Contents

Previous Topic

- Configuring Cisco Unified Presence Release 7.x for Interdomain Federation

- Common Cisco Adaptive Security Appliance Problems and Recommended Actions
- Common Integration Problems and Recommended Actions

Common Cisco Adaptive Security Appliance Problems and Recommended Actions

- About Certificate Configuration Problems
- Errors When Creating the TLS Proxy Class Maps
- Subscriptions Don't Reach Access Edge
- Problems With Cisco Adaptive Security Appliance After Upgrade

About Certificate Configuration Problems

- Certificate Failure Between Cisco Unified Presence and Cisco Adaptive Security Appliance
- Certificate Failure Between Cisco Adaptive Security Appliance and Microsoft Access Edge
- Certificate Error in SSL Handshake
- Error When Submitting Certificate Signing Request to VeriSign

Certificate Failure Between Cisco Unified Presence and Cisco Adaptive Security Appliance

Problem: The certificate configuration between Cisco Unified Presence and Cisco Adaptive Security Appliance is failing.

Solution: The time and time zones on Cisco Adaptive Security Appliance may not be configured correctly.

- Set the time and time zones on Cisco Adaptive Security Appliance.
- Check that the time and time zones are configured correctly on Cisco Unified Presence and Cisco Unified Communications Manager.

Related Topics

- Prerequisite Configuration Tasks for this Integration
- Getting More Information

Certificate Failure Between Cisco Adaptive Security Appliance and Microsoft Access Edge

Problem: The certificate configuration between Cisco Adaptive Security Appliance and Microsoft Access Edge is failing at certificate enrollment on Cisco Adaptive Security Appliance.

Solution: If you are using SCEP enrollment on Cisco Adaptive Security Appliance, the SCEP add-on may not be installed and configured correctly. Install and configure the SCEP add-on.

Related Topics

- CA Trustpoints
- Getting More Information

Certificate Error in SSL Handshake

Problem: A certificate error displays in the SSL handshake.

Solution: There is no FQDN in the certificate. You need to configure the domain on the Cisco Unified Presence CLI, and regenerate the certificate on Cisco Unified Presence to have FQDN. You need to restart the SIP proxy on Cisco Unified Presence when you regenerate a certificate.

Related Topics

- Configuring the Cisco Unified Presence Domain from the CLI
- Getting More Information

Error When Submitting Certificate Signing Request to VeriSign

Problem: I am using VeriSign for certificate enrollment. When I paste the Certificate Signing Request into the VeriSign website, I get an error (usually a 9406 or 9442 error).

Solution: The subject-name in the Certificate Signing Request is missing information. If you are submitting a renewal certificate signing request (CSR) file to VeriSign, the subject-name in the Certificate Signing Request must contain the following information:

- Country (two letter country code only)
- State (no abbreviations)
- Locality (no abbreviations)
- Organization Name
- Organizational Unit
- Common Name (FQDN)

The format of the subject-name line entry should be:

```
(config-ca-trustpoint)# subject-name cn=<fqdn>,
OU=<organisational_unit>,O=<organisation_name>,C=<country>,St=<state>,L=<locality>
```

Related Topics

- CA Trustpoints
- Getting More Information

SSL Errors When Cisco Unified Presence Domain or Hostname is Changed

Problem: I changed the Cisco Unified Presence domain from the CLI, and I am getting SSL certificate errors between Cisco Unified Presence and Cisco Adaptive Security Appliance.

Solution: If you change the Cisco Unified Presence domain name from the CLI, the Cisco Unified Presence self-signed cert, sipproxy.pem, regenerates. As a result you must reimport the sipproxy.pem certificate into Cisco Adaptive Security Appliance. Specifically you must delete the current sipproxy.pem certificate on Cisco Adaptive Security Appliance, and reimport the (regenerated) sipproxy.pem certificate.

Related Topics

- How to Configure Security Certificate Exchange Between Cisco Unified Presence and Cisco Adaptive Security Appliance
- Getting More Information

Errors When Creating the TLS Proxy Class Maps

Problem: The following errors are displayed when configuring the TLS Proxy class maps:

```
ciscoasa(config)# class-map ent_cup_to_foreign

ciscoasa(config-cmap)# match access-list ent_cup_to_foreign

ERROR: Specified ACL (ent_cup_to_foreign) either does not exist or
its type is not supported by the match command.

ciscoasa(config-cmap)# exit

ciscoasa(config)# class-map ent_foreign_to_cup

ciscoasa(config-cmap)# match access-list ent_foreign_to_cup

ERROR: Specified ACL (ent_foreign_to_cup) either does not exist or
its type is not supported by the match command.

ciscoasa(config-cmap)#
```

Solution: The access list for the foreign domain does not exist. In the example above the access list called **ent_foreign_to_cup** does not exist. Create an extended access list for the foreign domain using the **access list** command.

Related Topics

- Certificate Configuration Problems
- Subscriptions Don't Reach Access Edge
- Problems With Cisco Adaptive Security Appliance After Upgrade
- Getting More Information

Subscriptions Don't Reach Access Edge

Problem: Subscriptions from Microsoft Office Communicator do not reach the Access Edge. OCS reports network function error with Access Edge as the peer. The Access Edge service will not start.

Solution: On Access Edge, the Cisco Unified Presence domain may be configured in both the Allow tab and the IM provider tab. The Cisco Unified Presence domain should only be configured in the IM Provider tab. On Access Edge, remove the Cisco Unified Presence domain entry from the Allow tab. Make sure there is an entry for the Cisco Unified Presence domain on the IM Provider tab.

Related Topics

- Certificate Configuration Problems
- Errors When Creating the TLS Proxy Class Maps
- Problems With Cisco Adaptive Security Appliance After Upgrade
- Getting More Information

Problems With Cisco Adaptive Security Appliance After Upgrade

Problem: The Cisco Adaptive Security Appliance does not boot after a software upgrade.

Solution: You can download a new software image to the Cisco Adaptive Security Appliance using a TFTP server and using the ROM Monitor (ROMMON) on the Cisco Adaptive Security Appliance. ROMMON is command line interface used for image loading and retrieval over TFTP and related diagnostic utilities.

Procedure

1. Attach a console cable (the blue cable that is distributed with the Cisco Adaptive Security Appliance) from the console port to a port on a nearby TFTP server.
2. Open hyperterminal or equivalent.
3. Accept all default values as you are prompted.
4. Reboot the Cisco Adaptive Security Appliance.
5. Hit ESC during bootup to access ROMMON.

6. Enter this sequence of commands to enable Cisco Adaptive Security Appliance to download the image from your TFTP server

```
ip <Cisco Adaptive Security Appliance inside interface>
server <TFTP server>
interface Ethernet 0/1
file <name of new image>
```

Note: The Ethernet interface you specify must equate to the Cisco Adaptive Security Appliance inside interface.

7. Place the software image on the TFTP server in a recommended location (depending on your TFTP software).

8. Enter this command to start the download:

```
tftpdnld
```

Note: You need to define a gateway if the TFTP server is in a different subnet.

Related Topics

- Updating the Access Lists
- TLS Proxy Debugging Commands
- Getting More Information

Common Integration Problems and Recommended Actions

- Unable to get Presence Exchange
- Problems sending and receiving IMs
- Losing Presence and IM Exchange After a Short Period
- Delay in Presence State Changes and IM Delivery Time
- 403 FORBIDDEN Returned Following a Presence Subscription Attempt
- Time Out on NOTIFY Message
- Cisco Unified Presence Certificate Not Accepted
- Problems Starting the Front-end Server on OCS
- Cisco Unified Personal Communicator Not Online after Login
- Unable to Remote Desktop to Access Edge

Unable to get Presence Exchange

Problem: Unable to exchange presence information between Cisco Unified Personal Communicator and Microsoft Office Communicator.

Solution:

OCS/Access Edge:

1. The certificate may have been configured incorrectly on the public interface of Access Edge. If you are using a Microsoft CA, ensure that you are using an OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2. The incorrect value displays on the general tab of the certificate (if it is correct it will not be visible). You can also see the incorrect value on an ethereal trace of the TLS handshake between Cisco Unified Presence and Access Edge.

    Regenerate the certificate for the public interface of the Access Edge with a certificate type of "Other" and OID value of 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2

2. The front end server may not be running on OCS.

    Ensure that the "Office Communications Server Front-End" service is running. You can check this service by selecting **Start > Programs > Administrative Tools > Computer Management**. In Services and Applications, select Services and locate the "Office Communications Server Front-End" service. If running, this service should have a status of "Started".

Cisco Unified Presence:

1. The certificate may have been configured incorrectly on Cisco Unified Presence.

    Generate the correct sipproxy-trust certificate for Cisco Unified Presence.

2. If you are using static routes, a static route may have been configured incorrectly. Also, the SIP Proxy domain may not have been properly set to the domain that the Cisco Unified Presence server resides in. Please note that the SIP Proxy will default to domain that was setup during fresh install.

    If you are using static routes, configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set e.g. if the federated domain is abc.com then the destination address pattern should be set to ".com.abc.*". Static routes are configured in Cisco Unified Presence Administration by selecting **Presence > Routing > Static Routes**.

Cisco Unified Personal Communicator client:

    The DNS settings on the Cisco Unified Personal Communicator client may be configured incorrectly. Ensure that the client machine is pointing to the correct DNS. Logout and login of the Cisco Unified Personal Communicator client.

Related Topics

- How to Configure the Certificate for External Access Edge Interface
- How to Exchange Certificates Using Self-Signed Certificates
- DNS Configuration
- Certificate Configuration Problems
- Getting More Information

Problems sending and receiving IMs

Problem: Problems sending and receiving IM's between a Microsoft Office Communicator user and a Cisco Unified Personal Communicator 7.0 user.

Solution:

DNS Settings:

DNS SRV records may not have been created, or configured incorrectly. To check if the DNS SRV records have been configured correctly, perform an nslookup for type=srv from both Cisco Unified Presence and Access Edge.

On Access Edge:

1. From a command prompt on Access Edge, enter **nslookup**.
2. Enter **set type=srv.**
3. Enter the SRV record for the Cisco Unified Presence domain e.g. **_sipfederationtls._tcp.abc.com** where **abc.com** is the domain name. If the SRV record exists, the FQDN for Cisco Unified Presence/Cisco Adaptive Security Appliance is returned.

On Cisco Unified Presence:

1. Using a remote access account, ssh into the Cisco Unified Presence server.
2. Perform the same steps as per the Access Edge above, except in this case use the OCS domain name.

Microsoft Office Communicator client:

The Microsoft Office Communicator 2007 user may have their presence set to "Do Not Disturb" (DND). If Microsoft Office Communicator 2007 is set to DND then it will not receive IM's from other users. Set the presence of the Microsoft Office Communicator user to another state.

Cisco Unified Presence:

1. If you are using static routes instead of DNS SRV, a static route may have been configured incorrectly. Configure a static route that points to the public interface of the Access Edge. The static route should have a route type set to "domain" and have a reversed destination pattern set e.g. if the federated domain is "abc.com" then the destination address pattern should be set to ".com.abc.*".

Static routes are configured in Cisco Unified Presence Administration by selecting **Presence > Routing > Static Routes**.

2. The Federation IM Controller Module Status may be disabled. In Cisco Unified Presence Administration, select **System > Service Parameters**, and select the SIP Proxy service. At the end of the screen, check that the **Federation IM Control Module Status** parameter is set to On.
3. The Federated Domain may have not have been added, or configured incorrectly. In Cisco Unified Presence Administration, select **Presence > Inter-Domain Federation** and check that the correct federated domain has been added.

Related Topics

- DNS Configuration
- Adding a Federated Domain
- Getting More Information

Losing Presence and IM Exchange After a Short Period

Problem: Can share presence and IMs between Cisco Unified Personal Communicator and Microsoft Office Communicator but after a short period, they start to lose each others presence, and then can no longer exchange IM's.

Solution:

OCS/Access Edge:

1. On Access Edge, both the internal and external edges may have the same FQDN. Also in DNS there may be two "A" record entries for that FQDN, one resolving to the IP address of the external edge and the other to the IP address of the internal edge.

   On Access Edge, change the FQDN of the internal edge, and add an updated record entry in DNS. Remove the DNS entry that was originally resolving to the internal IP of the Access Edge. Also reconfigure the certificate for the internal edge on Access Edge.

2. On OCS, under global settings and front end properties, the FQDN for the access edge may have been entered incorrectly. On OCS, reconfigure the server to reflect the new FQDN of the internal edge.

DNS Settings:

DNS SRV records may not have created, or configured incorrectly. Add the necessary "A" records and SRV records.

Related Topics

- Configuring the Microsoft Components for Federation
- Getting More Information

Delay in Presence State Changes and IM Delivery Time

Problem: There is a delay in the delivery time of IMs and presence state changes between Cisco Unified Personal Communicator and Microsoft Office Communicator.

Solution: On the Cisco Unified Presence server, the **Disable Empty TLS Fragments** option may not be selected for the Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context.

Procedure

1. Select **Cisco Unified Presence Administration > System > Security > TLS Context Configuration**.
2. Click **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**.
3. Check **Disable Empty TLS Fragments.**
4. Click **Save.**

Related Topics

- Getting More Information

403 FORBIDDEN Returned Following a Presence Subscription Attempt

Problem: Cisco Unified Presence attempts to subscribe to the presence of a Microsoft Office Communicator user and receives a 403 FORBIDDEN message from the OCS server.

Solution: On the Access Edge server, the Cisco Unified Presence server may not have been added to the IM service provider list. On the Access Edge server, add an entry for the Cisco Unified Presence server to the IM service provider list. On the DNS server for Access Edge, ensure that there is a _sipfederationtls record for the Cisco Unified Presence domain that points to the public address of the Cisco Unified Presence server

or

On the Access Edge server, the Cisco Unified Presence server may have been added to the Allow list. On the Access Edge server, remove any entry from the Allow list that points to the Cisco Unified Presence server.

Related Topics

- Configuring the Microsoft Components for Federation
- Getting More Information

Time Out on NOTIFY Message

Problem: Cisco Unified Presence times out when sending a NOTIFY message (when federating directly between Cisco Unified Presence and Microsoft OCS using TCP).

Solution: On the Cisco Unified Presence server, the **Use Transport in Record-Route Header** may need to be enabled.

Procedure

1. Select **Cisco Unified Presence Administration > System > Service Parameters**.
2. Select the **Cisco UP SIP Proxy** service.
3. In the SIP Parameters (Clusterwide) section, select **On** for the Use Transport in Record-Route Header parameter**.**
4. Click **Save.**

Related Topics

- Getting More Information

Cisco Unified Presence Certificate Not Accepted

Problem: Access Edge is not accepting the certificate from Cisco Unified Presence.

Solution: The TLS handshake between Cisco Unified Presence/Cisco Adaptive Security Appliance and the Access Edge may be failing.

OCS/Access Edge:

1. Ensure that the IM Provider list on the Access Edge contains the public FQDN of the Cisco Unified Presence server, and it matches the subject CN of the Cisco Unified Presence certificate. If you have opted not to populate the Allow List with the FQDN of Cisco Unified Presence, then you must ensure that the subject CN of the Cisco Unified Presence certificate resolves to the FQDN of the SRV record for the Cisco Unified Presence domain.
2. Ensure that FIPS is enabled on Access Edge (use TLSv1).
3. Ensure that Federation is enabled globally on OCS, and enabled on the front end server.
4. If failing to resolve DNS SRV, ensure that DNS is set up correctly and perform an nslookup for type=srv from Access Edge:
    1. From a command prompt on Access Edge, enter **nslookup**.
    2. Enter **set type=srv.**
    3. Enter the SRV record for the Cisco Unified Presence domain, for example. **_sipfederationtls._tcp.abc.com** where **abc.com** is the domain name. If the SRV record exists, the FQDN for Cisco Unified Presence/Cisco Adaptive Security Appliance is returned.

Cisco Unified Presence/Cisco Adaptive Security Appliance:

Check the ciphers on Cisco Unified Presence and Cisco Adaptive Security Appliance. In Cisco Unified Presence Administration, select **System > Security > TLS Context Configuration > Default Cisco UP SIP Proxy Peer Auth TLS Context**, and ensure that the "TLS_RSA_WITH 3DES_EDE_CBC_SHA" cipher is selected.

Related Topics

- Configuring the Microsoft Components for Federation
- Adding the TLS Peer to the Selected TLS Peer Subjects List on Cisco Unified Presence
- Getting More Information

Problems Starting the Front-end Server on OCS

Problem: The front-end server on OCS will not start.

Solution: On OCS, the FQDN of the private interface of the Access Edge may have been defined in the list of Authorized Hosts. Remove the private interface of the Access Edge from the list of Authorized Hosts on OCS.

During OCS install, two Active Directory user accounts are created called RTCService and RTCComponentService. These accounts are given an administrator-defined password, however, on both of these accounts the "Password never expires" option is not selected by default so the password will expire periodically. To reset the password of the RTCService or RTCComponentService on the OCS server, follow the procedure below.

Procedure

1. Right-click on the user account.
2. Select **Reset Password**.
3. Right-click on the user account.
4. Select **Properties**.
5. Select the **Account** tab.
6. Check **Password never expires**.
7. Click **OK**.

Related Topics

- Getting More Information

Cisco Unified Personal Communicator Not Online after Login

Problem: Cisco Unified Personal Communicator client does not have available online status after login.

Solution: The client computer may be pointing to the incorrect DNS server. Update the correct DNS server on the client PC and then login to Cisco Unified Personal Communicator again.

Related Topics

- Configuring the Microsoft Components for Federation
- Getting More Information

Unable to Remote Desktop to Access Edge

Problem: Unable to successfully remote desktop to the Access Edge Server with FIPS enabled on Windows XP.

Solution: This is a known Microsoft issue. The workaround to resolve the issue involves installing a Remote Desktop Connection application on the Windows XP computer. To install Remote Desktop Connection 6.0, follow the instructions at the following Microsoft URL:

http://support.microsoft.com/kb/811770

Related Topics

- Getting More Information