- If users will access your Web Conferencing server through a firewall, make sure that TCP port 443 is open inbound on your firewall for both of the hostnames or IP addresses on your server.
- You can use SSL on any server (internal or DMZ); however, you cannot use or configure WIA (Windows Integrated Authentication) on that server.
- *For Cisco Unified MeetingPlace Release 6.0 Maintenance Release 5 and later:* We do not support SSL certificates that require a key stronger than 1024 bits.

Task List

1. Use the SSL/TLS configuration page to generate certificate signing requests to send to an authorized

Certificate Authority in order to apply for a digital identity certificate. You need two certificates: one for the Home Page hostname, and one for the Web Conferencing hostname. For instructions, see the To Create a New Certificate Signing Request and Obtain a Certificate File.
2. When you receive the certificate files from your certificate provider, apply the certificates to the Cisco Unified MeetingPlace Web Conferencing website. For instructions, see the To Apply the SSL Certificate to the Cisco Unified MeetingPlace Web Conferencing Websites.
3. Depending on your security needs, see (Optional) To Disable Support for Low Encryption Ciphers and SSL v2
4. Enable the Require SSL field on the Web Server administrative page. For instructions, see the To Enable SSL.
5. Test the SSL connection. For instructions, see the To Test the Web Server Over an HTTPS Connection.

To Create a New Certificate Signing Request and Obtain a Certificate File

1. Sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin** .
3. Click **SSL/TLS** . The SSL/TLS page appears.
4. Click the **Edit** icon for the Home Page hostname.
5. In the applicable fields, enter your company name and organization unit/department.
6. In the applicable fields, enter the complete, official names of your city/locality and state/province. Do not use abbreviations.
7. Choose your country/region.
8. Click **Generate Request** . The new certificate signing request (CSR) appears in the text box below. The request is signed with an auto-generated private key. To see the value of the private key, click the **Private Key** link.
9. Copy the contents of the CSR text box to a text file, and send this file to your certificate provider in return for a certificate file.

   Caution! If your certificate provider asks for your server type, specify Apache or Custom, not Microsoft or IIS. If you attempt to install a Microsoft or IIS certificate by using the SSL/TLS configuration pages, when you attempt to reboot the system, Cisco Unified MeetingPlace Web Conferencing does not restart, logs an error about the certificate, and disables SSL so you can restart and fix the problem.
10. Click **Back** .
11. Repeat Step 3 through Step 10 for the Web Conferencing hostname.
12. When you receive the .cer files from your certificate provider, continue with the To Apply the SSL Certificate to the Cisco Unified MeetingPlace Web Conferencing Websites.

To Apply the SSL Certificate to the Cisco Unified MeetingPlace Web Conferencing Websites

1. Sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin** .
3. Click **SSL/TLS** . The SSL/TLS page appears.
4. Click the **Edit** icon for the Home Page hostname.

5. Open the certificate file for the Home Page hostname in a text editor, and copy the text to the clipboard.
6. In the text box at the bottom of the page labeled 'Step 3,' paste the text from the certificate you obtained for this hostname. It should be one block of text beginning with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----.
7. Click **Install Certificate** . The host is now set up with a certificate.
8. Click **Back** .
9. Return to the SSL/TLS page and repeat this process for the Web Conferencing certificate.
10. Continue with the To Enable SSL.

(Optional) To Disable Support for Low Encryption Ciphers and SSL v2

Cisco authorizes Cisco Unified MeetingPlace Web Conferencing customers to disable the support for low encryption ciphers and SSL v2 on their Cisco Unified MeetingPlace Web Conferencing servers based on their security requirements.

You must assume all work related to this security hardening as well as the operational consequences of this security lock-down, including the fact that some end-users might be unable to use the Cisco Unified MeetingPlace Web Conferencing servers because of incompatible browsers/ client SSL implementation, or encryption strength limitations.

To perform this lock-down for the Microsoft IIS web server component used by Cisco Unified MeetingPlace Web Conferencing:

See the following Microsoft Knowledge Base articles:

- How to Control the Ciphers for SSL and TLS on IIS (IIS restart required)
  http://support.microsoft.com/default.aspx?scid=KB;en-us;q216482
- How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (Windows restart required).
  http://support.microsoft.com/default.aspx?scid=kb;EN-US;245030
- How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (Windows restart required)
  http://support.microsoft.com/default.aspx?scid=kb;en-us;187498

To perform this lock-down for the Adobe Connect application web server used by Cisco Unified MeetingPlace Web Conferencing:

See the following Adobe article:

http://livedocs.adobe.com/fms/2/docs/wwhelp/wwhimpl/common/html/wwhelp.htm?context=LiveDocs_Parts&fil
Note: the Server.xml file that contains the SSLCipherSuite tag to be edited can be found in the following folder on the Cisco Unified MeetingPlace Web Conferencing server:
C:\Program Files\Cisco Systems\MPWeb\WebConf\comserv\win32\conf

Warning! any upgrade of the Cisco Unified MeetingPlace Web Conferencing software with a maintenance release will overwrite the changes that you have made in Server.xml. These changes must be re-applied after the upgrade.

To Enable SSL

1. From the SSL/TLS page, click **Toggle SSL** to turn SSL on.
2. Click **Reboot Server** . The server shuts down and restarts.
   Note: If the Web Conferencing server cannot validate the SSL certificates, the server will log an error and toggle SSL to off. In this case, you will need to restart the Web Conferencing service and fix the issue, then repeat the steps in this procedure.

To Test the Web Server Over an HTTPS Connection

1. From the web server, use a web browser to connect to https://hostname.domain.com, the Fully Qualified Domain Name, or FQDN, of the web server.
   If the Cisco Unified MeetingPlace Web Conferencing home page appears, the connection to the Home Page hostname is successful.
   If any security warning dialog boxes appear, configure SSL not to show the dialog boxes. For detailed information, see Microsoft Knowledge Base Articles 813618 and 257873 on the Microsoft website.
2. Sign in to Cisco Unified MeetingPlace Web Conferencing.
3. Click **Immediate Meeting** .
   If the meeting console opens, the connection to the Web Conferencing hostname is successful.

How to Replace an Expired Intermediate Certificate for the Home Page

NOTE: As of April 2006, all SSL certificates issued by VeriSign require the installation of an intermediate Certificate Authority (CA) certificate. The SSL certificates are signed by an intermediate CA using a two-tier hierarchy (also known as trust chain) which enhances the security of SSL certificates.

For more information, go to: http://www.verisign.com/support/advisories/page_040611.html

Download the Updated VeriSign Intermediate CA

1. Go to the VeriSign intermediate CA certicates web page and select the CA certificate for your product. See the note below.
2. Copy and paste the contents into a text (Notepad) file.
3. Save the file as newintermediate.cer.

Note: When downloading the intermediate CA certificate, ensure that you select the appropriate one for your SSL certificate: either Secure Site with EV Certificates (Secure Server) or Secure Site Pro with EV Certificates (Global). If you are not sure which certificate you have purchased, follow these steps:

- Go to VeriSign Search Certificates page.
- Type your Common Name or Order Number.
- Click **Search**.
- Click the certificate name for your certificate.

Create a Certificate Snap-In

1. From the Web server, click **Start > Run**.
2. In the text box, type **mmc**.
3. Click **OK**.
4. For IIS 5.0: From the Microsoft Management Console (MMC) menu bar, select **Console > Add/Remove Snap-in**.
5. For IIS 6.0: From the Microsoft Management Console (MMC) menu bar, select **File > Add/Remove Snap-in**.
6. Click **Add**.
7. From the list of snap-ins, select **Certificates**.
8. Click **Add**.
9. Select **Computer account**.
10. Click **Next**.
11. Select **Local computer** (the computer this console is running on).
12. Click **Finish**.
13. In the snap-in list window, click **Close**.
14. In the Add/Remove Snap-in window, click **OK**.
15. Save these console settings for future use.

Remove the Expired Intermediate CA

1. From the left pane, double-click **Certificate (Local Computer)**.
2. Click **Intermediate Certification Authorities > Certificates**.
3. Locate the certificate issued to www.verisign.com/CPS Incorp.by Ref.LIABILITY LTD. (C)97 VeriSign (expiration date of 1/7/2004).
4. Right-click the certificate.
5. Click **Delete**.
6. From the left pane, click **Trusted Root Certification Authorities > Certificates**.
7. Locate the certificate issued to Class 3 Public Primary Certification Authority (expiration date of 1/7/2004).
8. Right-click the certificate.
9. Click **Delete**.

Install the New Intermediate CA

1. From the left pane, click **Intermediate Certification Authorities**.
2. Right-click **Certificates**.
3. Click **All Tasks > Import**.
4. At the Certificate Import Wizard, click **Next**.
5. Select the Intermediate CA Certificate file.
6. Click **Next**.
7. Select **Place all certificate in the following store: Intermediate Certification Authorities**.
8. Click **Next**.
9. Click **Finish** .

10. Restart the Web Server.

If this does not resolve the issue, then physically reboot the Web Server. The Web Server should now only have one Intermediate CA that expires in 2016.

How to Replace an Expired Intermediate Certificate for Web Conferencing

NOTE: As of April 2006, all SSL certificates issued by VeriSign require the installation of an intermediate Certificate Authority (CA) certificate. The SSL certificates are signed by an intermediate CA using a two-tier hierarchy (also known as trust chain) which enhances the security of SSL certificates.

For more information, go to: http://www.verisign.com/support/advisories/page_040611.html

1. Follow the steps in the Download the Updated VeriSign Intermediate CA procedure. In that procedure, you copied the contents of the intermediate CA certificate into a file called newintermediate.cer.
2. Follow the steps in the To Apply the SSL Certificate to the Cisco Unified MeetingPlace Web Conferencing Websites procedure.
3. When prompted to copy the certificate, copy the text from file called newintermediate.cer.
4. Add the intermediate certificate provided by your certificate authority provider to the SSL certificate PEM files.

NOTE: When pasting these two certificates within the same PEM file, the order of these certificates matters. The signed server certificate has to be pasted first and then the intermediate certificate should be pasted below the signed server certificate. Be careful when pasting these certificates into the file as extra spaces or dashes can cause problems with the certificate file. Once you make the changes, restart Flash Communication services and the Breeze Application service.

How to Backup and Restore the SSL Private Key

This section describes how to export and subsequently reimport the SSL private key into the MPWEB database. We recommend that you make this part of your standard backup procedure. You will need to complete these procedures anytime you need to move the SSL certificate, for example, from an old Web Server machine to a new Web Server machine or when you are rebuilding a machine.

Exporting the Private Key

This procedure describes how to export the private key/certificate pair on the Web Server so that you can manually copy the SSL files in case you need to restore SSL on the Web Server.

1. Open the Internet Services Manager on the Cisco Unified MeetingPlace Web Server by doing the following:

Click **Start > Programs > Administrative Tools > Internet Information Services Manager**.

2. Navigate to Default Web Site.
3. Click the + sign beside Local Server > Web Sites to open the appropriate directory trees.
4. Right-click **Default Web Site**.
5. Choose **Properties**.
   The Default Web Site Properties window appears.
6. Click the Directory Security tab.
7. Click **Server Certificate**.
   The Web Server Certificate wizard appears.
8. Click **Next**.
9. Choose **Export the current certificate to a pfx file**.
10. Click **Next**.
11. Click **Browse** and choose to save the certificate file to your desktop.
12. Click **Next**.
13. Enter a password to encrypt the certificate.
14. Enter the password again to confirm it.
15. Click **Next**.
    The Export Certificate Summary Screen appears and the exported certificate file is now on your desktop.
16. Click **Next**.
17. Click **Finish** to close the Web Server Certificate wizard.
18. Click **OK** or **Cancel** to close the Default Web Site Properties window.
19. Close IIS Manager.

Copying and Saving the Private Key for Future Use

Before You Begin

Complete the Exporting the Private Key section.

1. Open a DOS prompt.
2. Click **Start > Run**.
3. Enter **cmd**.
4. Enter the path to your desktop in the cmd.exe window. For example: **cd Documents and Settings\Administrator\Desktop**
5. Enter the full path to OpenSSL.exe keeping the following in mind:

- After -in, enter the full path to where you placed the file during the Exporting the Private Key section.
- After -out, enter the full path to where you want to send the exported file.
- Example: **\Program Files\Cisco Systems\MPWeb\DataSvc\openssl.exe pkcs12 -in \Documents and Settings\Administrator\Desktop\mycertificate.pfx -out \Documents and Settings\Administrator\Desktop\mycertificate.pem -nodes**
- This converts the PFX format to a PEM format. The mycertificate.pem file will have all the certificates starting with the Private key.

6. Enter the import password when prompted. This is the password you defined in the Web Server Certificate wizard during the export process.

7. Save the PEM file. You will need it whenever you need to reapply the certificate.

Importing the Private Key in to the MPWEB Database

Before You Begin

Complete the Copying and Saving the Private Key for Future Use section.

1. Open SQL Server Enterprise Manager.
2. Click **Start > All Programs > Microsoft SQL Server > Enterprise Manager**.
3. Navigate to the MPWEB database.
4. Click the + sign next to SQL Server Group > LOCAL > Databases > MPWEB to open the appropriate directory trees.
5. Click **Tables** in the MPWEB directory.
   A list of tables opens in the right pane.
6. Right-click Web in the right pane.
7. Choose **Open table > Return all rows**.
   The Web database table appears.
8. Scroll to the right until you see the SSLPrivateKey column.
9. Open the PEM file in Notepad. You saved the PEM file when you completed the Copying and Saving the Private Key for Future Use section.
10. Copy the private key in its entirety. The private key begins with ?Begin RSA Private key? and ends with ?end RSA private key?.
11. Paste the private key into the SSLPrivateKey field.
12. Click the field before the SSLPrivateKey column.
13. Press the Tab key on your keyboard to select all of the data in the SSLPrivateKey field.
14. Right-click and choose **Paste** to paste the value you copied from Notepad.
15. Click somewhere else on the screen to remove your cursor from the SSLPrivateKey field.
16. Close SQL Server Enterprise Manager.
17. (Optional) Enable SSL if it is not already enabled.
18. Reboot the server.