Main page: Cisco Unified Presence, Release 7.x

Contents

- 1 Previous Topic
- 2 Configuring TLS Peer Subjects
  - 2.1 Procedure
  - 2.2 Troubleshooting Tips
  - 2.3 Related Topics
  - 2.4 What To Do Next
- 3 Configuring TLS Contexts
  - 3.1 Before You Begin
  - 3.2 Procedure
  - 3.3 Troubleshooting Tips
  - 3.4 Related Topics

Previous Topic

- Configuration and Maintenance of Cisco Unified Presence

- Configuring TLS Peer Subjects

- Configuring TLS Contexts

Configuring TLS Peer Subjects

Note: A TLS peer subject is automatically created when a self-signed certificate is imported.

Procedure

1. Perform one of the following actions:

If you want to:	Action
Add a TLS peer subject	1. Select **System > Security > TLS Peer Subjects**. 2. Select **Add New**.

Update a TLS peer subject	1. Find the record. See the Finding a Network Component topic for instructions. 2. Edit the record as required.

2. Enter the TLS peer subject configuration settings as described in the table below.

Field	Description
Peer Subject Name	Specifies the subject CN of the certificate that the server presents. Open the certificate, look for the CN and paste it here. Maximum characters: 128
Description	Specifies a description of the peer subject. Maximum characters: 128

3. Select Save.

Troubleshooting Tips

- You must restart the SIP proxy server before any changes that you make to the TLS peer subjects take effect. To restart the proxy server, select Presence **> Routing > Settings**.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information

What To Do Next

Configuring TLS Contexts

Configuring TLS Contexts

Before You Begin

Configure a TLS peer subject on Cisco Unified Presence.

Procedure

1. Perform one of the following actions:

If you want to:	Action
Add a TLS context	1. Select **System > Security > TLS Context Configuration**. 2. Select **Add New**.
Update a TLS context	1. Find the record. See the Finding a Network Component topic for instructions. 2. Edit the record as required.

2. Enter the TLS context configuration settings as described in the table below.

Field	Description
Name	Specifies the unique name of the TLS context.
Description	Specifies a description of this TLS context.
Authorization Policy	Specifies the authorization type for this particular TLS context. From the list box, select either **Server** or **Peer** (default).
Disable Empty TLS Fragments	Specifies whether to enable or disable empty TLS fragments.
TLS Cipher Mapping	Displays the available and selected TLS ciphers. You can add and remove the following ciphers: ◊ TLS_WITH_RSA_AES_128_CBC_SHA ◊ TLS_WITH_RSA_AES_256_CBC_SHA ◊ TLS_WITH_RSA_NULL_SHA ◊ TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS Peer Subject Mapping	Displays the available and selected TLS peer subjects.

3. Move the appropriate TLS cipher to Selected TLS Ciphers

4. Move the appropriate TLS peer subject to Selected TLS Peer Subjects.

5. Select **Save**.

Troubleshooting Tips

You must restart the SIP proxy server before any changes that you make to the TLS context take effect. To restart the proxy server, select Presence **> Routing > Settings**.

Related Topics

- How to Find and Delete Components in Cisco Unified Presence Administration
- Getting More Information