



Preparing Cisco UMG to Support E-SRST and SRSV Functionality

Last updated: December 2, 2010

If you want to configure your Cisco UMG system for E-SRST and SRSV functionality, follow these procedures:

- [Prerequisites, page 51](#)
- [About Security for Cisco UMG, page 52](#)

Prerequisites

Complete the following tasks before you configure your Cisco UMG for E-SRST and SRSV.

Table 1 *Prerequisites for Configuring E-SRST and/or SRSV Functionality for Cisco UMG*

Task	For more information, see
Install Cisco Unified Communications Manager, including security certificates at the central office.	http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html
Install Cisco Unity Connection, including security certificates at the central office.	http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html
Enable SMTP support on the Cisco Unity Connection.	How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection, page 52
Install a Cisco Unified SRST system at the branch office, including security certificates. The supported options are: • Sites using E-SRST require CUCME-as-SRST. • Sites using SRSV only can use either CUCME-as-SRST or original SRST.	For CUCME-as-SRST, also known as SRST Fallback Mode, see: • http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmest.html For original SRST, see: • http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

Table 1 **Prerequisites for Configuring E-SRST and/or SRSV Functionality for Cisco UMG**

Task	For more information, see
For sites deploying SRSV, install Cisco Survivable Remote Site Voicemail-Cisco Unity Express (SRSV-CUE) at the branch office.	http://www.cisco.com/en/US/products/ps10769/tsd_products_support_series_home.html

How to Enable SMTP Support for Cisco UMG on Cisco Unity Connection

You must configure the Cisco Unity Connection system to allow Cisco UMG to upload messages to it. There are two basic configurations to allow Cisco UMG to work with Cisco Unity Connection:

- Add Cisco UMG addresses to the SMTP access list.
- Allow untrusted connections to Cisco Unity Connection SMTP.

The quickest setup is to allow untrusted SMTP connections on Cisco Unity Connection but this configuration is also the most unsecure. Adding devices to the trusted list requires manually entering Cisco UMG addresses into all Cisco Unity Connections systems by using the System Settings > SMTP Configuration > Server page of the Cisco Unity Connection administration application.

For more information about Cisco Unity Connection SMTP configuration, see the following:

- *[Interface Reference Guide for Cisco Unity Connection Administration: System Settings: SMTP Server](#)*
- *[Interface Reference Guide for Cisco Unity Connection Administration: System Settings: Search IP Address Access List](#)*

About Security for Cisco UMG

- [About Security, page 52](#)
- [About Security Certificates, page 53](#)
- [Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager, page 53](#)
- [Installing the Security Certificates, page 54](#)

About Security

Security certificates play an essential role in the protection of voicemail messages as they are transferred from the branch site to the central office across the WAN network. Security certificates are required to provide a secure connection between systems. Security is needed for the following:

- Between Cisco Unity Connection and Cisco Unified Communications Manager
- Between Cisco Unified Communications Manager and the Cisco UMG
- Between Cisco UMG and the Cisco Unified SRSV-CUE device at the branch
- Between Cisco UMG and the Cisco Unified SRST or CUCME-as-SRST device at the branch

About Security Certificates

Use one of these methods to generate and sign security certificates:

- Trust chains. Trust chains use Certificate Authorities (CAs) to simplify large deployments. You install security certificates for the CUCM, Cisco Unity Connection, and Cisco UMG that were all signed by a CA and the connections are all part of a trusted chain.
- Self-signed certificates. You use self-signed certificates for each device. In this case, the Cisco UMG needs the security certificate from each device to which it connects.

There are two kinds of security certificates: distinguished encoding rules (DER) and privacy-enhanced mode (PEM).

Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager

Use this method to retrieve the certificates from the Cisco Unity Connection and Cisco Unified Communications Manager systems. You will later add these certificates to the Cisco UMG system.



Note

Described below is one method, using the Firefox browser, that you can follow to retrieve certificates in the PEM format. There may be other methods to retrieve security certificates.

Procedure

- Step 1** Using Firefox, open a web browser.
- Step 2** Navigate to the Cisco Unity Connection home page. It is not necessary to log in.
- Step 3** Select **Edit > Preferences**.
- Step 4** Click **Advanced**.
- Step 5** Click the **Encryption** tab.
- Step 6** Click **View Certificates**.
- Step 7** Click the **Servers** tab.
- Step 8** Locate the servers from Cisco and click the arrow to expand the list of servers. Find the system name of the Cisco Unity Connection system.
- Step 9** Highlight the row with the Cisco Unity Connection system.
- Step 10** Click **Export...**
- Step 11** Save the certificate file to a convenient location.
- Step 12** Use Notepad to open the certificate file.
- Step 13** Ensure that it has text that include lines with ---- BEGIN CERTIFICATE ----- and ---- END CERTIFICATE -----.
- Step 14** Repeat this procedure on the Cisco Unified Communications Manager system.

Installing the Security Certificates

Cisco UMG needs both the Cisco Unity Connection and Cisco Unified Communications Manager public certificates installed to enable it to communicate securely with Cisco Unity Connection and Cisco Unified Communications Manager over the REST and AXL interfaces respectively.

Before You Begin

Download the security certificates from Cisco Unity Connection and Cisco Unified Communications Manager. See the [“Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager”](#) section on page 53.



Note

The following procedure installs security certificates in the PEM format. Your experience may be slightly different if you are using security certificates in the DER format.

Procedure

-
- Step 1** Enter the following CLI command:
- ```
crypto key import trustcert label LABEL terminal
```
- where *LABEL* is the name of the security certificate.
- The system displays the following:
- ```
Enter certificate...
End with a blank line or "quit" on a line by itself
```
- Step 2** Paste the contents of the security certificate, starting with the line ----- BEGIN CERTIFICATE----- and ending with the line ----- END CERTIFICATE -----.
- The system displays the following:
- ```
Certificate info

Owner: C=US, ST=MA, L=BXB, O=Cisco, OU=None, CN=CCM-7
Issuer: C=US, ST=MA, L=BXB, O=Cisco, OU=None, CN=CCM-7
Valid from: Thu Dec 18 14:34:23 EST 2008 until: Wed Dec 18 14:34:23 EST 2013
Certificate fingerprint (MD5): AD:B2:7F:7A:BB:91:08:0B:5A:59:51:45:BE:F1:CA:42

Do you want to continue to import this certificate, additional validation will be
performed? [y/n]:
```
- Step 3** Enter *y* to import the certificate.
- Step 4** Repeat steps 1 to 3 for the security certificate for Cisco Unified Communications Manager.
- Step 5** At the prompt, enter the following to exit config mode:
- ```
exit
```
- Step 6** At the prompt, enter the following to reload the system:
- ```
reload
```
- The system asks you if you really want to reload.
- Step 7** Enter *y* to confirm that you really want to reload the system.
-

**Related Topics**

Refer to the [Command Reference for Cisco Unified Messaging Gateway Release](#) for information about the CLI commands.

