Main page: Cisco Unified MeetingPlace, Release 7.0

Up one level: Configuration

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.

Contents

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.

Backing Up the Breeze Certificate

Procedure

1. Open a DOS prompt.
2. Enter the following command: **Copy c:\Program Files\Cisco Systems\MPWeb\WebConf\comserv\win32\conf_defaultRoot_\cert.pem file to** *backup path*.

About Restoring Breeze and Home Page Certificates

See the Applying the SSL Certificate section for more information on restoring Breeze and home page certificates.

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

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.