



Troubleshooting Guide for Cisco Configuration Engine 3.5.3

Revised: May 2, 2011, OL-17767-03

This document contains troubleshooting information for the Cisco Configuration Engine (Cisco CE). It contains the following sections:

- [Checking the Version Number of Cisco Configuration Engine, page 1](#)
- [Troubleshooting Logging and Connection Issues, page 2](#)
- [Troubleshooting Installation Checks, page 5](#)
- [Troubleshooting the OpenLDAP and BDB, page 8](#)
- [Troubleshooting the Cisco CE Services, page 9](#)
- [Troubleshooting the Web Services, page 10](#)
- [Troubleshooting the Initial Configuration, page 11](#)
- [Troubleshooting a Configuration Update, page 13](#)
- [Troubleshooting an Image Update, page 19](#)
- [Troubleshooting IMGW, page 21](#)
- [Troubleshooting the Router, page 22](#)
- [General Troubleshooting, page 22](#)



Note

This is not an administration manual. For comprehensive information about administering the Cisco CE, see the *Cisco Configuration Engine Administration Guide*.

Checking the Version Number of Cisco Configuration Engine

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

- Start the Cisco CE 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.

Troubleshooting Logging and Connection Issues

To troubleshoot logging and connection issues, see the following sections:

- [System Login Problem, page 2](#)
- [System Cannot Connect to the Network, page 3](#)
- [Cannot Connect to the System Using a Web Browser, page 4](#)
- [Problems Connecting to the System with Secure Shell, page 4](#)
- [Cannot Connect to the System Using Telnet, page 5](#)

System Login Problem

Problem You cannot log in to the system.

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

- LDAP is corrupted.
- 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 set up program, run the set up program as described in the *Cisco Configuration Engine Solaris Installation and Configuration Guide 3.5.3*.
- 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** For corrupted LDAP issue, if you receive the following error messages:

Server encountered the following error:

```
javax.naming.CommunicationException: 127.0.0.1:389 [Root exception is
java.net.ConnectException: Connection refused]
    at com.sun.jndi.ldap.Connection.<init>(Connection.java:207)
    at com.sun.jndi.ldap.LdapClient.<init>(LdapClient.java:118)
    at com.sun.jndi.ldap.LdapClient.getInstance(LdapClient.java:1580)
    at com.sun.jndi.ldap.LdapCtx.connect(LdapCtx.java:2616)
    at com.sun.jndi.ldap.LdapCtx.<init>(LdapCtx.java:287)
    at com.sun.jndi.ldap.LdapCtxFactory.getUsingURL(LdapCtxFactory.java:175)
```

Restart the database by providing the following commands:

```
$CISCO_CE_HOME/bin/ce_shutdown -all
export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$CISCO_CE_INSTALL_ROOT/bdb/lib:$CISCO_CE_INSTALL_ROOT/unixodbc/lib
$CISCO_CE_INSTALL_ROOT/bdb/bin/db_recover -h
$CISCO_CE_INSTALL_ROOT/openldap/var/openldap-data
$CISCO_CE_HOME/bin/ce_startup -all
```

- Step 4** 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 can 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 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 for 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 Domain Name System (DNS) server is a good target host.
 If the **ping** command can reach the well-known host and 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 the network settings are configured correctly. Run the set up program again by entering the **setup** command in the shell prompt.
-  **Note** You cannot run the set up program 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 prevents 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 can occur for the following reasons:

- System cannot connect to the network.
- Encryption is enabled (plain text is disabled).
- 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 3 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:
`$CISCO_CE_HOME/bin/ce_shutdown`
`$CISCO_CE_HOME/bin/ce_startup`
If the LDAP directory contains thousands of devices, restart and wait for 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 for 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.
- System is extremely slow, even though it is connected to the network.
- 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 the **Setup**.
- Step 2** Verify that the system can obtain 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 the DNS names to the IP addresses, the DNS server is not working properly.
- Step 3** Resolve the network DNS problem.
- Step 4** If the system can resolve the DNS names to the IP addresses but you still cannot connect to the system by 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 when the system is connected to the network.

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

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

Troubleshooting Installation Checks

This section describes the installation checks performed by `ce_install.sh` and `ce_check.sh` scripts. To troubleshoot by using the installation checks script, see the following sections:

- [Root User Check, page 5](#)
- [Check for OS, CPU, RAM, and Disk space, page 6](#)
- [Checks for dependent and CE Packages, page 6](#)
- [Check for Dependent OS Packages, page 7](#)
- [Installation Checks Performed by CE Check Script, page 7](#)
- [Check for OS Dependent Package Files Missing, page 7](#)

Root User Check

Problem If the user trying to install or run the check install script is not a root user, the following error message is displayed:

```
Reading XML file ./installRule.linux5.xml
check Root user.....
```

Error!!! Only user "root" can run check script!

Solution The root user option should be used to install the Cisco CE.

Check for OS, CPU, RAM, and Disk space

Problem The install and check install script validates the OS, CPU speed, RAM, and disk space usage to ensure that the configuration requirements are sufficient to install the Cisco Configuration Engine. The example below shows that the minimum RAM requirement is not meet within Cisco Configuration Engine.

```

===== System Requirement Check :          =====
check OS..... ok
check CPU..... ok
check Ram..... Error the machine has only 515536 Kbytes memory. Minimum requirement:
2000000 Kbytes.
check Disk Space '/var/tmp'..... ok
    
```

Solution Check the system requirements and provide the proper configuration to install the Cisco Configuration Engine.

Checks for dependent and CE Packages

Problem The install and check install scripts will check if any of the Cisco Configuration Engine packages are already installed and displays the warning message as shown below:

```

=====
Below lists package(s) which should not exist before CE 3.5.3 install. Please remove them
before running CE 3.5.3 installation script.
=====
..... package: SUNJava2-SDK, existing version: 1.6.0_05-0
..... package: mod_jk2, existing version: 2.0.4-4jpp_4rh
..... package: CSCOcnsfcgs, existing version: 1.4-0
..... package: ACE, existing version: 5.6.0-0
..... package: CSCOadmincommon, existing version: 1.3-0
..... package: CSCOcnscommon, existing version: 1.4-0
..... package: CSCOcnses, existing version: 1.9-0
..... package: CSCOcnsnsm, existing version: 1.5-0
..... package: CSCOcnsims, existing version: 1.5-0
..... package: CSCOcnspl, existing version: 1.3-0
..... package: CSCOdats, existing version: 1.3-0
..... package: CSCOemail, existing version: 1.0-0
..... package: CSCOencryption, existing version: 1.4-1
..... package: CSCOGroupAdmin, existing version: 1.5-1
..... package: CSCOimgw, existing version: 1.4-0.0
..... package: CSCOimgwConfig, existing version: 1.4-0.0
..... package: CSCOimgwDeviceServer, existing version: 1.4-0.0
..... package: CSCOnsmAdmin, existing version: 1.0-0
..... package: CSCOsrvr, existing version: 1.5-0
..... package: CSCOTools, existing version: 1.2-0
..... package: CSCOudiAdmin, existing version: 1.0-0
..... package: xerces-c, existing version: 2.8-0
    
```

Solution Uninstall the Cisco CE properly and then try to install or run the install check script.

Check for Dependent OS Packages

Problem The Cisco CE install and check install script will check for the OS dependent packages and display error messages if the required packages are not installed.

Below lists package(s) which should be shared between CE and other projects. It is now detected that these component(s) are not installed or of different version from that required by CE 3.5.2. Please remove the inappropriate packages and install required packages before re-running CE 3.5.2 installation script.

```
..... package: httpd, existing version: not installed
..... expected version: 2.0.52

..... package: httpd-suexec, existing version: not installed
..... expected version: 2.0.52

..... package: mod_ssl, existing version: not installed
..... expected version: 2.0.52
```

Please install the 3 missing package mentioned above from your Operating System distribution mentioned below.

Red Hat Enterprise Linux AS release 4 (Nahant Update 6)

Solution Install the required software from the distribution supported by the customer.

Installation Checks Performed by CE Check Script

Problem The check install script will check for the OS package being installed on the system.

```
Package 'httpd'is shared...

/bin/rpm -V httpd
S.5...T c /etc/rc.d/init.d/httpd
..?..... /usr/sbin/suexec
system failed: 256 exit_value = 1 signal_num = 0 dumped_core = 0

Following command failed: see ./checkError.log for details
/bin/rpm -V httpd

Warning package httpd is not properly installed
Run the command '/bin/rpm -V httpd' to see the issues
```

Solution Verify the error to see if the configurations are change and reinstall the packages accordingly.

Check for OS Dependent Package Files Missing

Problem The check install script will check for any missing files from the OS package that is installed on the system.

```
Package 'mod_ssl'is shared...

/bin/rpm -V mod_ssl
S.5...T c /etc/httpd/conf.d/ssl.conf
system failed: 256 exit_value = 1 signal_num = 0 dumped_core = 0

Following command failed: see ./checkError.log for details
/bin/rpm -V mod_ssl

Warning package mod_ssl is not properly installed
Run the command '/bin/rpm -V mod_ssl' to see the issues
```

Error file or directory /usr/lib/httpd/modules/mod_ssl.so doesn't exist
Please re-install the mod_ssl from your Operating System distribution mentioned below.
Red Hat Enterprise Linux Server release 5.2 (Tikanga)

Solution Reinstall the package properly from the OS distribution.

Troubleshooting the OpenLDAP and BDB

To troubleshoot Open Lightweight Directory Access Protocol (OpenLDAP) and Berkeley Data Base (BDB), see the following sections:

- [OpenLDAP Server Not Responding, page 8](#)
- [BDB Using Excessive Disk Space, page 8](#)

OpenLDAP Server Not Responding

Problem The OpenLDAP server is not responding.

Possible Cause This problem can occur after a system crash, power outage, or manual shutdown. If the OpenLDAP sever does not shut down gracefully, the data will corrupt.

Solution To resolve this problem, stop the OpenLDAP server, and then recover the data. Follow these steps:

Step 1 To stop the OpenLDAP server, enter the following command:
`/etc/init.d/NetAppOpenLDAP stop`

Step 2 To recover the data, enter the following command:
`$CISCO_CE_INSTALL_ROOT/bdb/bin/db_recover -h`
`$CISCO_CE_INSTALL_ROOT/openldap/var/openldap-data`

BDB Using Excessive Disk Space

Problem The BDB is using excessive disk space.

Possible Cause BDB creates transaction logs in the `$CISCO_CE_INSTALL_ROOT/openldap/var/openldap-data` file. If transaction logs are not purged, the BDB uses excessive disk space.

For information about the disk space, see the “System Requirements” and “Understanding Disk Space Calculation” sections in the *Cisco Configuration Engine Installation and Configuration Guide, 3.5.3*.

Solution To resolve this problem, follow these steps:

Step 1 To verify whether dbpurge.sh is running as a cron job, enter the following command:
`crontab -l`

Step 2 If crontab -l is not in the list, run the set up program to add it.

Step 3 To manually purge BDB transaction logs, enter the following command:
`$CISCO_CE_INSTALL_ROOT/CSCOcnsie/bin/dbpurge.sh`

Troubleshooting the Cisco CE Services

To troubleshoot Cisco Configuration Engine services, see the following sections:

- [Cisco CE Not Working Properly, page 9](#)
- [No Response Received for the XML Request, page 9](#)

Cisco CE Not Working Properly

Problem The Cisco Configuration Engine is not working properly.

Possible Cause This can occur if any of the processes fails.

Solution Use the Cisco CE monitor feature to check the status of the processes. The CE monitor checks the status of a set of processes at a configured time interval and reports the status in the `/var/log/CNSCE/ce_monitor/ce_monitor.log` file. The CE monitor exits if any of the processes fails.

To check the status of the processes, follow these steps:

-
- Step 1** Check the status of CE monitor to determine whether the service is up or down:
- For Linux, enter: `/etc/rc.d/init.d/MonitorCE status`
 - For Solaris, enter: `/etc/init.d/MonitorCE status`
- Step 2** Check the `/var/log/CNSCE/ce_monitor/ce_monitor.log` file to identify which process is down.
- Step 3** If a particular process is down, check the process to determine the problem.
-

No Response Received for the XML Request

Problem An XML request was sent, but you did not get a response.

Solution To resolve this problem, do the following in any order:

- To monitor events on the bus, use the **cns-listen** utility.
- For Intelligent Modular Gateway (IMGW) devices, do the following:
 - Set the IMGW logging level to **verbose**.
 - Check the following log files under the `/var/log/CNSCE/imgw` directory:
 - IMGW-LOG-<hostname>** (log file for the IMGW runtime)
 - IMGW-DEVMOD-LOG** (log file for debugging the IMGW script)
- For agent-enabled devices, configure **cns debug** on the router.

Troubleshooting the Web Services

To troubleshoot Web Services, see the following sections:

- [Cisco CE GUI Not Displaying, page 10](#)
- [Undeploying Services, page 10](#)
- [Timeout Error Message for Cisco Networking Services Agents, page 11](#)
- [Troubleshooting the Initial Configuration, page 11](#)

Cisco CE GUI Not Displaying

Problem The Cisco CE GUI is not displaying.

Solution To resolve this problem, follow these steps:

-
- Step 1** Check whether the Cisco CE service endpoint is up. Go to: `http://<CE hostname>/cns/services/<services>`. If the web page is displayed, the service is up.
- Step 2** If the web page is not displayed, check the **httpd status** (web server status).
- Step 3** If the httpd status is okay, deploy all or individual services.
- Go to: `cd $CISCO_CE_INSTALL_ROOT/CSCOcsie/bin.`
 - To deploy all services, enter the following command:
`./deploy.all.websvc`
 - To deploy an individual service, enter the following command:
`./deploy.<service>.websvc`
-

Undeploying Services

Problem How do I undeploy services?

Solution To undeploy services, follow these steps:

-
- Step 1** Go to: `cd $CISCO_CE_INSTALL_ROOT/CSCOcsie/bin.`
- Step 2** To undeploy all services, enter the following command:
`./undeploy.all.websvc`
- Step 3** To undeploy an individual service, enter the following command:
`./undeploy.<service>.websvc`
-

Timeout Error Message for Cisco Networking Services Agents

Problem When working with Cisco Networking Services (CNS) agents, you get a Connection Timeout error message.

Solution To resolve this problem, do the following in any order:

- Make sure that the CNS agent is enabled and is configured correctly:
 - CEConfigService requires CNS Config Agent.
 - acquireConfig() requires CNS Exec Agent.
 - CEImageService requires CNS Image Agent.
 - CEExecService requires CNS Exec Agent.



Note Do not use `execImmediate()` and `execImmedWithConversation()` to send the 12.4 XML payloads to the 12.3 agents.

- Check the log files. The following log files are located in the `/var/log/CNSCE/` directory:
 - **websvc/websvc.log** (web service general log)
 - **cfgsrv/cfgsrv/log** (config service log)
 - **imgsrv/imgsrv.log** (image service log)
 - **cfgsrv/exec-srv.log** (exec service log)
- Monitor the Event Bus. Go to: `cd $CISCO_CE_INSTALL_ROOT/CSCOcsie/tools`. Then enter the following command:


```
./cns-listen "cisco.>"
```
- Monitor the Simple Object Access Protocol (SOAP) XML payload. Go to: `cd $CISCO_CE_INSTALL_ROOT/CSCOcsie/tools`. Then enter the following command:


```
./ssldump -d port 80
```

Troubleshooting the Initial Configuration

To troubleshoot the initial configuration, see the following sections:

- [Problem with Initial Configuration, page 11](#)
- [Monitor Event Traffic and Cisco CE Process Status, page 13](#)

Problem with Initial Configuration

Problem The initial configuration does not work.

Solution To resolve this problem, follow these steps:

-
- Step 1** Make sure that you can access the device from Cisco CE and you can access Cisco CE from the device. Use the **ping** command to validate connectivity.
 - Step 2** Make sure that the device is agent-enabled.

In router configuration mode, enter **cns?**. If the **cns** command list is displayed, the device is agent-enabled. If the device is not agent-enabled, this command fails.

Step 3 Make sure that the Cisco CE is set up properly.

Cisco CE is set up in either crypto or plaintext mode. Make sure that the device set up and the Cisco CE set up are consistent.

Step 4 Make sure that the system processes are running properly. Enter the following on the Cisco CE server:

- To verify that all TibGates are up, enter the following command:

```
/etc/rc.d/init.d/EvtGateway status
```

```
/etc/rc.d/init.d/EvtGateway status
```



Note For information about TibGate event gateway ports, see the “Scalability Among Event Gateway Ports” chapter in the *Cisco Configuration Engine Installation and Configuration Guide, 3.5*.

- To verify that the httpd is up, enter the following command:

```
httpd status
```

- To verify that the Java process is up, enter the following command:

```
ps -ef | grep -i java | grep ConfigEngine
```

Step 5 Check the object status for the device in Cisco C E. If the status is green, the Cisco CE and the device are connected.

If the status is red, verify that the Event ID and Config ID matches with what is defined on the device. From the Cisco CE user interface, do the following:

- Choose **Devices > Edit Device**. The Edit Device page appears with a Groups list.
- From the Groups list, choose the group that contains the device, click the icon for the device.
- From the left pane, choose **Edit Information**. The Enter Device Information page appears.
- Click **Next**. The Select Group Membership page appears.
- Click **Next**. The Device IDs page appears.
- Verify that the Event ID matches with what is defined on the router.

Step 6 Verify the agent is set up on the device.

In non-configuration mode, enter the **show run** command to display the agent settings that are running. Then verify the following:

- ip host** <ce_host.domain_name> <ce_ipaddress>
- cns trusted-server** <ce_host.domain>
- cns trusted-server all-agents** <ce_host.domain_name>
- cns id string** <ce_ipaddress>
- cns id string** <ce_ipaddress> **event**
- cns event** <ce_ipaddress> <event-gateway port>
- cns config init** <ce_ipaddress>
- cns exec**

Step 7 If the authentication feature is enabled in Cisco CE, make sure that the device password (**cns password** <password string>), matches with what is defined in the Cisco CE user interface.

**Note**

You cannot see the password setting after you have configured it on the router, nor can you edit the password in Cisco CE. Therefore, you must reset the password. To reset the password, use the `resync device` feature in Cisco CE.

- Step 8** If you have tried all of the preceding steps but the initial configuration still does not work, use the **`debug cns config all`** command to enable debugging on the agent. Analyze the output to verify that the agent is set up correctly with proper connectivity.
- Step 9** If the initial configuration still does not work, reboot the device.

Monitor Event Traffic and Cisco CE Process Status

Use the following log files to monitor event traffic and Cisco CE process status:

- `/var/log/CNSCE/cfgsrv/cfgsrv.log, error.log`—Check the `cfgsrv` log file when the config agent is enabled and initial configuration is issued on the device.
- `/var/log/CNSCE/evtgateway/TibGateLog-<port>`—Check the TibGate log file when the event agent is enabled on the device.
- `/var/log/httpd/*.log, /var/log/CNSCE/tomcat/*.out, *.txt, *.log`—Check the Apache & Tomcat log files to make sure that the web server is running properly.
- `/var/log/CNSCE/appliance-setup.log`—Check the setup log file for Cisco CE set up, especially in crypto set up mode.
- `/var/log/CNSCE/websvc`—Check the web service log file to see whether the application programming interface (API) is invoked.

Troubleshooting a Configuration Update

To troubleshoot a configuration update, see the following sections:

- [CNS-Enabled Device Unable to Connect with Cisco CE, page 13](#)
- [CNS-Enabled Device Configuration Update Failed, page 15](#)
- [Configuration Update Stuck in Queue After Data Migration, page 17](#)
- [Configuration Update Stuck in Queue After Data Backup and Restore, page 18](#)

CNS-Enabled Device Unable to Connect with Cisco CE

Problem A device is created in the Cisco CE user interface but the device indicator displays a red status.

Possible Cause The red status indicates that the device is unable to connect with Cisco CE or it is still trying to connect. A connection delay can occur due to the device setting of the backoff timer. After the time has expired, the indicator does not turn to green, follow the steps given below.

Solution To resolve this problem, follow these steps:

- Step 1** Make sure that the Event ID and Config ID matches with what is defined on the device. Do the following from the Cisco CE user interface:
- Choose **Devices > Edit Device**. The Edit Device page appears with a Groups list.
 - From the Groups list, choose the group that contains the device, click the icon for the device.
 - From the left pane, choose **Edit Information**. The Enter Device Information page appears.
 - Click **Next**. The Select Group Membership page appears.
 - Click **Next**. The Device IDs page appears.
 - Verify that the Event ID and Config IP matches with what is defined on the router.

- Step 2** Make sure that the device type is **Agent Enabled Device**. From the Cisco CE user interface, do the following:
- Choose **Devices > Edit Device**. The Edit Device page appears with a Groups list.
 - From the Groups list, choose the group that contains the device. Click the icon for the device.
 - From the left pane, choose **Edit Information**. The Enter Device Information page appears.
 - Verify that the device type is **Agent Enabled Device**.

Step 3 Ping or telnet to the device to verify that the device is reachable from Cisco CE.

Step 4 From the Cisco CE server, make sure that TibGate, httpd, and the Java process are up.

- To verify that all TibGates are up, enter the following command:

```
/etc/rc.d/init.d/EvtGateway status
/etc/rc.d/init.d/EvtGateway status
```



Note For information about TibGate event gateway ports, see the “Scalability Among Event Gateway Ports” chapter in the *Cisco Configuration Engine Installation and Configuration Guide, 3.5.3*.

- To verify that the httpd is up, enter the following command:
`httpd status`
- To verify that the Java process is up, enter the following command:
`ps -ef | grep -i java | grep ConfigEngine`

Step 5 Check the following on the device:

- Make sure that the following Event ID string is defined:

```
cns id string <id string>
cns id string <id string> event
```

The default value of the `<id string>` is the hostname of the device. This ID must be the same as the Config ID defined in the Cisco CE host.

- To verify that the Cisco CE hostname or IP address is specified to receive the events, enter the following command:
`cns event <configengine hostname or ip address> keepalive 30 10`
- To verify that the Cisco CE hostname or IP address is reachable from the device, enter the following command:
`ping <configengine hostname or ip address>`

- d. If you are unable to reach the device through the ping command, use the **ip host** command to configure the device:


```
ip host <hostname> <ip address>
ip host <hostname.domainname> <ip address>
```
- e. (Optional) To resolve the hostnames, set up the DNS on the device by entering the following command:


```
ip name-server <ip address of DNS>
```

Step 6 If the device status changes from green to red after Cisco CE set up, follow the steps in “[Device Status](#)” section on page 25.

CNS-Enabled Device Configuration Update Failed

Problem The Device configuration update fails.

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

- Invalid commands in the configuration template.
- Device is not online (RED).

Solution To resolve this problem, follow these steps:

Step 1 If the device appears RED (offline), go to Step 2 and 3 to make the device GREEN (online) before proceeding with step 1.

- a. In the Cisco CE host, do the following:

Start the event listener and enter the following commands:

```
cd $CISCO_CE_INSTALL_ROOT/CSCOcnstools
./cns-listen ?cisco.>?
```

Check the cfgsrv log file. This file is located at: */var/log/CNSCE/cfgsrv/cfgsrv.log*.

In the device, use the **debug cns all** command to enable debugging. If debug messages displays the *CNS_INVALID_CLI_CMD* as shown below, the config template can contain invalid commands. Solution is to apply those commands one by one on the router to find which command failed and remove or fix them from the template.

```
85E1E440: 7572653E 3C696465 6E746966 6965723E ure><identifier>
85E1E450: 31323635 38333937 32393339 32313C2F 12658397293921</
85E1E460: 6964656E 74696669 65723E3C 636F6E66 identifier><conf
85E1E470: 69672D69 643E4643 48313333 39543032 ig-id>myDevice
85E1E480: 383C2F63 6F6E6669 672D6964 3E3C6572 </config-id><er
85E1E490: 726F722D 696E666F 3E3C6C69 6E652D6E ror-info><line-n
85E1E4A0: 756D6265 723E3930 3C2F6C69 6E652D6E umber>90</line-n
85E1E4B0: 756D6265 723E3C65 72726F72 2D6D6573 umber><error-mes
85E1E4C0: 73616765 3E434E53 5F494E56 414C4944 sage>CNS_INVALID
85E1E4D0: 5F434C49 5F434D44 3C2F6572 726F722D _CLI_CMD</error-
85E1E4E0: 6D657373 6167653E 3C2F6572 726F722D message></error-
85E1E4F0: 696E666F 3E3C2F63 6F6E6669 672D6661 info></config-failure>
85E1E500: 696C7572 653E>
```

Step 2 Check the following on the Cisco CE:

- a. Make sure that the Event ID and Config ID matches with what is defined on the device.

- b. Make sure that the object status for the device in Cisco CE is green. Green indicates that the Cisco CE and the device are connected.
- c. To verify that TibGate is up and running, enter the following command:

```
/etc/rc.d/init.d/EvtGateway status
/etc/rc.d/init.d/EvtGateway status
```



Note If encryption is enabled, the TibGate ports begin with even numbers that begins from 11012. If encryption is not enabled, the TibGate ports begin with odd numbers that begins from 11011. Each TibGate port can support a maximum of 500 devices. You specify the number of the TibGates during the Cisco CE set up program. Make sure that the number of devices on each TibGate port does not exceed the maximum. For details, see the “Scalability Among Event Gateway Ports” chapter in the *Cisco Configuration Engine Installation and Configuration Guide, 3.5.3*.

- d. If the authentication feature is enabled in the Cisco CE, make sure that the device password (**cns password <password string>**) that is defined in the Cisco CE user interface, matches with what is defined on the device. Otherwise, use the **resync device** command to reset the CNS password.

To use the **resync** command from the Cisco CE user interface, do the following:

- a. Go to **Devices > Resync Device**. The Resync Device page appears with a Groups list.
- b. From the Groups list, choose the group that contains the device you want to resynchronize. Then click the icon for the device.
- c. In the confirmation window, click **Ok**.
- e. Make sure that the downloading configuration semantics and syntax for the device are correct.
- f. If the device in the Cisco CE was initially set as None, then deleted, and then re-created as an agent-enabled device, you must rename the Config ID and Event ID on both the device and the Cisco CE user interface.
- g. During the Cisco CE setup, a port other than the default port 80 is configured for HTTP, make sure that the same port number is also configured on the device.

Step 3 Check the following on the device:

- a. Make sure that the following Event ID string is defined:

```
cns id string <id string>
cns id string <id string> event
```

The default value of the *<id string>* is the hostname of the device. This ID must be the same as the Config ID defined in the Cisco CE host.

- b. To verify that the Cisco CE hostname or IP address is specified to receive events, enter the following command:

```
cns event <configengine hostname or ip address> keepalive 30 10
```



Note Make sure that the TibGate port of this device is correct. The TibGate port must match the port that is defined in the Cisco CE.

- c. If the authentication feature is enabled on the Cisco CE, make sure that the device password (**cns password <password string>**) matches with what is defined in the Cisco CE user interface.



Note You cannot see the password setting after you configure it on the router, nor can you edit the password in Cisco CE. Therefore, you must reset the password. To reset the password, use the Resync Device feature in the Cisco CE.

- d. During the Cisco CE set up, if a port other than the default port 80 is configured for HTTP, make sure that the same port number is configured on the device. To configure the http port on the device, enter the following command:

```
cns config partial <CE hostname> <http port>
```

Step 4 If you have tried all the preceding steps and the device configuration update still fails, enable the debugging tools.

- In the Cisco CE host, do the following:
 - To start event listener, enter the following commands:


```
cd $CISCO_CE_INSTALL_ROOT/CSCOcnsie/tools  
./cns-listen "cisco.>"
```
 - Check the cfgsrv log file. This file is located at: */var/log/CNSCE/cfgsrv/cfgsrv.log*.
- In the device, use the **debug cns config all** command to enable debugging. Analyze the output to verify that the device is set up correctly with proper connectivity.

Step 5 Rerun the scenario, check the event traffic and the information from the device, capture the data, and then contact the Cisco TAC for assistance.

Configuration Update Stuck in Queue After Data Migration

Problem The configuration update is stuck in queue after data migration.

Possible Cause This problem can occur if you did not enter the correct country code and company code information during the set up program.

Solution After data migration from release 3.0 to 3.5, the OpenLDAP schema is transferred to a new host. To reuse the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches what is defined on the old host. Follow these steps:

Step 1 To reinitialize the system, enter the following command:

```
/opt/ConfigEngine/CSCOcnsie/reinitialize
```

Step 2 To run data migration again, enter the following command:

```
/opt/ConfigEngine/CSCOcnsie/bin/datamigrate
```

Step 3 To run the set up program again, enter the following command:

```
/opt/ConfigEngine/CSCOcnsie/setup
```



Note Make sure that you run the set up program in bash shell. If the shell is not in bash, press **ctrl-c** to exit. Configure your shell in bash, and then rerun the set up program.

Step 4 When entering the set up parameters, make sure that the country code and the company code information for the new host matches what is defined on the old host.



Note The country code and the company code in the OpenLDAP schema are case sensitive.

For detailed information about the parameters in the set up program, see the *Cisco Configuration Engine Administration Guide*.

Example

```
Choose operational mode of system. 0=internal directory mode, 1=external directory mode.
[0]
Enter country code: us
Enter company code: cisco
```

Configuration Update Stuck in Queue After Data Backup and Restore

Problem The configuration update is stuck in the queue after data backup and restore.

Possible Cause This problem can occur if you did not enter the correct country code and company code information during the set up program.

Solution When you back up data and restore it, the OpenLDAP schema is transferred to a new host. To reuse the existing OpenLDAP schema for the new host, make sure that the country code and the company code information on the new host matches what is defined on the old host. Follow these steps:

-
- Step 1** To reinitialize the system, enter the following command:
`/opt/ConfigEngine/CSCOcnsie/reinitialize`
 - Step 2** To run the data restore again, enter the following command:
`/opt/ConfigEngine/CSCOcnsie/bin/datarestore`
 - Step 3** To run the set up program again, enter the following command:
`/opt/ConfigEngine/CSCOcnsie/setup`



Note Make sure that you run the set up program in bash shell. If the shell is not in bash, press **ctrl-c** to exit. Configure your shell in bash, and then rerun the Setup program.

- Step 4** When entering the set up parameters, make sure that the country code and the company code information for the new host matches what is defined on the old host.



Note The country code and the company code in the OpenLDAP schema are case sensitive.

For detailed information about the parameters in the Setup program, see the *Cisco Configuration Engine Administration Guide*.

Example

```
Choose operational mode of system. 0=internal directory mode, 1=external directory mode.
[0]
Enter country code: us
Enter company code: cisco
```

Troubleshooting an Image Update

To troubleshoot an image update, see the following sections:

- [Information About Log Files, page 19](#)
- [Cannot Activate Image, page 19](#)
- [Activation Failed Due to Device Error, page 19](#)
- [Image Update Stopped, page 20](#)

Information About Log Files

The Log4j file is used as the logging facility for the Cisco CE server and the image server. The property file is located at: `<INSTALL_DIR>/CSCOcfgs/conf/logs.properties`. You can control the logging behavior by editing the `logs.properties` configuration file. This file is located at: `cd $CISCO_CE_INSTALL_ROOT/CSCOcnstie/conf`. The default level for logging is set to Debug. Accepted values are Debug, Info, Warn, Error, and Fatal.

- `/var/log/CNSCE/imgsrv/imgsrv.log`—Contains log messages from the server concerning the actions that you have performed that pertain to images, such as creating, updating, or deleting images. This log file also contains detailed message exchanges between the image server and devices during image distribution and activation.
- `/var/log/httpd/*.log`, `/var/log/CNSCE/tomcat/*.out`, `/*.txt`, `/*.log`—Contains log messages regarding the status of the web server.
- `/var/log/CNSCE/websvc`—Contains log messages regarding web service APIs.
- `/var/log/CNSCE/imgw/*`—Contains log messages regarding the IMGW.

Cannot Activate Image

Problem You are trying to activate an image but cannot activate it.

Possible Cause This problem can occur if the activation template does not contain the correct configuration. If the activation radio button is not checked when you associate the image with the device.

Solution To resolve this problem, make sure that the configuration is correct. Then try again to activate the image. Make sure the box is checked when associating the image with the device.

http://www.cisco.com/en/US/docs/net_mgmt/configuration_engine/3.5/administration/guide/image.html#wp1230605.

Activation Failed Due to Device Error

Problem Activation failed due to a device error. The device does not load the specified image.

Solution To resolve this problem, make sure that the image information matches the image that you have downloaded.

Image Update Stopped

Problem Image update stops and you receive the following error message:

```
2004-01-13 19:04:52,677 [c7200-1] DEBUG message.EvtMsgSender - Sent msg to
Identifier=1074049490996 of Type=MSG_IMAGE_UPDATE_STOPPED.
```

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

- File system could not be found.
- Space was insufficient for distributing the specified image.
- Server was unable to access the image file from a specified location.

Solution To resolve this problem, follow these steps:

Step 1 If the job stopped because the file system was not found, check the `imgsvr` log file to verify whether the file system name in the destination field is correct. This log file is located at: `/var/log/CNSCE/imgsvr.log`.

Example:

```
2005-11-03 15:31:39,974 [TP-Processor9] DEBUG action.UpdateImageProcess - RefCISDevice:
ImageID=[d2NonAgent],CN=[d2NonAgent],Inventory Device
Ref=[d2NonAgent],Password=[null],Activations=[{}],ActivationTemplate=[DemoRouter.cfgtpl],
Img_And_Dist=[{img1=HashCode=[558448476],Name=[DIST1131057049654],ImgRef=[img1],
Destination=[Colorado],Location=[http://cluster-rm/cns/LoadPage?HtmlFilename=home.html],
, EraseFileSys=[true],OverWrite=[true] . ,
image2=HashCode=[457703260],Name=[DIST1131057049658],ImgRef=[img2],Destination=[Denver],
Location=[http://cluster-rm/cns/LoadPage?HtmlFilename=home.html],EraseFileSys=[true],
OverWrite=[false] . }].
```

Step 2 If the job stopped because the space was insufficient for distributing the specified image, check the `imgsvr` log file to verify whether the file system has sufficient space for downloading the specified image. This log file is located at: `/var/log/CNSCE/imgsvr.log`.

Example:

```
2004-01-13 19:18:21,563 [c7200-1] DEBUG evaluation.DeviceEvaluator
-DeviceEvaluation=[Reachable=[true], Distribution Eval List Size=[1]:
List=[Required=[true],Reason=[Compare ImageFile in RunningImageInfo, Check FreeSpace and
Running Image MD5.],ErrorInfo=[null],SufficientSpace=[false] . , Activation Eval List
Size=[1]: List=[Required=[true],Reason=[Compare ImageFile in RunningImageInfo, Check
FreeSpace and Running Image MD5.],ErrorInfo=[null],SufficientSpace=[false] . }].
```

```
2004-01-13 19:18:21,563 [c7200-1] DEBUG distribution.DevicePerformer - Distribution
is required, but Space is not sufficient.
```

Step 3 If the job stopped because the server was unable to access the image from the specified location, make sure that you can access the URL in the image location field.

Example:

```
2005-11-04 15:52:52,690 [Thread-377] DEBUG evaluation.DeviceEvaluator - Retrieving
Inventory from Device=[ImageID=[d1],CN=[d1],Inventory Device
Ref=[d1],Password=[null],Activations=[{}],ActivationTemplate=[DemoRouter.cfgtpl],Img_An
d_Dist=[{img4=HashCode=[1543307114],Name=[DIST1131144742987],ImgRef=[img4],Destination=
[California], Location=[http://hostname/cns/LoadPage?HtmlFilename=home.html], EraseFileSys
=[true],OverWrite=[true] . }]. . . .
```

In Progress Job Fails

Problem Job gets stuck in *IN PROGRESS* state.

Solution Make sure the following commands are configured for image agent on the device.



Note

Substitute *myCE* with your Cisco CE hostname and *myCE_domain* with your Cisco CE fqdn.

```
//for plain text
cns trusted-server all-agents myCE
cns trusted-server all-agents myCE_domain
cns image server http://myCE 80/cns/HttpMsgDispatcher status
http://myCE 80/cns/HttpMsgDispatcher
//for crypto ssl connections - assume we use port 11012
cns trusted-server all-agents myCE
cns trusted-server all-agents myCE_domain
cns image server https://myCE 443/cns/HttpMsgDispatcher status
https://myCE 443/cns/HttpMsgDispatcher
```

Troubleshooting IMGW

To troubleshoot IMGW, see the following section:

- [Obtaining Detailed Debugging Information, page 21](#)

Obtaining Detailed Debugging Information

Problem How do I obtain the debugging information?

Solution To obtain the detailed debugging information, you must configure the log files for IMGW. To configure the log files for IMGW, follow these steps:

-
- Step 1** Configure the logging level for the IMGW daemon. During the Cisco CE set up program, configure the IMGW parameters to one of the listed values. Logging levels are Verbose, Error, and Silent.
- Step 2** To configure the logging level for the IMGW servlet, edit the following two lines in the `$CISCO_CE_INSTALL_ROOT/CSCOimgw/conf/imgw.properties` file:
- **IMGW_LOGFILE** `/var/log/CNSCE/IMGW/imgwservlet.log`
(/* location of IMGW servlet log file *)
 - **IMGW_LOGGING_LEVEL** `DEBUG`
(/* debug level - ERROR or DEBUG *)
-

Troubleshooting the Router

To troubleshoot the router, see the following section:

- [Enabling Debugging on the Router, page 22](#)

Enabling Debugging on the Router

Problem How do I enable debugging on the router?

Solution To enable debugging on the router, follow these steps:

-
- Step 1** To enable debugging on the router, use the **debug cns image all** command.
- Step 2** If you are not on the console, enter the **term mon** command.
- Step 3** After the job completes, verify the file on the router by entering the **dir** command. The image file should display.
-

General Troubleshooting

For general troubleshooting tips, see the following sections:

- [Error Message: Failed to Create the Device on Remote Database, page 22](#)
- [CNS-listen Command Failed to Execute, page 23](#)
- [Configuring the CNS Event Backup with SSL., page 23](#)
- [HTTPD is Down When Crypto is Enabled, page 24](#)
- [Web Service Deployment Error When Crypto is Enabled, page 24](#)
- [Backup and Restore Fails, page 25](#)
- [Device Status, page 25](#)
- [Backup Job Fails, page 26](#)

Error Message: Failed to Create the Device on Remote Database

Problem You get the following error message:

```
Failed to create the Device. Could not create Object: DN=
[cn=jctest, ou=CISDevices,ou=CISObjects,ou=configengine,o=cisco
[LDAP: error code 50 - no write access to parent]
```

Solution To resolve this problem, follow these steps:

-
- Step 1** On the remote directory server machine, stop the OpenLDAP server by entering the following commands:
- In Solaris, enter: **/etc/init.d/NetAppOpenLDAP stop**
 - In Linux, enter: **/etc/rc.d/init.d//NetAppOpenLDAP stop**

Step 2 Open the `$CISCO_CE_INSTALL_ROOT/openldap/etc/openldap/slapd.conf` file. Then add the following:

```
# open write permission to support external directory
access to *
    by * write
    by * read
    by anonymous auth
```

Step 3 To start the OpenLDAP server, enter the following commands:

- In Solaris, enter: `/etc/init.d/NetAppOpenLDAP start`
- In Linux, enter: `/etc/rc.d/init.d/NetAppOpenLDAP start`

CNS-listen Command Failed to Execute

Problem The `cns-listen` command failed to execute.

Possible Cause This problem could occur if the values you entered for the CNS Event Bus Service and the CNS Event Bus Daemon parameters do not match the values you used in the `$cns-listen` command.

Solution To resolve this problem, make sure that you use the same value in the command that you entered for the parameters. For example:

```
Enter CNS Event Bus Service Parameter: [7500] 7800
Enter CNS Event Bus Daemon Parameter: [7500] 7900
cns-listen command:
$cd $CISCO_CE_HOME/tools
$cns-listen -service 7800 -daemon 7900
```

Configuring the CNS Event Backup with SSL.

The configuration is explained with two servers in the set up. The primary server is `imgw-test15.cisco.com` and the backup server is `imgw-test35.cisco.com`. The sample configuration shown below is explained using the terminal `enrollment` mode.

To configure the CNS event backup with SSL, follow these steps:

Step 1 Create the trust point. This example shows how to create the trust point.

```
crypto ca trustpoint imgw-test15.cisco.com
enrollment mode ra
enrollment terminal
usage ssl-client
crypto ca trustpoint imgw-test35.cisco.com
enrollment mode ra
enrollment terminal
usage ssl-client
```

Step 2 Enter the Key by using the copy and paste method. This example shows how to enter key by using the copy and paste method.

```
crypto ca authenticate imgw-test15.cisco.com
<Enter the crypto base64 key for imgw-test15>
```

```
crypto ca authenticate imgw-test35.cisco.com
<Enter the crypto base64 key for imgw-test35>
```

Step 3 Configure the IP host. This example shows how to configure the IP host.

```
ip host imgw-test35.cisco.com 172.27.250.134
ip host imgw-test15.cisco.com 172.27.117.223
ip host imgw-test15 172.27.117.223
ip host imgw-test35 172.27.250.134
ip domain-lookup
```

Step 4 Configure the cns password if applicable. For more information, see My test was without cns password.

Step 5 CNS configuration is done. This example shows the CNS configuration.

```
cns trusted-server all-agents imgw-test15.cisco.com
cns trusted-server all-agents imgw-test15
cns trusted-server all-agents imgw-test35.cisco.com
cns trusted-server all-agents imgw-test35
cns id hardware-serial
cns id hardware-serial event
cns id hardware-serial image
cns event imgw-test15.cisco.com encrypt 11014 reconnect-time 10
cns event imgw-test35.cisco.com encrypt 11014 backup
cns config partial imgw-test15.cisco.com encrypt 443
cns exec encrypt 443
cns image server
https://imgw-test15.cisco.com/cns/HttpMsgDispatcher status
https://imgw-test15.cisco.com/cns/HttpMsgDispatcher
```

HTTPD is Down When Crypto is Enabled

Problem The HTTPD service is down when crypto is enabled.

Possible Cause This problem can occur during the Cisco Configuration Engine Setup program and when you use invalid values for the remote key file and remote certificate file.

Solution To resolve the problem, make sure that you use valid values for the remote key file and remote certificate file. For example:

```
Enable cryptographic (crypto) operation between Event Gateway(s)/Config
server and device(s) (y/n)? [n] y
Enter absolute pathname of remote key file: /opt/server.key
Enter absolute pathname of remote certificate file: /opt/server.crt
```

Web Service Deployment Error When Crypto is Enabled

Problem You get the following web service deployment error messages:

```
Following command failed: see /var/log/CNSCE/appliance-setup.log for
details/opt/CSCOcsie/bin/deploy.config.websvc [-wsdl]
```

```
Deploying image web services ...
```

```
Following command failed: see /var/log/CNSCE/appliance-setup.log for
details/opt/CSCOcsie/bin/deploy.image.websvc [-wsdl]
```

Solution To resolve this problem, follow these steps:

-
- Step 1** Make sure that the Tomcat and HTTPD status is up.
 - Step 2** Enter the following command:

```
wget https://$HostName/cns/services/CEAdminService
```

If the command fails to execute, the domain name might not be set up correctly.
 - Step 3** Verify the host network settings at:

```
/etc/hosts, /etc/resolv.conf
```
-

Backup and Restore Fails

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 Universal Time Coordinate (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 ]
#
```

Device Status

Problem After Cisco Configuration Engine setup, the device status changes from green to red in a few minutes. This problem occurs on the Solaris 10 platform, right after restarting the Cisco Configuration Engine services.

Possible Cause This problem could occur if the TibGate processes shut down a few minutes after starting.

Solution To resolve this problem, follow these steps:

-
- Step 1** To check whether the TibGate processes are running, enter *one* of the following commands:
`/etc/init.d/EvtGateway`
`/etc/init.d/EvtGatewayCrypto`
- Step 2** If the TibGate processes are not running, ask your System Administrator to disable NISPlus service.
- Step 3** If the device status is still red, see the [“CNS-Enabled Device Unable to Connect with Cisco CE” section on page 13](#) for a possible solution.
-

Backup Job Fails

Problem The scheduled backup job fails.

Possible Cause The **crontab** command is used to schedule the 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 the 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.

Event Gateway Problem

Problem . I setup my Cisco Configuration Engine correctly, but the device is shown as RED or could not be auto-discovered. Why my device is not connecting to Cisco Configuration Engine?

Solution To resolve this problem, follow these steps:

-
- Step 1** Make sure the **cns trusted-server all-agents ce-host** and **cns config partial ce-host** commands are configured on the device where **ce-host** is the IP address or the hostname of the Cisco Configuration Engine.
- Step 2** Make sure all the TibGate processes are running by using the command: **/etc/init.d/EvtGateway status** and/or **/etc/init.d/EvtGatewayCrypto status** depending upon its mode (plain-text or crypto) enabled between the Cisco Configuration Engine and the devices. If the TibGate processes cannot be started and with the permission denied error, disable the SELinux by modifying the **/etc/selinux/config** file, change the status of SELINUX to disabled then uninstall the Cisco Configuration Engine. Reboot the server before reinstalling the Cisco Configuration Engine.
- Step 3** If results from the step 1 and 2 are verified and devices are still not in green, change the value of the **WAIT_AFTER_CONFIG** to a bigger value like 2 or 2.5, in the **\$CISCO_CE_HOME/conf/resource.properties** file. Restart the Cisco Configuration Engine by using the command **\$CISCO_CE_HOME/bin/setup -r**.
-

Device Status in Red

Problem . I setup my Cisco Configuration Engine correctly and I could see the new port assigned to the device by using the `$(CISCO_CE_HOME)/tools/cns-listen` debugging tool. I could not see the device and the device status is in red. However, the device shows up in the device discovery GUI and the connect event is never received by the Cisco Configuration Engine.

Solution To resolve this problem, follow these steps:

-
- Step 1** Make sure the `cns trusted-server`, `all-agents ce-host`, and `cns config partial ce-host` commands are configured on the device where `ce-host` is the IP address or the hostname of the Cisco Configuration Engine.
 - Step 2** If this is a slow network, increase the `WAIT_AFTER_CONFIG` timer in `$(CISCO_CE_HOME)/conf/resource.properties` and try the operation again. Increasing the wait timer will impact the overall performance. So, make sure to find a shortest wait time that works in your network environment. 1 means 1 second. 1.5 means 1.5 seconds, and so on.
 - Step 3** After changing the value, restart the Cisco Configuration Engine by using the command `$(CISCO_CE_HOME)/bin/setup -r`.
-

Configure Device with Ports

Problem Can I configure my device to point to the same Cisco Configuration Engine but different ports as the primary and backup Cisco Configuration Engine?

Solution No. The Cisco Configuration Engine can only either be the primary or the backup, but cannot be both.

Config Initial Status

Problem After I use the port auto-assignment function, I could not get the status of my config initial.

Solution Command `cns config initial ce-host` reports the config initial status through Event Gateway (by default). If you are using port auto-assignment function, you should post the status through HTTP. For example, `cns config initial ce-host` status <http://ce-host/cns/PostStatus> should be configured on the device.

Device with Same Configuration

Problem When I push a configuration job to a device, another device got the same config?

Solution . The DeviceID needs to be unique within the Cisco Configuration Engine namespace. Make sure that the two devices do not have the same config Id, event Id, and image Id.

Cisco CE Server Crashes on Linux Server

Problem On the Linux server, the Cisco Configuration Engine server crashes or the TibGate processes could not start and displays the following error messages:

```
/ce/ConfigEngine/CSCOcnsie/bin/TibGate: error while loading shared libraries:
/ce/ConfigEngine/CSCOcnsie/bin/TibGate: error while loading shared libraries:
/ce/ConfigEngine/CSCOcnsie/bin/TibGate: error while loading shared libraries:
reloc: Permission denied
Start Dispatcher TibGate (Event Gateway) process at port 11011
/ce/ConfigEngine/CSCOcnsie/bin/TibGate: error while loading shared libraries:
/ce/ConfigEngine/CSCOcnsie/bin/TibGate: error while loading shared libraries:
reloc: Permission denied
Start TibGate (Event Gateway) process at port 11013
```

Solution Make sure the SELinux is not enabled on the Linux as this might be the default option during installation. To disable SELinux, **edit /etc/selinux/config**, change SELINUX to disabled. Uninstall the Cisco CE, and then reboot the server before reinstalling the Cisco Configuration Engine.

GUI Display Problem in Internet Explorer 6.0

Problem Discover device option has a GUI display issue in the Internet Explorer version 6.0 for more than 2000 devices.

Possible Cause When more than 2000 devices are discovered by using Internet Explorer 6.0, then for some of the devices listed in the discover window are not displayed properly. It was just blank. This is an issue only with the Internet Explorer version 6.0.

Solution You can discover up to 2000 devices without any issues. User can **click > select** 2000 devices at one shot and create them. The other work around will be to use Internet Explorer 7.0 browser.

Accessing Cisco CE GUI

Problem After I setup the Cisco CE, I cannot access the Cisco Configuration Engine GUI.

Solution Make sure that the firewall on your Linux server is not enabled. To disable the firewall on a Linux server, you can use the following commands: **/etc/init.d/iptables save** and **/etc/init.d/iptables stop**.

Device Configuration Problem

Problem Device got unintended configuration update.

Solution Make sure to use the correct configuration template and the DeviceID is unique within the Cisco Configuration Engine namespace. For example, use the hardware-serial or UDI as DeviceID.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Troubleshooting Guide for Cisco Configuration Engine 3.5.3

© 2011 Cisco Systems, Inc. All rights reserved.

