



About Security for Cisco UMG

Last updated: August 5, 2011

- [About Security, page 133](#)
- [About Security Certificates, page 133](#)
- [Retrieving Security Certificates from Cisco Unity Connection and Cisco Unified Communications Manager, page 134](#)

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 Cisco UMG
- Between Cisco UMG and the Cisco Unified SRSV-CUE device at the branch site
- Between Cisco UMG and the Cisco Unified SRST or CUCME-as-SRST device at the branch site

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 Cisco Unified Communications Manager, 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, Cisco UMG needs the security certificate from each device to which it connects.

The TLS security certificate can be represented in one of two formats: 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.

Procedure

-
- Step 1** Log in to the Cisco Unified OS Administration interface.
 - Step 2** Select **Security > Certificate Management**.
 - Step 3** Click **Find** to show the certificates.
 - Step 4** Click the *.pem or *.der link for the desired certificate.
 - Step 5** Click **Download** to save the certificate to the local file system.
-