Main page: Cisco Unified MeetingPlace Express, Release 2.x

About Certificates

To use SSL to provide secure web communications to and from Cisco Unified MeetingPlace Express, you must obtain two certificates from a trusted certificate authority (CA):

- One for the End-User Interface and the Administration Center
- One for web conferencing

Cisco Unified MeetingPlace Express does not support self-signed certificates. If you use self-signed, or unsigned, certificates, parts of the web meeting room will not work correctly.

Whether or not SSL is enabled, e-mail notifications use click-to-attend URLs that begin with "http" instead of "https." When SSL is enabled, the system automatically redirects users to an "https" URL.

Note: If you are using Segmented Meeting Access (SMA), you must also use SSL to provide secure web communications between the primary and secondary servers. In this instance, you must obtain four certificates: two for the primary server and two for the secondary server. To set up the SSL for the secondary server, you use the same procedures as for the primary server, except that you use a different set of pages in the Administration Center.

NOTE: For Release 2.1 only, we now support the use of intermediate SSL certificates.

Using SSL in E-mail/Exchange Integration

NOTE: The following section applies to Release 2.1 only.

To secure e-mail communication, most SMTP and Exchange servers support TLS (which is the new version of SSL protocol). If TLS is enabled on the SMTP server, Cisco Unified MeetingPlace Express, Release 2.1 will always use it (by sending the STARTTLS command).

(Note that this behavior is different from earlier Cisco Unified MeetingPlace Express releases. In those releases, TLS was never used for SMTP connections.)

If TLS is enabled on the Exchange server, configure TLS on the Exchange Server Configuration page by altering ?TLS Enabled? field.

Using Non-Trusted and Self-Signed Certificates

NOTE: The following section applies to Release 2.1 only.

Certificates that are not issued by a recognized CA are considered to be non-trusted. Self-signed certificates are almost always non-trusted. Non-trusted and self-signed certificates are not supported for web conferencing.

However, some customer systems may use non-trusted or self-signed certificates on their SMTP or Exchange servers. In this case, SMTP and Exchange integration breaks.

To resolve this issue, use the 2_X_hotfix_03_CSCsw87431 hotfix which imports certificates to the list of trusted certificates in the Java keystore.

Related Topics:

Troubleshooting SSL Issues