Troubleshooting

This appendix provides troubleshooting information. It contains information about:

- Contacting Cisco TAC
- Checking the Version Number of Cisco Configuration Engine
- Cannot Log in to the System
- System Cannot Connect to the Network
- Cannot Connect to the System Using a Web Browser
- Problems Connecting to the System with Secure Shell
- Cannot Connect to the System Using Telnet
- Backup and Restore Not Working Properly
- Cannot Back Up Jobs
- Using the cns-send and cns-listen Commands

Note For additional troubleshooting information, see the *Troubleshooting Guide for Cisco Configuration Engine*.

Contacting Cisco TAC

In some of the sections, you might be advised to contact the Cisco Technical Assistance Center (TAC) for assistance. You can obtain TAC assistance online at http://www.cisco.com/tac.

Checking the Version Number of Cisco Configuration Engine

To check the version number of the Cisco Configuration Engine software, do one of the following:

- Start the Cisco Configuration Engine application, and look for the version number in the displayed login screen.
- Use the **version** command. This command is located in the *cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/bin* directory.

Cannot Log in to the System

Problem You cannot log in to the system.

Possible Cause This problem could occur for one of the following reasons:

– You did not run the Setup program to create the initial system configuration.

– You lost all of the user account passwords.

Solution To resolve this problem, follow these steps:

Step 1 If you did not run the Setup program, run the Setup program as described in the *Cisco Configuration Engine Solaris Installation & Configuration Guide, 2.0.*

Step 2 If you do not know the passwords for the system user accounts, reconfigure the system to create a new user account.

Step 3 If you still cannot log in to the system, contact the Cisco Technical Assistance Center (TAC) for assistance.

System Cannot Connect to the Network

Problem The system cannot connect to the network.

Possible Cause This problem could occur for the following reasons:

– The network cable is not connected to an Ethernet port.

– The Ethernet interface is disabled or misconfigured.

– The system is configured correctly, but the network is down or misconfigured.

– The system is not configured correctly.

Solution To resolve this problem, follow these steps:

Step 1 Verify that the network cable is connected to an Ethernet port and that the Link light is on.

• If the network cable is not connected, connect it.

• If the network cable is connected but the Link light is not on, check these probable causes:

– The network cable is faulty.

– The network cable is the wrong type (for example, a crossover type is used, instead of the required straight-through type).

– The port on the default gateway to which the system connects is down.

Step 2 If you still cannot connect to the network, use the **ping** command to perform the following tests:

a. Try to connect to a well-known host on the network. A DNS server is a good target host.

If the **ping** command can reach the well-known host, the system is connected to the network. If it cannot connect to the host, the problem is with the network configuration or the host. Contact your network administrator for assistance.

b. If the **ping** command cannot reach the well-known host, try to reach another host on the same subnet as the system.

If the **ping** command can reach a host on the same subnet, but cannot reach a host on a different subnet, the default gateway is probably down or misconfigured.

Step 3 If the **ping** command cannot reach any hosts, use the **ifconfig** command to determine whether the Ethernet interface is disabled or misconfigured.

If the Ethernet interface is disabled, enable it. If it is misconfigured, configure it correctly.

Step 4 If the interface is enabled and correctly configured but you still cannot connect to the network, ensure that all network setting are configured correctly. Run the Setup program again by entering the **setup** command in the shell prompt.

> ✎
>
> **Note** You cannot run the Setup program a second time by logging in as **setup**. For security reasons, the account is disabled after it is used once successfully.

Step 5 Contact your network administrator to verify that there are no conditions on the network that prevent the system from connecting to the network.

Step 6 If no conditions are preventing the system from connecting to the network, contact the Cisco TAC for assistance.

Cannot Connect to the System Using a Web Browser

Problem You cannot connect to the system by entering its IP address in a web browser.

> **Possible Cause** This problem could occur for the following reasons:
>
> – The system cannot connect to the network.
>
> – Encryption is enabled (plain text is disabled).
>
> – The HTTP service is not running.

Solution To resolve this problem, follow these steps:

Step 1 Make sure that the system can connect to the network.

If it cannot connect to the network, see the "System Cannot Connect to the Network" section on page A-2 for possible resolution.

Step 2 Try to connect to the system by using a web browser.

If encryption is enabled:

- Use **https://**… to connect.
- Verify that the certificate is correct.

Step 3 If you still cannot connect, stop and start the web server by entering the following commands:

```
/etc/rc.d/init.d/httpd stop
/etc/rc.d/init.d/httpd start
```

If the LDAP directory contains thousands of devices, restart and wait 20 minutes.

Step 4   Repeat Step 2.

Step 5   If you cannot connect, restart the system.

If the LDAP directory contains thousands of devices, restart and wait 20 minutes.

Step 6   If you still cannot connect to the system, contact the Cisco TAC for assistance.

Problems Connecting to the System with Secure Shell

Problem   When connecting to the system using Secure Shell (SSH), you experience one of these problems:

- You cannot connect to the system.
- The system is extremely slow, even though it is connected to the network.
- The system cannot correctly process requests from management applications.

    Possible Cause   The system cannot obtain DNS services from the network.

Solution   To resolve this problem, follow these steps. Connect to the console if you cannot connect by using SSH.

Step 1   Do one of the following:

- Set up the name servers properly by editing the */etc/resolv.conf* file.
- Re-execute **Setup**.

Step 2   Verify that the system can obtain Domain Name System (DNS) services from the network by entering the following command:

```
# host <dns-name>
```

where *<dns-name>* is the DNS name of a host on the network that is registered in DNS. When you enter this command, it responds with the IP address of the host.

If the system cannot resolve DNS names to IP addresses, the DNS server is not working properly.

Step 3   Resolve the network DNS problem.

Step 4   If the system can resolve DNS names to IP addresses but you still cannot connect to the system using SSH, contact the Cisco TAC for assistance.

Cannot Connect to the System Using Telnet

Problem   You cannot connect to the system by using Telnet even though the system is connected to the network.

    Possible Cause   This problem could occur if the Telnet service is disabled on the system.

Solution   To resolve this problem, use SSH to connect to the system.

Backup and Restore Not Working Properly

Problem Backup and restore is not working properly.

Possible Cause This problem could occur for the following reasons:

- The time base for the host system is not set to the UTC time zone.
- The time has changed.
- The cron job has not started.

Solution To resolve this problem, follow these steps:

Step 1 Connect to the console if you cannot connect using SSH.

Step 2 Log in to the host system as root.

Step 3 To determine whether the time is correct, enter the following command:

date

Step 4 To determine the state of the cron job, enter the following command:

/etc/rc.d/init.d/crond restart

Example:

```
# /etc/rc.d/init.d/crond restart
Stopping cron daemon:                                    [  OK  ]
Starting cron daemon:                                    [  OK  ]
#
```

Cannot Back Up Jobs

Problem Cannot back up jobs.

Possible Cause The **crontab** command is used to schedule backup jobs. This command requires space in the */var* partition to execute. If the */var* partition is full, the **crontab** command fails to execute, which causes backup job failure.

Solution To resolve this problem, clean up the */var* partition on the system (move some files to *the /home/* directory). Then resubmit the backup job from the Cisco Configuration Engine user interface.

Using the cns-send and cns-listen Commands

Use the **cns-send** and **cns-listen** commands to send and receive test messages to the event gateway in the Cisco Configuration Engine. These commands are located in the */opt/CSCOcnsie/tools* directory.

cns-send

The syntax for the cns-send command is:

cns-send -version

or

cns-send [-service *<service>*] **[-network** *<network>*] **[-daemon** *<daemon>*] **[-file** *<filename>*]
<subject> **[***<message>***]**

Syntax Description		
	-version	Outputs the version of cns-send.
	-service *<service>*	(Optional) The port number (default: 7500).
	-network *<network>*	(Optional) Network interface (in local machine) where messages are sent.
	-daemon *<daemon>*	(Optional) Internal port of application to the rvd daemon (default: 7500).
	-file *<filename>*	(Optional) Filename containing the XML-message. The filename can be sent instead of individual subject/messages.
	<subject>	Subject name of the message.
	<message>	(Optional) Message in the message field.

To use the cns-send command, follow these steps:

Step 1 Log in to the host system as root.

Step 2 Change directories to **/opt/CSCOcnsie/tools**.

Step 3 Type **./cns-send -file** *<filename>* *<subject>*

✎
Note The cns-send command sends messages in the opaque data format.

cns-listen

The syntax for the cns-listen command is:

cns-listen -version

or

cns-listen [-service *<service>*] **[-network** *<network>*] **[-daemon** *<daemon>*] *<subject_list>*

Syntax Description	**-version**	Outputs the version of cns-listen.
	-service *<service>*	(Optional) The port number (default: 7500).
	-network *<network>*	(Optional) Network interface (in local machine) where messages are received.
	-daemon *<daemon>*	(Optional) Internal port of application to the rvd daemon (default: 7500).
	<subject_list>	Subjects listen to.

To use the cns-listen command, follow these steps:

Step 1   Log in to the host system as root.

Step 2   Change directories to **/opt/CSCOcnsie/tools**.

Step 3   Type **./cns-listen** *<subject_list>*.

Usage Guidelines	Use the greater than symbol (>) for a wildcard.

Examples	**./cns-listen "cisco.cns.config.load"**
	./cns-listen "cisco.cns.>"