

For general troubleshooting tips, see the following sections:

### Contents

- [1 Failed to Create the Device on Remote Database](#)
- [2 CNS-listen Command Failed to Execute](#)
- [3 Configuring the CNS Event Backup with SSL](#)
- [4 HTTPD Service Down](#)
- [5 Web Service Deployment Error](#)
- [6 Backup and Restore Fails](#)
- [7 Device Status](#)
- [8 Backup Job Fails](#)
- [9 Event Gateway Problem](#)
- [10 Device Status in Red](#)
- [11 Configure Device with Ports](#)
- [12 Config Initial Status](#)
- [13 Device with Same Configuration](#)
- [14 Cisco CE Server Crashes on Linux Server](#)
- [15 GUI Display Problem in Internet Explorer 6.0](#)
- [16 Accessing Cisco CE GUI](#)
- [17 Device Configuration Problem](#)

### 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:

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
```

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
```

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 can occur if the values entered for the CNS Event Bus Service and the CNS Event Bus Daemon parameters do not match the values 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:

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
```

2. Enter the Key using the copy and paste method. This example shows how to enter the Key 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>
```

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
```

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

## General\_Troubleshooting

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 Service Down

**Problem:** The HTTPD service goes down when the crypto is enabled.

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

**Solution:** To resolve the problem, make sure that you use valid values for the remote key file and the 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

**Problem:** You get the following web service deployment error messages:

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

**Solution:** To resolve this problem, follow these steps:

1. Make sure that the Tomcat and HTTPD status is up.
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.
```

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 can 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:

1. Connect to the console if you cannot connect using SSH.
2. Log in to the host system as root.
3. To determine whether the time is correct, enter the following command:

```
# date
```

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 set up, the device status changes from green to red in a few minutes. This problem occurs on the Solaris 10 platform, after re-starting the Cisco Configuration Engine services.

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

**Solution:** To resolve this problem, follow these steps:

1. To check whether the TibGate processes are running, enter one of the following commands:

```
/etc/init.d/EvtGateway
/etc/init.d/EvtGatewayCrypto
```

2. If the TibGate processes are not running, ask your system administrator to disable NISPlus service.
3. If the device status is still red, see the ?CNS-Enabled Device Unable to Connect with Cisco Configuration Engine? section 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:** After setting up the Cisco Configuration Engine correctly, the device is shown as RED or could not be auto-discovered. Why my device is not connecting to the Cisco Configuration Engine?

**Solution:** To resolve this problem, follow these steps:

1. Make sure that 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.
2. Make sure that 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.
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 such as 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:** After setting up the Cisco Configuration Engine correctly, 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:

1. Make sure that 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.
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.
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/CSCOcsie/bin/TibGate: error while loading
shared libraries:
/ce/ConfigEngine/CSCOcommon/lib/libibmldap.so: cannot
restore segment prot after reloc: Permission denied
Start Dispatcher TibGate (Event Gateway) process at port 11011
/ce/ConfigEngine/CSCOcsie/bin/TibGate: error while loading
shared libraries:
/ce/ConfigEngine/CSCOcommon/lib/libibmldap.so: cannot
restore segment prot after reloc: Permission denied
Start TibGate (Event Gateway) process at port 11013
```

**Solution:** Make sure that 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.

## General\_Troubleshooting

**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 Cisco Configuration Engine, 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 device ID is unique within the Cisco Configuration Engine namespace. For example, use the hardware-serial or UDI as device ID.