Main page: Cisco Unified MeetingPlace, Release 8.0

Up one level: Configuration

Note: This topic does *not* apply to deployments in which users schedule meetings from the Cisco WebEx site. For information about Cisco WebEx integration deployments, see the *Planning Guide for Cisco Unified MeetingPlace* at http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace%2C_Release_8.0_--_Planning_Your_Deployment.

- How to Configure Restricted Meeting ID Patterns
- How to Configure Secure Sockets Layer for the Web Server
- How to Replace an Expired Intermediate Certificate for the Home Page
- How to Replace an Expired Intermediate Certificate for Web Conferencing
- How to Back Up and Restore the SSL Private Key
- Allowing Guests to Search Through Public Meetings

Contents

How to Configure Restricted Meeting ID Patterns

As a system administrator, you can restrict Cisco Unified MeetingPlace from accepting certain meeting ID patterns that you consider unsecure. For example, you can restrict meeting ID patterns that repeat the same digit three times in a row, such as 111 or 222.

Keep the following points in mind when determining which meeting ID patterns to restrict:

- Restricted meeting ID patterns affect both numerical and vanity meeting IDs. Therefore, if you select to restrict patterns that repeat the same digit three times, Cisco Unified MeetingPlace will disallow both the numerical meeting ID "333" and the vanity meeting ID "deepdive," because "deepdive" translates to 3337383.
- Keep the length of your minimum meeting ID requirement in mind. Repeating the same digit three times when the length of your minimum meeting ID is four digits long can be considered a security risk. However, repeating the same digit three times when the length of your minimum meeting ID is eight digits long may not.

- There is always the chance of a meeting ID hitting the rule pattern and causing a problem. Judicious use of the rule is critical for the reduction of such incidents.

  Specifically, only meeting IDs that schedulers manually enter via the Cisco Unified MeetingPlace web user portal or Microsoft Outlook are immediately checked against the restricted meeting ID patterns that you configure on the Web Server. If a conflict is found, then the scheduler is prompted to enter an unrestricted meeting ID.
  In contrast, the configured restricted meeting ID patterns will cause errors if they conflict with meeting IDs that are entered or generated using one of the following methods:
  - ◊ Scheduler leaves the meeting ID field blank, so the system randomly generates the meeting ID.
  - ◊ User schedules the meeting via the TUI or Cisco Unified MeetingPlace PhoneView.
  - ◊ A reservationless meeting uses the profile number of the meeting owner as the meeting ID.

Note: You cannot schedule a meeting with a supported meeting ID pattern through the phone or other scheduling endpoint, then attempt to modify it or reschedule it through the web. This rescheduling behavior is not supported.

Adding Restricted Meeting ID Patterns

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Restricted Meeting ID Patterns**.
4. For Pattern, enter the restricted meeting ID pattern as a regular expression using the Perl syntax.
   ```
   Example:
   .*(012|123|234|345|456|567|678|789|890|098|987|876|765|654|543|432|321|
   ```
5. Enter a brief description to explain the intent of the pattern in the field provided.
   ```
   Example: Block sequences of 3 increasing or decreasing
   numbers.
   ```
6. Select **Add**.
   The pattern displays in the "View" section of the page.
7. Repeat Step 4 through Step 6 for each additional restricted ID pattern.

Related Topics

- How to Configure Restricted Meeting ID Patterns
- Restricting the Use of Vanity Meeting IDs in the Securing the Cisco Unified MeetingPlace System module

Deleting Restricted Meeting ID Patterns

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.

3. Select **Restricted Meeting ID Patterns**.
4. Scroll down to the "View" section of the screen.
5. Locate the pattern you want to delete.
6. Select **Delete**.

Related Topics

- How to Configure Restricted Meeting ID Patterns
- Restricting the Use of Vanity Meeting IDs in the Securing the Cisco Unified MeetingPlace System module

How to Configure Secure Sockets Layer for the Web Server

Secure Sockets Layer (SSL) secures information by encrypting the data for travel across the network. Complete the following procedures in the order shown to configure SSL.

- Restrictions for Configuring Secure Sockets Layer
- Changing the Web Server Hostname From an IP Address to a Hostname
- Creating a New Certificate Signing Request and Obtaining a Certificate File
- Applying the SSL Certificate
- Enabling SSL
- Testing the Web Server Over an HTTPS Connection
- (Optional) Disabling Support for Low Encryption Ciphers and SSL v2

Restrictions for Configuring Secure Sockets Layer

- 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.
- Self-signed certificates are not supported.
- Make sure that the Hostname [Home Page] field value is a hostname, not an IP address.

  The same restriction applies to the Hostname [Web Conferencing] field, which appears only if you upgraded from Release 7.0 to Release 8.0.

- If users will access your Web 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 Web Server (internal or DMZ); however, you cannot use or configure WIA (Windows Integrated Authentication) on that server.
- We do not support SSL certificates that require a key stronger than 1024 bits.

Related Topics

- How to Configure Secure Sockets Layer for the Web Server
- Windows Integrated Authentication in the Configuring User Authentication for the Cisco Unified MeetingPlace Web Server module

Changing the Web Server Hostname From an IP Address to a Hostname

The Web Server hostname was populated during the Cisco Unified MeetingPlace Web Server software installation. The Hostname [Home Page] was assigned the first IP address in the operating system. If you upgraded from Release 7.0 to Release 8.0, then the Hostname [Web Conferencing] was assigned the second IP address in the operating system.

You should not need to redefine these unless either of the following applies:

- You want users to be able to access the Cisco Unified MeetingPlace Web Server by using the fully qualified domain name (FQDN) of the server or
- You plan to configure SSL for this server. If enabling SSL, you must use hostnames rather than IP addresses.

Before You Begin

This procedure assumes that you have already installed the Cisco Unified MeetingPlace Web Server software.

Restrictions

Do not perform this procedure if the Web Server is not in a Domain Name Server (DNS).

Procedure

1. Open your web browser and enter the URL of your Web Server.
   - For internal Web Servers, the default URL structure is **http://***server*, where *server* is the name of your internal Web Server.
   - For external (DMZ) Web Servers, you can only access the administration pages from the server box itself and only through port 8002. If you try to access the administration pages on the external Web Server by using http://*server*/mpweb/admin/, the system will display a 404 "Page Not Found" error.
     To access the administration pages for the external (DMZ) server, you must be on the web server box and enter the following URL: **http://localhost:8002/mpweb/admin/**
     Note: If SSL is enabled on your system, you must still enter the URL with http and not https. The system automatically signs you in using the preconfigured *admin* profile.
2. Sign in to the web user portal.
3. Select **Admin** if you are not already on the Cisco Unified MeetingPlace Web Administration page.
4. Select **Web Server**.
5. Scroll down to the "View" section of the page.
6. Select the name of the Web Server that you want to configure.
   Information about this Web Server populates the "Edit" section of the page.
7. For Hostname [Home Page], enter the fully qualified domain name (FQDN) of the primary network interface on the Web Server.
   `Example: hostname.domain.com.`
   Note: This hostname must be resolvable by its intended users.

8. For Hostname [Web Conferencing], enter the FQDN of the secondary network interface on the Web Server.
   `Example: hostnamewc.domain.com.`
   Note: This field appears only if you upgraded from Release 7.0 to Release 8.0.
   Note: This hostname must be different from that used for Hostname [Home Page]. It must be resolvable by its intended users. Depending on your hostname choice, the hostnames might not have been automatically registered with the DNS during the OS installation. We recommend that you check the DNS, both the forward and reverse lookup zones, and add entries manually if needed.
9. Select **Submit**.
10. (Optional) If you are working on a Windows system with Internet Explorer, select **Test Server Configuration**.

Related Topics

- Signing In to the Cisco Unified MeetingPlace Web Administration in the Quick Start Configuration for Cisco Unified MeetingPlace Web User Portal for Scheduling and Joining Meetings module
- Field Reference: Web Server Specific Fields in the Web Administration References for Cisco Unified MeetingPlace module
- How to Resolve Test Server Configuration Problems in the Troubleshooting the Cisco Unified MeetingPlace Web Server module
- How to Switch the Order of IP Addresses on the Web Server in the Monitoring and Maintaining the Cisco Unified MeetingPlace Web Server module

What to Do Next

- If you changed the Hostname [Web Conferencing] field, then you must restart the Cisco Unified MeetingPlace Web Master Service for the field change to take effect. See the Stopping, Starting, or Restarting the Cisco Unified MeetingPlace Web Master Service module.
- If you are configuring SSL, proceed to Creating a New Certificate Signing Request and Obtaining a Certificate File.

Creating a New Certificate Signing Request and Obtaining a Certificate File

Use the SSL/TLS configuration page to generate certificate signing requests to send to an authorized Certificate Authority in order to apply for digital identity certificates. You need a certificate for the Home Page hostname. If you upgraded from Release 7.0 to Release 8.0, then you also need a certificate for the Web Conferencing hostname.

Before You Begin

Complete Changing the Web Server Hostname From an IP Address to a Hostname.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.

3. Select **SSL/TLS**.
4. Select the **Edit** icon for the Web Conferencing hostname.
5. Enter your company name and organization unit/department in the applicable fields.
6. Enter the complete, official names of your city/locality and state/province in the applicable fields.
   Note: Do not use abbreviations.
7. Select your country/region.
8. Select **Generate Request**.
   The new certificate signing request (CSR) displays in the text box. The request is signed with an auto-generated private key.
9. Select the **Private Key** link to see the value of the private key.
10. 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, the Cisco Unified MeetingPlace Web Server software will not restart when you attempt to reboot the system. Instead it will log an error about the certificate and disable SSL so that you can restart and fix the problem.
11. Select **Back** to return to the main Administration page.
12. Repeat Step 3 through Step 11 for the Web Conferencing hostname.

What to Do Next

When you receive the .cer file from your certificate provider, proceed to Applying the SSL Certificate.

Applying the SSL Certificate

When you receive the certificate from your certificate provider, apply the certificate to the Cisco Unified MeetingPlace website by completing the following procedure.

Before You Begin

Complete Creating a New Certificate Signing Request and Obtaining a Certificate File.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **SSL/TLS**.
4. Select the **Edit** icon for the Web Conferencing hostname.
5. Open the certificate file for the Web Conferencing hostname in a text editor, and copy the text to the clipboard.
6. In the text box at the bottom of the page, paste the text from the certificate you obtained for this hostname.
   Make sure the text you paste includes the begin and end certificate delimiters.
7. Select **Install Certificate**.
   The host is now set up with a certificate.
8. Select **Back** to return to the main Administration page.

What to Do Next

Proceed to Enabling SSL.

Enabling SSL

Complete this procedure to enable the Require SSL field on the Web Server administration page.

Before You Begin

- Complete Applying the SSL Certificate.
- Make sure that you are still on the SSL/TLS page.

Procedure

1. Select **Toggle SSL** to turn SSL on.
2. Select **Reboot Server**.

   The server shuts down and restarts.
   Note: If the Web 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 Cisco Unified MeetingPlace Web Master Service and fix the issue, then repeat the steps in this procedure.

Related Topics

- Stopping, Starting, or Restarting the Cisco Unified MeetingPlace Web Master Service module

What to do Next

Proceed to Testing the Web Server Over an HTTPS Connection.

Testing the Web Server Over an HTTPS Connection

Before You Begin

Complete Enabling SSL.

Procedure

1. Use a web browser to connect to https://hostname.domain.com, the Fully Qualified Domain Name, of the Web Server.

- If the Cisco Unified MeetingPlace home page displays, 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. If your system was upgraded from Release 7.0 to Release 8.0, then complete these steps to test the connection to the Web Conferencing hostname:
    1. Find a meeting that meets the following conditions:
        - Meeting occurred before the upgrade from Release 7.0 to Release 8.0.
        - The meeting has a recording.
    2. Verify that you can access and play the meeting recording.

Related Topics

- For information about finding meetings and playing recordings, see the *User Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html.

(Optional) Disabling Support for Low Encryption Ciphers and SSL v2

Cisco authorizes Cisco Unified MeetingPlace customers to disable the support for low encryption ciphers and SSL v2 on their Cisco Unified MeetingPlace Web 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 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, 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&file=00000

Note: You can find the Server.xml file that contains the SSLCipherSuite tag to be edited in the following folder on the Cisco Unified MeetingPlace Web Server: C:\Program Files\Cisco Systems\MPWeb\WebConf\comserv\win32\conf

Caution! Any upgrade of the Cisco Unified MeetingPlace Web Server 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.

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:
https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=RELATED_RESC

Topics in this section include:

Downloading the Updated VeriSign Intermediate CA

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).

Procedure

1. If you are not sure which certificate you have purchased, follow these steps:
    1. Go to VeriSign Search Certificates page.
    2. Type your Common Name or Order Number.
    3. Select Search.
    4. Select the certificate name for your certificate.
2. Go to the VeriSign intermediate CA certificates web page and select the CA certificate for your product.
3. Copy and paste the contents into a text (Notepad) file.
4. Save the file as newintermediate.cer.

Creating a Certificate Snap-In

Procedure

1. From the Web server, select **Start > Run**.
2. In the text box, type **mmc**.
3. Select **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. Select **Add**.
7. From the list of snap-ins, select **Certificates**.
8. Select **Add**.
9. Select **Computer account**.
10. Select **Next**.
11. Select **Local computer** (the computer this console is running on).
12. Select **Finish**.
13. In the snap-in list window, select **Close**.
14. In the Add/Remove Snap-in window, select **OK**.
15. Save these console settings for future use.

Removing the Expired Intermediate CA

Procedure

1. From the left pane, double-click **Certificate (Local Computer)**.
2. Select **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. Select **Delete**.
6. From the left pane, select **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. Select **Delete**.

Installing the New Intermediate CA

Procedure

1. From the left pane, select **Intermediate Certification Authorities**.
2. Right-click **Certificates**.
3. Select **All Tasks > Import**.
4. At the Certificate Import Wizard, select **Next**.
5. Select the Intermediate CA Certificate file.

6. Select **Next**.
7. Select **Place all certificate in the following store: Intermediate Certification Authorities**.
8. Select **Next**.
9. Select **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

This topic applies only if you upgraded from Release 7.0 to Release 8.0.

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:
https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR657&actp=RELATED_RESC

1. Follow the steps in the Downloading the Updated VeriSign Intermediate CA.

   In that procedure, you copied the contents of the intermediate CA certificate into a file called newintermediate.cer.
2. Follow the steps in the Applying the SSL Certificate.
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 Back Up 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 any time you need to move the SSL certificate, for example, from an old Web Server computer to a new Web Server computer or when you are rebuilding a computer.

- Exporting the Private Key
- Copying and Saving the Private Key for Future Use
- Importing the Private Key in to the MPWEB Database

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.

Procedure

1. Open the Internet Services Manager on the Cisco Unified MeetingPlace Web Server.
   Select **Start > Programs > Administrative Tools > Internet Information Services Manager**.
2. Navigate to Default Web Site.
   Select the **+** sign beside Local Server > Web Sites to open the appropriate directory trees.
3. Right-click **Default Web Site**.
4. Select **Properties**.
   The Default Web Site Properties window displays.
5. Select the **Directory Security** tab.
6. Select **Server Certificate**.
   The Web Server Certificate wizard displays.
7. Select **Next**.
8. Select **Export the current certificate to a pfx file**.
9. Select **Next**.
10. Select **Browse** and select to save the certificate file to your desktop.
11. Select **Next**.
12. Enter a password to encrypt the certificate.
13. Enter the password again to confirm it.
14. Select **Next**.
    The Export Certificate Summary Screen displays and the exported certificate file is now on your desktop.
15. Select **Next**.
16. Select **Finish** to close the Web Server Certificate wizard.
17. Select **OK** or **Cancel** to close the Default Web Site Properties window.
18. Close IIS Manager.

What to Do Next

Proceed to Copying and Saving the Private Key for Future Use.

Copying and Saving the Private Key for Future Use

We recommend that you complete this procedure as part of your standard backup procedure on the Web Server.

Before You Begin

Complete Exporting the Private Key.

Procedure

1. Open a DOS prompt.
    1. Select **Start > Run**.
    2. Enter **cmd**.
2. Enter the path to your desktop in the cmd.exe window.
   ```
   Example: C:\> cd "Documents and
   Settings\Administrator\Desktop"
   ```
3. Enter the full path to OpenSSL.exe keeping the following in mind:
    - After -in, enter the full path to where you placed the file when you exported the private key.
    - After -out, enter the full path to where you want to send the exported file.
      ```
      Example:C:\Documents and
      Settings\Administrator\Desktop>"\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.
4. Enter the import password when prompted.
   This is the password you defined in the Web Server Certificate wizard during the export process.
5. Save the PEM file. You will need it whenever you need to reapply the certificate.

Related Topics

- Exporting the Private Key

Importing the Private Key in to the MPWEB Database

Before You Begin

- Complete Copying and Saving the Private Key for Future Use.
- Back up the complete database before performing this procedure.

Procedure

1. Open the SQL Query Analyzer.
2. Select **Start > All Programs > Microsoft SQL Server > Query Analyzer**.
3. Log in with your SQL username, ?sa,? and password (which you set during the installation of MPWeb).
4. Type in the following commands:
    - **use mpweb**
    - **update web**
    - **set sslprivatekey='Your private key'**

5. Your private key begins with ?BEGIN RSA PRIVATE KEY? and ends with ?END RSA PRIVATE KEY?. Copy your private key and paste it between the quotes. You can find your Private key in your PEM file that you saved when you copied and saved the private key for future use.
   Note: Make sure you include the quotation marks.
6. Select the green arrow to Execute Query.
7. Determine if your Private Key insertion was successful by entering the following commands in the Query Analyzer window:
   - **use mpweb**
   - **select sslprivatekey from web**
8. Select the green arrow to Execute Query and your private key appears the following window.

Related Topics

- Enabling SSL
- Copying and Saving the Private Key for Future Use

About Home Page and Web Conf SSL certificates

When you import the private key using SQL query Analyzer enable SSL by performing the procedure described in the Enabling SSL section.

Procedure

1. Change the web server hostname from an IP Address to a hostname.
2. Apply the SSL certificate.
3. Enable SSL.

Allowing Guests to Search Through Public Meetings

Guest users have fewer privileges than users who sign in with their profiles. Complete this procedure to allow guests to search through public meetings.

Procedure

1. Sign in to the Cisco Unified MeetingPlace web user portal.
2. Select **Admin**.
3. Select **Web Server**.
4. Scroll down to the "View" section of the page.
5. Select the name of the Web Server that you want to configure.
   Information about this server populates the "Edit" section of the page.
6. Select **Yes** for Allow Public Meetings in Find Meeting List.
7. Select **Yes** for Allow Guest Access to Find Meetings Page.
8. Select **Submit**.

Tip: To allow external users (those outside your firewall) and sites (Cisco Unified MeetingPlace systems outside your network) to access a meeting and the associated meeting materials, make sure that Allow External Web Participants is set to Yes for the meeting. This parameter is set by the meeting scheduler from

the New Meeting scheduling page, and it is only visible if your Cisco Unified MeetingPlace system has an external site-that is, a Web Server located in an Internet-accessible segment of your network, such as in a DMZ zone.

Related Topics

- Field Reference: Web Server Customization Values in the Web Administration References for Cisco Unified MeetingPlace module