Secure Survivable Remote Site Telephony (SRST) Reference

This chapter provides information about SRST references.

Securing SRST

A SRST-enabled gateway provides limited call-processing tasks if the Unified Communications Manager cannot complete the call.

Secure SRST-enabled gateways contain a self-signed certificate. After you perform SRST configuration tasks in Unified Communications Manager Administration, Unified Communications Manager uses a TLS connection to authenticate with the Certificate Provider service in the SRST-enabled gateway. Unified Communications Manager then retrieves the certificate from the SRST-enabled gateway and adds the certificate to the Unified Communications Manager database.

After you reset the dependent devices in Unified Communications Manager Administration, the TFTP server adds the SRST-enabled gateway certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled gateway.

Tip The phone configuration file only contains a certificate from a single issuer. Consequently, the system does not support HSRP.

Securing SRST Tips

Ensure that the following criteria are met to secure the connection between the secure phone and the SRST-enabled gateway:

- The SRST reference contains a self-signed certificate.
- You configured Mixed Mode through the Cisco CTL Client.
- You configured the phone for authentication or encryption.
- You configured the SRST reference in Unified Communications Manager Administration.
- You reset the SRST-enabled gateway and the dependent phones after the SRST configuration.

Note Unified Communications Manager provides the PEM format files that contain phone certificate information to the SRST-enabled gateway.

Note For LSC authentication, download the CAPF root certificate (CAPF.der). This root certificate allows the secure SRST to verify the phone LSC during the TLS handshake.

- When the cluster security mode equals nonsecure, the device security mode remains nonsecure in the phone configuration file, even though Unified Communications Manager Administration may indicate that the device security mode is authenticated or encrypted. Under these circumstances, the phone attempts nonsecure connections with the SRST-enabled gateway and Unified Communications Manager.

Note Cluster security mode configures the security capability for your standalone server or a cluster.

- When the cluster security mode equals nonsecure, the system ignores the security-related configuration; for example, the device security mode, the Is SRST Secure? check box, and so on. The configuration does not get deleted in from the database, but security is not provided.
- The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals Mixed Mode, the device security mode in the phone configuration file is set to authenticated or encrypted, the Is SRST Secure? check box is checked in the **SRST Configuration** window, and a valid SRST-enabled gateway certificate exists in the phone configuration file.
- If you configured secure SRST references in a previous Unified Communications Manager release, the configuration automatically migrates during the upgrade.
- If phones in encrypted or authenticated mode fail over to SRST, and, during the connection with SRST, the cluster security mode switches from Mixed Mode to Nonsecure Mode, these phones will not fall back to Unified Communications Manager automatically. You must power down the SRST router to force these phones to reregister to Unified Communications Manager. After phones fall back to Unified Communications Manager, you can power up SRST, and failover and fallback will be automatic again.

Set Up Secure SRST

The following procedure provides the tasks to perform the SRST configuration process for security.

Procedure

Step 1 Verify that you performed all necessary tasks on the SRST-enabled gateway, so the device supports Unified Communications Manager and security.

For more information, see the *CiscoIOS SRST Version System Administrator Guide* that supports this version of Unified Communications Manager.

Step 2 Verify that you performed all necessary tasks to install and configure the CiscoCTL Client.

Step 3 Verify that a certificate exists in the phone.

For more information, refer to the Cisco Unified IP Phone documentation for your phone model.

Step 4 Verify that you configured the phones for authentication or encryption.

Step 5 Configure the SRST reference for security, which includes enabling the SRST reference in the Device Pool Configuration window.

Step 6 Reset the SRST-enabled gateway and phones.

Related Topics

Apply Security Profiles to Phone
Cisco CTL Client Setup
Set Up Secure SRST References, on page 3

Set Up Secure SRST References

Consider the following information before you add, update, or delete the SRST reference in Cisco Unified Communications Manager AdministrationUnified Communications Manager Administration:

- Adding a Secure SRST Reference—The first time that you configure the SRST reference for security, you must configure all settings that are described in Table 1: Configuration Settings for Secure SRST References, on page 5.
- Updating a Secure SRST Reference—Performing SRST updates in Unified Communications Manager Administration does not automatically update the SRST-enabled gateway certificate. To update the certificate, you must click the **Update Certificate** button; after you click the button, the contents of the certificate display, and you must accept or reject the certificate. If you accept the certificate, Unified Communications Manager replaces the SRST-enabled gateway certificate in the trust folder on the Unified Communications Manager server or on each Unified Communications Manager server in the cluster.
- Deleting a Secure SRST Reference—Deleting a secure SRST reference removes the SRST-enabled gateway certificate from the Unified Communications Manager database and the cnf.xml file in the phone.

  For information on how to delete SRST references, refer to the *Administration Guide for Cisco Unified Communications Manager* .

To configure a secure SRST reference, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **System** > **SRST**.

The **Find and List** window displays.

Step 2 Perform one of the following tasks:

a) To add a new SRST reference, click **Add New** in the **Find** window. (You can also display a profile and then click **Add New**.) The configuration window displays with the default settings for each field.

b) To copy an existing SRST reference, locate the appropriate SRST reference as described in the *Administration Guide for Cisco Unified Communications Manager*, and click the **Copy** icon for that record in the Copy column. (You can also display a profile and then click **Copy**.) The configuration window displays with the configured settings.

c) To update an existing SRST reference, locate the appropriate SRST reference as described in the *Administration Guide for Cisco Unified Communications Manager*.

The configuration window displays with the current settings.

Step 3 Enter the security-related settings as described in Table 1: Configuration Settings for Secure SRST References, on page 5.

For descriptions of additional SRST reference configuration settings, refer to the *Administration Guide for Cisco Unified Communications Manager*.

The **Find and List** window displays.

Step 4 After you check the Is SRST Secure? check box, a dialog box displays a message that you must download the SRST certificate by clicking the Update Certificate button. Click **OK**.

Step 5 Click **Save**.

Step 6 To update the SRST-enabled gateway certificate in the database, click the **Update Certificate** button.

Tip This button displays only after you check the Is SRST Secure? check box and click **Save**.

Step 7 The fingerprint for the certificate displays. To accept the certificate, click **Save**.

Step 8 Click **Close**.

Step 9 In the SRST Reference Configuration window, click **Reset**.

What to do next

Verify that you enabled the SRST reference in the **Device Pool Configuration** window.

Related Topics

Where to Find More Information About Securing SRST

SRST Reference Security Settings

The following table describes the available settings for secure SRST references in Unified Communications Manager Administration.

Table 1: Configuration Settings for Secure SRST References

Setting	Description
Is SRST Secure?	After you verify that the SRST-enabled gateway contains a self-signed certificate, check this check box. After you configure the SRST and reset the gateway and dependent phones, the CiscoCTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The CiscoCTL Client retrieves the certificate from the SRST-enabled gateway and stores the certificate in the Unified Communications Manager database. **Tip** To remove the SRST certificate from the database and phone, uncheck this check box, click **Save**, and reset the dependent phones.
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway. Unified Communications Manager uses this port to retrieve the certificate from the SRST-enabled gateway. The CiscoSRST Certificate Provider default port equals 2445. After you configure this port on the SRST-enabled gateway, enter the port number in this field. **Tip** You may need to configure a different port number if the port is currently used or if you use a firewall and you cannot use the port within the firewall.The port number must exist in the range of 1024 and 49151; otherwise, the following message displays: Port Numbers can only contain digits.
Update Certificate	**Tip** This button displays only after you check the Is SRST Secure? check box and click Save. After you click this button, the CiscoCTL Client replaces the existing SRST-enabled gateway certificate that is stored in the Unified Communications Manager database, if a certificate exists in the database. After you reset the dependent phones, the TFTP server sends the cnf.xml file (with the new SRST-enabled gateway certificate) to the phones.

Related Topics

Securing SRST Tips, on page 2
Where to Find More Information

Delete Security From SRST Reference

To make the SRST reference nonsecure after you configure security, uncheck the Is SRTS Secure? check box in the SRST Configuration window. A message states that you must turn off the credential service on the gateway.

SRST Certificate Deletion From Gateway

If the SRST certificate no longer exists in the SRST-enabled gateway, you must remove the SRST certificate from the Unified Communications Manager database and the phone.

To perform this task, uncheck the **Is SRST Secure?** check box and click **Update** in the SRST Configuration window; then, click **Reset Devices**.