

Troubleshooting

This appendix provides troubleshooting information. It contains information about:

- Contacting Cisco TAC
- Cannot Log In to the System
- System Cannot Connect to the Network
- Cannot Connect to the System Using a Web Browser
- System Cannot Start from the Disk
- Cannot Connect to System with Telnet or Telnet Interaction is Slow
- Backup and Restore not Working Properly
- How to Use the showversion Command
- How to Use the cns-send and cns-listen Commands

Contacting Cisco TAC

In some of the following 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.

For more information, refer to the "Obtaining Technical Assistance" section on page xiii.

Cannot Log In to the System

Problem: You cannot log in to the system.

Probable causes:

- You did not run the setup program to create an initial system configuration.
- You lost all of the user account passwords.

Resolution:

Step 1 Did you run the setup program after starting the system for the first time?

If no, run the setup program as described in the "Running the Setup Program" section on page 2-1. If yes, continue.

- Step 2 Do you know the password for any system user accounts?
 If no, reconfigure the system to create a new user account. Refer to the "How to Manage User Accounts" section on page 3-6 for more information.
 If yes, continue.
- Step 3 If you are certain you entered a valid username and password, contact the TAC for assistance.

System Cannot Connect to the Network

Problem: The system cannot connect to the network.

Probable causes:

- The network cable is not connected to the Ethernet 0 port.
- The Ethernet 0 interface is disabled or misconfigured.
- The system is configured correctly, but the network is down or misconfigured.
- The system is not configured correctly.

Resolution:

Step 1 Verify that the network cable is connected to the Ethernet 0 port and 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, these are the probable causes:
 - The network cable is faulty.
 - The network cable is the wrong type (for example, a cross-over type, rather than the required straight-through type).
 - The port on the default gateway to which the system connects is down.

If the network cable is connected and the Link light is on but the system cannot connect to the network, continue.

- **Step 2** 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 another host, the system is connected to the network. If it cannot connect to a particular host, the problem is with the network configuration or that host. Contact your network administrator for assistance.

If the ping command cannot reach another host, continue.

b. Attempt 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.

If the ping command cannot reach any hosts, continue.

Step 3 Use the show interfaces command to determine if the Ethernet 0 interface is disabled or misconfigured.

If the Ethernet 0 interface is disabled, enable it. If it is misconfigured, configure it correctly. For more information, refer to "Running the Setup Program" section on page 2-1.

If the interface is enabled and correctly configured, continue.

Step 4 To ensure all network setting are configured correctly, run the **Setup** program again by entering the **setup** command in the shell prompt.



Note You cannot run **Setup** a second time by logging in as **setup** because that account is disabled for security reasons 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.

If conditions prevent the system from connecting to the network, have your network administrator correct them.

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

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.

Probable causes:

- The system cannot connect to the network.
- Encryption is enabled (plaintext disabled).
- The HTTP service is not running.

Resolution:

- **Step 1** Make sure that the system can connect to the network by following the procedure in the "System Cannot Connect to the Network" section on page A-2.
- **Step 2** When you are sure that the system is connected to the network, attempt to connect the system using a web browser.

If encryption is enabled:

- Use https:\\... to connect.
- Ensure the certificate is correct.

If you still cannot connect, continue

Step 3 To stop and start the web server only, enter 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 Attempt to connect the system using a web browser.

If you cannot connect, continue.

Step 5 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 using a web browser, contact the Cisco TAC for assistance.

System Cannot Start from the Disk

Problem: The system cannot start from the disk during a restart.

Probable causes:

- The disk has a physical error.
- The disk image is corrupted.

Resolution:

- **Step 1** If the system does not start automatically from the maintenance image and the start process fails, power the system off and then on.
- **Step 2** Contact the Cisco TAC if the system still cannot start from the disk.



If you require a replacement system, refer to the "Installing a Replacement CNS 2100 Series System" section on page 2-25 for information about installing a replacement system.

Cannot Connect to System with Telnet or Telnet Interaction is Slow

Problem: You cannot connect to the system using Telnet or Telnet interaction with the system is extremely slow, even though the system is connected to the network.

Probable cause: The system cannot get DNS services from the network. The system will not function correctly without DNS. Telnet problems are the most visible symptom, but the system will have more serious problems. In most cases, it will not correctly process requests from management applications that use it.

Resolution: Perform the following steps. Connect to the console if you cannot connect using Telnet.

Step 1 To set up the name servers properly, edit the */etc/resolv.conf* file.

Or, you can re-execute **Setup** (see "How to Re-execute Setup" section on page 2-2).

Step 2 Verify that the system can get 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. The command returns the IP address of the host.

Step 3 If the system cannot resolve DNS names to IP addresses, the DNS server it is using is not working properly.

Resolve the network DNS problem, then continue.

Step 4 If the system can resolve DNS names to IP addresses but you still cannot connect to the system using Telnet or Telnet interaction with the system is extremely slow, contact the Cisco TAC.

Backup and Restore not Working Properly

Problem: Your backup and restore is not working properly.

Probable causes:

- The time base for the CNS 2100 Series system is not set to the UTC time zone.
- The time has changed.
- The cron job is not started.

Resolution: Perform the following steps:

- Step 1 Connect to the console if you cannot connect using Telnet.
- **Step 2** Log into the CNS 2100 Series system as root.

Example:

```
Kernel 2.2.16-11bipsec.uid32 on an i586
login: admin
Password:
Copyright (c) 2000 Cisco Systems, Inc.
Appliance 1.0 Wed Feb 21 22:20:29 UTC 2001
Build Version (152) Wed Nov 15 12:00:13 PST 2000
bash$ su
Password:
```

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

date

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

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

Example:

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

[OK]

OK]

Γ

How to Use the showversion Command

Use the **showversion** command to list all the current RPMs (package managers) loaded on your CNS 2100 Series system. This command is located in the */opt/CSCOcnsie/bin* directory.

Example1:

Using command: showversion

```
[root@ie2100-techdoc /root] # showversion
Cisco Intelligence Engine 2110
Cisco Configuration Registrar (tm) Software, Version 1.3(0.1) CRYPTO [pvgarde-re
naming]
Copyright (c) 2001, 2002 by cisco Systems, Inc.
Compiled Mon 01-Jul-2002 14:55 by pvgarde
Internal directory mode.
apache
 Version: 1.3.19
 Release: 5
IBMJava2-SDK
 Version: 1.3
 Release: 10.0
ACE
 Version: 5.2
 Release: 0
DCL
 Version: 2.4
 Release: 1
Tibco
 Version: 6.48
 Release: 0
tomcat
  Version: 3.2.3
 Release: 0
CSCOPer1500503
  Version: 1
  Release: 0
CSCOcnscommon
  Version: 1.0
  Release: 1
zCSCOcnssetup
  Version: 1.2
  Release: 2
CSCOImgwConfig
  Version: 1.2
  Release: 2
CSCOcnsnsm
 Version: 1.2
```

```
Release: 1
```

```
CSCOImgwDeviceServer
  Version: 1.2
  Release: 2
CSCOdat
  Version: 1.0
 Release: 1
CSCOcda
  Version: 0.0
  Release: 1
CSCOcnscfgs
  Version: 1.3
  Release: 0
CSCOTools
  Version: 1.0
  Release: 0
CSCOcnses
  Version: 1.5
  Release: 1
CSCOimgw
  Version: 1.2
  Release: 2
```

Example2:

Using command: showversion -m CSCOcnses

```
[root@ie2100-techdoc /root]# showversion -m CSCOcnses
Cisco Intelligence Engine 2110
Cisco Configuration Registrar (tm) Software, Version 1.3(0.1) CRYPTO [pvgarde-re
naming ]
Copyright (c) 2001, 2002 by cisco Systems, Inc.
Compiled Mon 01-Jul-2002 14:55 by pvgarde
```

Internal directory mode.

```
Name
          : CSCOcnses
                                        Relocations: (not relocateable)
Version
          : 1.5
                                             Vendor: Cisco Systems, Inc.
Release
           : 1
                                         Build Date: Mon Jul 1 14:25:50 2002
Install date: Tue Jul 2 07:06:08 2002
                                         Build Host: rm-build7.cisco.com
Group : Event Services
                                         Source RPM: CSCOcnses-1.5-1.src.rpm
Size
           : 537126
                                           License: Copyright (c) 1999, 2000
, 2001, 2002 by Cisco Systems, Inc. All Rights Reserved.
Summary
          : CNS Event Services
Description :
CNS Event Services
```

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

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

- **Step 1** Log into the CNS 2100 Series system as root.
- Step 2 Change directories to /opt/CSCOcnsie/tools.
- Step 3 Type ./cns-send -file <filename> <subject>



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></service>	(Optional) The port number (default: 7500).	
	<pre>-network <network></network></pre>	(Optional) Network interface (in local machine) where messages are received.	
	-daemon <daemon></daemon>	(Optional) Internal port of application to the rvd daemon (default: 7500).	
	<subject_list></subject_list>	Subjects listen to.	
	To use the cns-listen command, follow these steps:		
Step 1	Log into the CNS 2100 Series system as root.		
Step 2	Change directories to /opt/CSCOcnsie/tools.		
Step 3	Type ./cns-listen <subject_list></subject_list>		
Usage Guidelines	Use the greater than syr	nbol (>) for a wildcard.	
Examples	./cns-listen "cisco.cns.config.load"		
	./cns-listen "cisco.cns.>	, "	

How to Re-activate IBM Director Agent After Setup

In this release, one of the IBM Director agents is disabled at the end of **Setup**. This happens to release unused CPU cycles.

To re-activate this agent follow these steps:

- **Step 1** Login as root.
- **Step 2** Type the following command string:

cp /etc/TWGagent/TWGagent.orig /etc/TWGagent/TWGagent /opt/CSCOcnsie.bin/TWGagent start



This procedure must be run after each **Setup**.