**Main page:** Cisco Unified Presence, Release 7.x

# Contents


- 1 Previous Topic
- 2 Debugging Information for Cisco Adaptive Security Appliance
  - 2.1 Cisco Adaptive Security Appliance Debugging Commands
    - 2.1.1 Table 1: Cisco Security Appliance Debugging Command
    - 2.1.2 Related Topics
  - 2.2 Capturing the Output on the Internal and External Interfaces
    - 2.2.1 Procedure
    - 2.2.2 Related Topics
  - 2.3 TLS Proxy Debugging Commands
    - 2.3.1 Table 2: TLS Proxy Debugging Commands
    - 2.3.2 Related Topics
- 3 Debugging Access Edge and OCS Server
  - 3.1 Initiating a Debug Session on OCS/Access Edge
    - 3.1.1 Procedure
    - 3.1.2 Related Topics
  - 3.2 Verifying the DNS Configuration on Access Edge
    - 3.2.1 Procedure
    - 3.2.2 Related Topics


**Previous Topic**

- Configuring Cisco Unified Presence Release 7.x for Interdomain Federation
- Debugging Information for Cisco Adaptive Security Appliance
- Debugging Access Edge and OCS Server

# Debugging Information for Cisco Adaptive Security Appliance

- Cisco Adaptive Security Appliance Debugging Commands
- Capturing the Output on the Internal and External Interfaces
- TLS Proxy Debugging Commands

## Cisco Adaptive Security Appliance Debugging Commands

Table 1: Cisco Security Appliance Debugging Command lists the debugging commands for the Cisco Adaptive Security Appliance.

**Table 1: Cisco Security Appliance Debugging Command**

| To | Use the Command | Notes |
|---|---|---|
| Show ICMP packet information for pings to the Cisco Adaptive Security Appliance interfaces | **debug icmp trace** | We strongly recommend that you disable debug messages once you have completed your troubleshooting. To disable ICMP debug messages, use the **no debug icmp** trace command. |
| Show messages relating to the certificate validation between Cisco Unified Presence/Cisco Adaptive Security Appliance or Cisco Adaptive Security Appliance/foreign domain | **debug crypto ca** | You can increase log level on ASA by adding the log level parameter to this command, for example:<br><br>**debug crypto ca 3** |
| | **debug crypto ca messages** | Shows only debug messages for input and output messages |
| | **debug crypto ca transactions** | Shows only debug messages for transactions |
| Show the SIP messages sent through Cisco Adaptive Security Appliance | **debug sip** | |
| Send log messages to a buffer (for later viewing) | **terminal monitor** | |
| Enable system log messages | **logging on** | We strongly recommend that you disable system log messages once you have completed your troubleshooting. To disable system log messages, use the **no logging on** command. |
| Send system log messages to a buffer | **logging buffer debug** | |
| Set system log messages to be sent to Telnet or SSH sessions | **logging monitor debug** | |
| Designate a (syslog) server to receive the system log messages | **logging host *<interface_name>* *<ip_ address>*** | • The *interface_name* argument specifies the Cisco Adaptive Security Appliance interface through which you access the syslog server.<br>• The *ip_address* argument specifies the IP address of the syslog server. |
| Ping the Interfaces | **ping** | Refer to the Troubleshooting section of the *Cisco Security Appliance Command Line Configuration Guide* for details on pinging the Cisco Adaptive Security Appliance interfaces, and also pinging between hosts on different interfaces to ensure that the traffic can pass successfully through the Cisco Adaptive Security Appliance. |

| | | |
|---|---|---|
| | | You can also ping an interface in ASDM by selecting **Tools > Ping**.<br><br>**Note:** You will not be able to ping the public Cisco Unified Presence IP address. However the MAC address of the ASA outside interface should appear in the ARP table (**arp -a**). |
| Trace the route of a packet | **traceroute** | You can also trace the route of a packet in ASDM via **Tools > Traceroute**. |
| Trace the life span of a packet through the Cisco Adaptive Security Appliance | **packet-tracer** | You can also trace the life span of a packet in ASDM via **Tools > Packet Tracer**. |

**Related Topics**

- Getting More Information

## Capturing the Output on the Internal and External Interfaces

**Procedure**

1. Enter config mode:

```
>Enable
>password
>config t
```

2. Define an access-list to specify the traffic to be captured, for example:

```
access-list cap extended permit ip 10.53.0.0 255.255.0.0 10.53.0.0
255.255.0.0
```

3. It is recommended that you clear the capture content before starting the tests. Use the command "clear capture in" to clear the internal interface capture, and the command "clear capture out" to clear the external interface capture.

4. Enter this command to capture the packets on the internal interface:

```
cap in interface inside access-list cap
```

5. Enter this command to capture the packets on the external interface:

```
cap out interface outside access-list cap
```

6. Enter this command to capture TLS specific packets:

```
capture <capture_name> type tls-proxy interface <interface_name>
```

7. Enter this command to retrieve the packet capture:

```
copy /pcap capture:in tftp://xx.xx.xx.xx

copy /pcap capture:out tftp://xx.xx.xx.xx
```

8. Enter this command to copy the output to disk and retrieve using ASDM (**Actions > File Management > File Transfer**):

```
copy /pcap capture:in disk0:in_1
```

**Related Topics**

- Getting More Information

## TLS Proxy Debugging Commands

Table 2: TLS Proxy Debugging Commands lists the debugging commands for the TLS Proxy.

**Table 2: TLS Proxy Debugging Commands**

| To | Use the Command(s) |
|---|---|
| Enable TLS proxy-related debug and syslog output | `debug inspect tls-proxy events`<br><br>`debug inspect tls-proxy errors`<br><br>`debug inspect tls-proxy all` |
| Show a TLS proxy session output | `show log` |
| Check the active TLS proxy sessions | `show tls-proxy` |
| View the detail of the current TLS proxy sessions<br><br>(Use when Cisco Adaptive Security Appliance successfully establishes connections with Cisco Unified Presence and the foreign domain) | `show tls-proxy session detail` |

**Related Topics**

- Getting More Information

# Debugging Access Edge and OCS Server

- Initiating a Debug Session on OCS/Access Edge
- Verifying the DNS Configuration on Access Edge

## Initiating a Debug Session on OCS/Access Edge

**Procedure**

1. Select **Start > Administrative Tools > Computer Management** on the external Access Edge server.
2. Right-click **Microsoft Office Communications Server 2007** in the left pane.
3. Select **Logging Tool > New Debug Session**.
4. Select **SIP Stack** in the Logging Options.
5. Select **All** for the Level value.
6. Select **Start Logging**.
7. Select **Stop Logging** when complete.
8. Select **Analyze Log Files**.

**Related Topics**

- Getting More Information

## Verifying the DNS Configuration on Access Edge

**Procedure**

1. On the external Access Edge server, select **Start > Administrative Tools > Computer Management**.
2. Right-click on **Microsoft Office Communications Server 2007**in the left pane.
3. Select the **Block** tab.
4. Check that the domain not blocked.
5. Ensure that the following options are selected in the **Access Methods** pane:
    - **Federate with other domains**
    - **Allow discovery of federation partners**
6. Check the Access Edge is publishing DNS SRV records.

**Related Topics**

- Getting More Information