



Diagnosing Problems With CiscoWorks Server

Use these tools and suggestions to diagnose problems with the CiscoWorks server:

- [Verifying Server Status](#)
- [Testing Device Connectivity](#)
- [Troubleshooting the CiscoWorks Server](#)
- [Troubleshooting Suggestions](#)

Verifying Server Status

There are several tools that enable you to gather and analyze information about your CiscoWorks Server. See [Table 10-1](#) and [Table 10-2](#).

Table 10-1 Server Status

Task	Purpose	Action
Administrative Tasks		
Perform self test.	Runs self-tests and generates a report with the results.	Select Server > Admin > Self Test.
All Users		
Check process status.	Checks whether back-end processes are in an interim state.	Select Server > Admin > Processes.
Collect server information.	Provides system information, environment, configuration, logs, and web server information.	Select Server > Admin > Collect Server Information Or Enter the following command: <ul style="list-style-type: none"> • <code>NMSROOT\bin\collect.info</code> (on Windows) • <code>NMSROOT/bin/collect.info</code> (on Solaris) where <i>NMSROOT</i> is the directory where you installed CiscoWorks.

Table 10-1 Server Status

Task	Purpose	Action
MDC Support	<p>The MDC Support utility collects log files, configuration settings, memory info, complete system related info, process status and host environment information.</p> <p>It also collects any other relevant data, into a deliverable tar (compressed form) file to support the MDCs installed.</p> <p>The MDC Support utility also queries CCR for any other support utilities registered, and run them.</p> <p>Other MDCs need to register their own support utilities that will collect their relevant data.</p>	<p>For Windows go to, <i>NMSROOT\MDC\bin</i> and run the command: MDCSupport.exe</p> <p>The utility creates a tar file in <i>NMSROOT\MDC\etc</i> directory.</p> <p>If <i>\etc</i> directory is full, or if you want to preserve the data collected previously by not over writing the tar file, you may create another directory by running the following command: MDCSupport.exe Directory</p> <p>For Solaris,</p> <ol style="list-style-type: none"> 1. Set LD_LIBRARY_PATH Environment variable to <i>/opt/CSCOpX/MDC/lib : /opt/CSCOpX/lib:</i> 2. Go to <i>/opt/CSCOpX/MDC/bin</i> and run the command: ./mdcsupport <p>The utility creates a tar file in <i>CSCOpX/MDC/etc</i> directory.</p>
MDCSupport (Continued)		<p>If <i>\etc</i> directory is full, or if you want to preserve the data collected previously by not over writing the tar file, you may create another directory by running the following command: ./mdcsupport Directory</p> <p>Before you close the command window, ensure that the MDC Support utility has completed its action.</p> <p>If you close the window prematurely, the subsequent instances of MDCSupport Utility will not function properly.</p> <p>If you happen to close the window, delete the <i>mdcsupporttemp</i> directory from <i>NMSROOT\MDC\etc directory</i>, for subsequent instances to work properly.</p>

Testing Device Connectivity

The connectivity tools enable you to test device connectivity and reachability and troubleshoot nonresponsive devices. Some connectivity tools require system administrative-level privileges (see [Connectivity Tools Tasks Table 10-2](#)).

Table 10-2 **Connectivity Tools Tasks**

Task	Purpose	Action
Traceroute	Detects routing errors between the network management station and a target device.	Select Device Center > Tools > Traceroute. See Using Traceroute for details.
Ping a device	Tests device reachability using an ICMP echo message and its reply.	Select Device Center > Tools > Ping See Using Ping for details.
Check Management Station to Device	Checks the connectivity between the CiscoWorks Server and a device.	Select Device Center > Tools > Management Station to Device See Checking Device Connectivity for details.
Packet Capture	Captures live data from the CiscoWorks machine to aid in troubleshooting.	Select Device Center > Tools > Packet Capture See Using Packet Capture for details.
To set an SNMP object on a device.	Sets an SNMP object on a device for purposes of controlling the device.	Select Device Center > Tools > SNMP Set See Using SNMP Set for details.
To walk the MIB tree of a device	Walks the MIB tree of a device starting from a given OID for troubleshooting, or gathering information about a device.	Select Device Center > Tools > SNMP Walk See Using SNMP Walk for details.
Telnet to a Device	Connects to a Device to using Telnet.	Select Device Center > Tools > Telnet See Checking Device Connectivity for details.

Troubleshooting the CiscoWorks Server

This section provides information on frequently asked questions (FAQs) and suggestions for troubleshooting the CiscoWorks Server components.

If the suggestions do not resolve the error, check the Release Notes supporting your platform for possible workarounds, or contact the Cisco TAC or your customer support.

Frequently Asked Questions

- When I connect to the CiscoWorks Server in the secure mode (HTTPS) using Netscape Navigator, the browser returns I/O errors and displays the message `Netscape has encountered bad data from the server`. Why does this happen?
- When I invoke CiscoWorks in the secure mode (HTTPS), there are too many dialog boxes. This makes the process tedious. Is there a way to reduce the number of dialog boxes and steps?
- When I invoke CiscoWorks, I am unable to get to the login page directly. Instead, I am facing a security alert related to the site's security certificate. It asks for my input to proceed further. Why?
- My server certificate for CiscoWorks has expired. What should I do?
- Which version of the Java Plug-in should I use for CiscoWorks to function properly?
- Is there anything I should do before I invoke Netscape Navigator sessions in UNIX systems to run CiscoWorks?
- Why do some CiscoWorks applications not appear in the product?
- Why cannot I start my CiscoWorks application?
- What kind of directory structure does CiscoWorks use when backing up data?
- I'm locked out of the CiscoWorks Server. Why did this happen, and how do I regain access?
- What if the database is inaccessible?
- How do I change the port for osagent in Windows?
- How do I change port for osagent in Solaris?
- How do I change the ESS port in Solaris?
- How do I change ESS port in Windows?
- I have configured the Active Directory Login Module but it does not work. How can I analyze the problem?
- How do I change the IP Address of the CiscoWorks Server after installing it, or after running it for a while?
- Do I need to change the CiscoWorks configuration after changing the IP address?
- How do I change the Hostname of the CiscoWorks Server after installing it, or after running it for a while?
- How do I find out which devices are supported by a particular application?
- How do I verify if SSH is enabled or disabled on my device using CiscoWorks Server?
- How do I verify if SSH is enabled or disabled on my device using CiscoWorks Server?
- Is it possible to have both CiscoWorks and ACS on the same machine?
- How do I change the casuser password in Windows?

- How do I change the CiscoWorks user password?
- How do I enable/disable ACS Communication on HTTPS from CLI?
- How do I change web server port numbers?
- How do I increase Tomcat heap size?
- How do I enable debugging in MICE?
- What does cmf stand for?
- Why does the Apache process not come up after installation or why does the process go down suddenly?
- Why task-2-role mapping is not synchronized between the ACS server and the CiscoWorks server, sometimes?
- What does a diskWatcher process do?
- How do I avoid the SSL port conflict between HPOV and Common Services servers and run them both on the same system?

Q. When I connect to the CiscoWorks Server in the secure mode (HTTPS) using Netscape Navigator, the browser returns I/O errors and displays the message `Netscape has encountered bad data from the server`. Why does this happen?

A. This problem occurs when you:

- Create a new server certificate using the same hostname
- Set the browser to accept the old server certificate, till it expires

Typically, this problem is fixed when you clear the entry for your old server certificate from the browser.



Note The I/O errors in Netscape Navigator running in secure mode (HTTPS) is often caused by configured certificates in the client computer.

Q. When I invoke CiscoWorks in the secure mode (HTTPS), there are too many dialog boxes. This makes the process tedious. Is there a way to reduce the number of dialog boxes and steps?

A. Yes. You have the following options:

- If you are using Self-signed certificates:
 - In Netscape Navigator, select the option **Accept the Server Certificate forever (until it expires)** in the New Site Certificate wizard, if you are confident about the identity of the server.
 - In Internet Explorer, install the certificate in the browser's trusted certificate stores, if you are confident about the identity of the server.
- Use a server certificate issued by a prominent third party certificate authority (CA).
- Configure the hostname in your server certificate properly, and use the same hostname to invoke CiscoWorks.

- Q.** When I invoke CiscoWorks, I am unable to get to the login page directly. Instead, I am facing a security alert related to the site's security certificate. It asks for my input to proceed further. Why?
- A.** CiscoWorks does not have any control over this behavior. This is an expected browser behavior (Microsoft Internet Explorer or Netscape Navigator), to ensure proper security.

This appears if one of the following conditions is not satisfied:

- The certificate of the server (CiscoWorks Server in this case) must be issued by trusted Certificate Authority.
- The date of the certificate must be valid. (Each certificate is assigned a validity period. It can range from 21 days to 5 years).
- The name of the certificate and name of the page (or the name typed in the address bar of the browser) are the same.

To view the certificate information:

- Click **View Certificate**, in the alert box for Internet Explorer.
- Click **Examine Certificate** in the alert box for Netscape Navigator.

The server should be invoked with the name same as the Issued to' field of the certificate.

To install the certificate in Internet Explorer:

Step 1 Click **View Certificate** in the alert box.

The Certificate dialog box displays the Certificate information.

Step 2 Click **Install Certificate**.

For Netscape Navigator, you may select the Accept this Certificate Permanently radio button in the security alert dialog box.

- Q.** My server certificate for CiscoWorks has expired. What should I do?
- A.** If you are using a self-signed certificate, you can create a new certificate using the Create Self Signed Certificate option. For more information, see [“Creating Self Signed Certificates” section on page 4-7](#).

If you are using a third party issued certificate, you must contact the certificate authority (CA) and renew the certificate. You can use a self-signed certificate till you get the certificate renewed by the CA.



Note

Before you perform any certificate management operations—creating or modifying certificates, back up the certificate files, the server private key in particular, and keep them in a safe location.

- Q.** Which version of the Java Plug-in should I use for CiscoWorks to function properly?
- A.** CiscoWorks supports Java Plug-in 1.4.2_08 only in all the supported clients and operating systems. We recommend that you do not install any other Plug-ins other than this one, for CiscoWorks to function properly.
- Q.** Is there anything I should do before I invoke Netscape Navigator sessions in UNIX systems to run CiscoWorks?
- A.** Yes. You must **source** the file /jpi.cshrc before invoking any Netscape session in UNIX systems, so that the environment is set for the browser to function properly on invoking CiscoWorks.

- Q.** Why do some CiscoWorks applications not appear in the product?
- A.** The CiscoWorks Server represents a common set of management services which are shared by multiple network management applications. These services are enabled when a suite is installed and an application that relies on a particular service enables it.

If a particular suite of applications does not use a particular service, the service might not appear on the CiscoWorks Homepage. Applications and application suites may not use these features at all, or to the fullest extent.

See the User Guide for your application suite to determine the extent to which these features are used.

- Q.** Why cannot I start my CiscoWorks application?
- A.** If you cannot start your CiscoWorks application and get error messages complaining that the WebServer might not be running. This may occur although **pdshow** indicates that those processes are up and running. You might need to check how your machine is resolving its server name and IP address.

The CiscoWorks CORBA applications require name resolution to work properly. Domain Name Service (DNS) is a must for CiscoWorks CORBA applications to work properly.

Configure the name resolution mechanism and restart the CiscoWorks Server to access the application correctly.

- Q.** What kind of directory structure does CiscoWorks use when backing up data?
- A.** CiscoWorks uses a standard database structure for backing up all suites and applications. See [Table 10-3](#) for sample directory structure for the CiscoWorks Server.

Table 10-3 Sample Backup Directory

Directory Path	Description	Usage Notes
/tmp/1	Number of backups	1, 2, 3...
/tmp/2/cmfb	Application or suite	Backs up CiscoWorks Server applications.
/tmp/1/cmfb/filebackup.tar	CiscoWorks Server application tar files	Application data is stored in the datafiles.txt which are compiled into the tar file.
/tmp/1/cmfb/data base	CiscoWorks Server database directory	Includes files for each database: xxx_DbVersion.txt xxx.db database files xxx.log database log files xxx.txt database backup manifest file

- Q.** I'm locked out of the CiscoWorks Server. Why did this happen, and how do I regain access?
- A.** There are several reasons why you might have been locked out. Most likely it is caused by the changes made using the Select Login Module option. You must replace the incorrect login module with a default configuration, log into CiscoWorks, and return to the login module to correct one or more of the following:
- Session Time out
 - Change from SSL mode to non-SSL mode
 - Change from non-SSL mode to SSL mode

- Log out from any other CiscoWorks application
- Visit other sites and then return to CiscoWorks

Do *not* alter the existing technologies in the default configuration file.

If all of the parameters listed are correct, see the “[Troubleshooting Suggestions](#)” section on page 10-26.

- Q.** What if the database is inaccessible?
- A.** If the server is not able to connect to the database, the database might be corrupt or inaccessible. This can occur if processes are not running. Try the following:

-
- Step 1** Log in to CiscoWorks as **admin**.
- Step 2** Select **Server > Admin > Process** to get a list of CiscoWorks back-end processes that have failed.
- Step 3** Select **Server>Admin> Self Test**.
- Click **Create** to create a report.
 - Click **Display** to display the report.
- Step 4** Select **Server > Admin > Collect Server Information**.
- Step 5** Click the **Product Database Status** link to get detailed database status.
- Step 6** Contact the Cisco TAC or your customer support to get the information you need to access the database and find out details about the problem.

After you have the required information, perform the following tasks for detecting and fixing database errors.

Depending upon the degree of corruption, the database engine may or may not start. For certain corruptions, such as bad indexes, the database can function normally until the corrupt index is accessed.

Database corruptions, such as index corruptions, can be detected by the dbvalid utility, which requires the database engine to be running.

To detect database corruption:

-
- Step 1** Log on as root (UNIX) or with administrator privileges (Windows).
- Step 2** Stop the Daemon manager if it is already running:
- UNIX—`/etc/init.d/dmgttd stop`
 - Windows—`net stop crmdmgttd` (enter this command in an MS-DOS window)
- Step 3** Make sure no database processes are running and there is no database log file. For example, if the database file is `/opt/CSCOpX/databases/rme/rme.db`, the database log file is `/opt/CSCOpX/databases/rme/rme.log`. This file is not present if the database process shuts down cleanly.
- Step 4** (UNIX only) Check if the database files(s) and the transaction log file (*.log) are owned by user casuser. If not, change the ownership of these files to user casuser and group casusers.

Step 5 Run the command:

```
cd NMSROOT/objects/db/conf
```

```
NMSROOT/bin/perl configureDb.pl action=validate dsn=<cmf>
```

The **dbvalid** command displays a list of tables being validated. The Validation utility scans the entire table, and looks up each record in every index and key defined on the table. If there are errors, the utility displays something like:

```
Validating DBA.xxxx
run time SQL error -- Foreign key parent_is has invalid or duplicate index
entries 1 error reported
```

If the above command reports any error, you may try:

- Restoring from a previous good backup
- or
- Reinitializing database



Caution All the current data will be lost.

To do this, you have to run the following command:

```
NMSROOT\bin\perl NMSROOT\bin\dbRestoreOrig.pl dsn=dsn dmprefix=dmprefix
```

For Common Services, *dsn* is *cmf* and *dmprefix* is *Cmf*.

Q. How do I ensure that *jrm* is running fine?

A. To check whether *jrm* is working on Windows, at the command prompt enter:

```
cwjava -cw NMSROOT com.cisco.nm.cmf.jrm.jobcli
```

To check whether *jrm* is working on Solaris, at the command prompt enter

```
cwjava -cw NMSROOT com.cisco.nm.cmf.jrm.jobcli
```

- If you get a message `Established connection with JRM`, then EDS, EDS-GCF and *jrm* are running.
- If you do not get the above message, contact the technical assistance center with the error message.
- If your *jrm* is down or inaccessible, you'll get a message while accessing the UIs.

Q. How do I change the port for *osagent* in Windows?

A. To change the port for *osagent* in Windows:

Step 1 Backup your Windows registry.

Step 2 In the Registry Editor, navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Daemon > RmeOrb**

Step 3 Change the value of *Args* from `-p 42342` to an unused port number, for example `-p 44444`.

Step 4 Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Daemon > RmeGatekeeper**

- Step 5** Change the value of Args from
-DNMSROOT=NMSROOT -DORBagentPort=42342 com.visigenic.vbroker.gatekeeper.GateKeeper -props NMSROOT\lib\visigenics\gatekeeper.cfg
 to
-DNMSROOT=NMSROOT -DORBagentPort=44444 com.visigenic.vbroker.gatekeeper.GateKeeper -props NMSROOT\lib\visigenics\gatekeeper.cfg
- Step 6** Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Environment**:
- Step 7** Change the value of OSAGENT_PORT and PX_OSA_PORT from 42342 to 44444.
- Step 8** Open the file *NMSROOT\lib\classpath\md.properties*, in any plain text editor, such as Notepad.
- Step 9** Change the value of OSAGENT_PORT and PX_OSA_PORT from 42342 to 44444.
- Step 10** Reboot the server.
NMSROOT is the installation directory for CiscoWorks Server.
-

Q. How do I change port for osagent in Solaris?

A. To do this:

-
- Step 1** Stop daemons.
- Step 2** Make sure that no CSCO processes are running.
- Step 3** Make sure all ports used by CiscoWorks are free.
 To do this, enter:

```
netstat -na | grep 423
netstat -na | grep 1741
```

 If these ports are free, you will not see any output.
- Step 4** Verify whether the port 44444 is free, using the following command:

```
netstat -na | grep 44444
```

 If the port is free, you will not see any output.
- Step 5** Back up *NMSROOT/objects/dmgt/dmgt.d.conf* file.
- Step 6** Edit the file **dmgt.d.conf** using a text editor.
- a. Change the line:
 RmeOrb y - *NMSROOT/lib/vbroker/bin/osagent* -p 42342 to RmeOrb y -
NMSROOT/lib/vbroker/bin/osagent -p **44444**
 - b. Change the port number for RmeGatekeeper from:
 RmeGatekeeper y RmeOrb *NMSROOT/lib/vbroker/bin/rungk.sh* 42342
 to
 RmeGatekeeper y RmeOrb *NMSROOT/lib/vbroker/bin/rungk.sh* **44444**
- Step 7** Open the file */etc/services* in a plain text editor such as vi.

Step 8 Comment out the entry for CSCOsa port and add the following entry:

```
cscosa 44444/udp # CSCO NM osagent
```



Note The change is for the port number only.

Step 9 Open /var/sadm/pkg/CSCOmd/pkginfo in a plain text editor, such as vi.

- Change the entry from
OSAGENT_PORT= 42342
to
OSAGENT_PORT=**44444**
- Change the entry from
PX_OSA_PORT=42342
to
PX_OSA_PORT=**44444**

Step 10 Restart the daemons. We recommend that you also reboot the server.

Q. How do I change the ESS port in Solaris?

A. There are 4 ports related to ESS:

- ESS Service Port: 42350/udp
- ESS listening port: 42351/tcp
- ESS HTTP Port: 42352/tcp
- ESS Routing Port: 42353/tcp

The ports mentioned above are default ports. The alternative ports defined for these in CiscoWorks are 44350, 44351, 44352, 44353 respectively.

To change the ports:

Step 1 Open the file *NMSROOT/objects/ess/conf/essproperties.conf* in a plain text editor, such as vi.

Step 2 Change the port numbers as required.

Step 3 Reboot the system.

Q. How do I change ESS port in Windows?

A. To do this:

Step 1 Back up your Windows registry.

Step 2 In the Registry Editor, navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco > Resource Manager > Current Version > Daemon > ESS**

Step 3 Change the value of Args from

```
-store NMSROOT\objects\ess\conf\rvrd.conf -logfile NMSROOT\log\ess.log -listen
42351 -no-http
```

to

```
-store NMSROOT\objects\ess\conf\rvrd.conf -logfile NMSROOT\log\ess.log -listen 42351
-no-http
```

Step 4 Change the corresponding entry in *NMSROOT\objects\ess\conf\essproperties.conf*.

Step 5 Reboot the server.

Q. I have configured the Active Directory Login Module but it does not work. How can I analyze the problem?

A. To analyze the problem, enable the Debug mode for the Active Directory Login module. To do this:

Step 1 Login as Admin.

Step 2 Go to **Server > Security > AAA Mode Setup**.

The Select Login Module dialog box appears.

Step 3 Select a login module from the Available Login Modules list box and Click on **Edit Options**.

The Login Module Options dialog box appears.

Step 4 Select the radio button **True** and click on **Finish**.

This enables the Debug option. Enabling debug mode allows the login module to add the detailed progress and failure information to log files. The log files are located at:

NMSROOT/MDC/Tomcatlogs/stdout.log

For all failed login attempts, the log files contain LDAP error messages, which specify the reason for the failure.

For example, if the Usersroot configuration is incorrect, then the login module cannot match the complete DN string with any entries in the Active Directory database.

It indicates which portion of the DN matched and which portion did not match. You can verify your Active Directory setup and the entries for the Usersroot.

In some cases, the log file contains error messages with NameError. This indicates that either you entered a wrong user Id or there is some spelling error in the Usersroot configuration.

Q. How do I change the IP Address of the CiscoWorks Server after installing it, or after running it for a while?

A. You can change the IP address on the server, and then access it using the new IP address.

To change the IP address on Windows:

Step 1 Click **Start > Settings > Network and Dial-up Connections > Local Area Connection**.

The Local Area Connection Status dialog box appears.

- Step 2** Click **Properties**.
The Local Area Connection Properties dialog box appears.
- Step 3** Select Internet Protocol (TCP/IP) and click **Properties**.
The Internet Protocol (TCP/IP) Properties dialog box appears.
- Step 4** Select the radio button **Use the following IP address**.
- Step 5** Change the IP address as required, in the IP Address field.
For the subnet mask and default gateway values, use the command `ipconfig` at the command prompt.
The subnet mask and default gateway values appear.
- Step 6** Enter these values in the subnet mask and default gateway fields.
- Step 7** Click **OK**.
- Step 8** Restart the server.
-

To change the IP address on Solaris, use the command `ifconfig` at the command prompt to change the IP address of the required interface.

For example, at the command prompt, you can enter:

```
ifconfig interfacename inet ipv4address
```

where the variable *interfacename* represents the name of the interface and *ipv4address* represents the new IP address.

- Q.** Do I need to change the CiscoWorks configuration after changing the IP address?
- A.** You do not need to change the CiscoWorks configuration whenever you change the IP address. CiscoWorks uses `hostname` for most of the communication. Only devices need to point to the new IP address. However, after changing the IP address, you must reboot the system on a Solaris server and restart the Daemon Manager on a Windows server. This is to make the changes effective.

- Q.** How do I change the Hostname of the CiscoWorks Server after installing it, or after running it for a while?
- A.** To change the hostname of the CiscoWorks Server, you need to update several files, and reboot the server:

Step 1 Change the hostname at **My Computer > Properties > Network Identification > Properties**.

Step 2 Change the hostname in all the following files:

Bundle	Solaris	Windows
LMS Bundle	<ul style="list-style-type: none"> • /etc/hosts. Modify loghost to the new hostname. • /etc/hostname.hme0 or the appropriate interface file. Modify the file to the new hostname. • /etc/nodename or the appropriate interface file. Modify nodename to the new hostname. <p>These files may require you to reboot the server.</p> <ul style="list-style-type: none"> • /opt/CSCOPx/lib/classpath/md.properties Change "PX_HOST" to the new hostname. • /var/sadm/pkg/CSCOMd/pkginfo Change "PX_HOST" to the new hostname. 	NMSROOT\lib\classpath h\md.properties file

For Solaris, the **sys-unconfig** command erases the hostname and IP addresses pertaining to the Solaris system (not the LMS or SMS software) and guides you through the server-renaming process.

You can also do this when you change the hostname in the hosts, hostname.hme0, and nodename files in the /etc directory.

Step 3 Change the hostname in following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet.
- HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Resource Manager.

You must look for all the instances of hostname under these registry entries, and replace them with the new hostname.

Step 4 Change the hostname in regdaemon.xml (*NMSROOT/MDC/etc/regdaemon.xml*).

Step 5 Change the hostname in web.xml (*NMSROOT/MDC/tomcat/webapps/classic/WEB-INF/web.xml*).

- Step 6** Create a file `NMSROOT/conf/cmhc/changehostname.info`, with the information on the updated hostname in the format:
- ```
OldhostName:NewhostName
```
- OldhostName*—Previous Hostname as registered with CCR(`regdaemon.xml`).
- NewhostName*—Current Hostname as registered with CCR(`regdaemon.xml`).
- The entries for hostname in `regdaemon.xml` and `changehostname.info` should be identical.
- Step 7** Delete `gatekeeper.ior` file:
- Windows—`NMSROOT\www\classpath`
- Solaris—`/opt/CSCOpX/www/classpath`
- Step 8** Some of the devices added before you change the hostname may not be properly classified in Device Center. To rectify this, run the following commands:
- For Windows:
- Enter `net stop crmdmgt` to stop daemon manager.
  - Enter `dbisqlc -c`

```
"uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dbf=NMSROOT\databases\cmf\cmf.db" -q
update PIDM_app_device_map SET app_hostname='NewhostName' where app_hostname='OldhostName'
```
- For Solaris:
- Enter `/etc/init.d/dmgt stop` to stop daemon manager.
- Enter `setenv LD_LIBRARY_PATH NMSROOT/objects/db/lib:NMSROOT/lib`
- Enter `dbisqlc -c`

```
"uid=cmfDBA;pwd=dbpassword;eng=cmfEng;dbf=NMSROOT/databases/cmf/cmf.db" -q
update PIDM_app_device_map SET app_hostname='\NewhostName\' where
app_hostname='\OldhostName\'
```
- `dbpassword` is CiscoWorks Common Services Database password.
- Step 9** Re-generate the Certificate. See [Creating Self Signed Certificates, page 4-7](#) for details. Enter the new hostname in the Hostname field.
- Step 10** Reboot the Machine.
- For RME on Solaris, you must change the hostname for CTMJrmServer daemon registration in the `/opt/CSCOpX/objects/dmgt/dmgt.conf` file, before rebooting the CiscoWorks server.
- See the Installation and Setup Guide for Resource Manager Essentials 4.0 on Solaris:
- [http://www.cisco.com/en/US/docs/net\\_mgmt/cisoworks\\_resource\\_manager\\_essentials/4.0.3/release/installation/solaris/guide/trbls.html](http://www.cisco.com/en/US/docs/net_mgmt/cisoworks_resource_manager_essentials/4.0.3/release/installation/solaris/guide/trbls.html)

When you change the hostname, ensure that you:

- Redo the integration, if you have integrated any third party network management application to CiscoWorks, using Integration Utility.
- Reimport the Certificates and redo the Multi Server setup if the machine is part of a Multi Server setup.

For example, if you are changing the hostname of a machine that is configured as a Slave, then it needs to reregister with the Master. If you are changing the hostname of a machine that is configured as a Master, then all its Slaves need to be updated with the new Master hostname.

- Add new hostname in ACS, if the AAA mode of the machine is set to ACS.

If the hostname of the machine changes, the stability of the system is not guaranteed and it fails in some cases.

See Release Notes for CiscoWorks Common Services for details.

---

**Q.** How do I find out which devices are supported by a particular application?

**A.** Select **Common Services > Software Center > Software Updates** Under Applications Installed, click the application name to see a list of the supported devices.

**Q.** How do I verify if SSH is enabled or disabled on my device using CiscoWorks Server?

**A.** To verify whether SSH is enabled or disabled using the CiscoWorks Server:

---

**Step 1** Log on to the CiscoWorks.

**Step 2** Select **Common Services > Device Center > Tools > Management Station to Device**.

**Step 3** Enter the device name in the Check Connectivity dialog box and select the SSH check box.

If SSH is enabled on the device, you will see:

SSH OK.

If SSH is not enabled on the device, you will see:

SSH failed.

---

**Q.** Is it possible to have both CiscoWorks and ACS on the same machine?

**A.** No. This is because ACS mandates CiscoWorks to be configured as an AAA client in it for CiscoWorks to avail AAA service. At the same time, ACS does not allow itself to be configured as an AAA client, which is required when ACS and CiscoWorks coexists. Hence the configuration required for ACS integration will fail.

**Q.** How do I change the casuser password in Windows?

**A.** You can change the casuser password using `resetCasuser.exe`. It can be executed only by an administrator or casuser. To change the casuser password:

---

**Step 1** Enter `NMSROOT\setup\support resetCasuser.exe` at the command prompt

You can:

1. Randomly generate the password
2. Enter the password
3. Exit.

**Step 2** Enter **2**, and press **Enter**.

It prompts you to enter the password.

**Step 3** Confirm the password.




---

**Note** You must know the password policy. If the password entered does not match the password policy, it exits.

---

**Q.** How do I change the CiscoWorks user password?

**A.** You can change the CiscoWorks user password using the CiscoWorks user password recovery utility.

To change the user password on Solaris:

---

**Step 1** Enter `/etc/init.d/dmgttd stop` to stop the Daemon Manager.

**Step 2** At the command prompt, enter `NMSROOT\bin resetpasswd username`

A message appears:

Enter new password for username:

**Step 3** Enter the new password.

**Step 4** Enter `/etc/init.d/dmgttd start` to start the Daemon Manager.

---

To change the user password on Windows:

---

**Step 1** Enter `net stop crmdmgttd` to stop the Daemon Manager.

**Step 2** At the command prompt, enter

`NMSROOT\bin resetpasswd username`

A message appears:

Enter new password for username:

**Step 3** Enter the new password.

Enter `net start crmdmgttd` to start the Daemon Manager.

---

**Q.** How do I enable/disable ACS Communication on HTTPS from CLI?

**A.** To enable/disable ACS communication on HTTPS:

---

**Step 1** Enter `NMSROOT/bin/perl NMSROOT/bin/camssl.pl`

The following message is displayed:

Usage: camssl.pl -enable | -disable

- To enable ACS communication on HTTPS:

Enter `NMSROOT/bin/perl NMSROOT/bin/camssl.pl -enable`

- To disable ACS communication on HTTPS:

Enter `NMSROOT/bin/perl NMSROOT/bin/camssl.pl -disable`

**Step 2** Restart the Daemon Manager:

On Windows:

Enter `net stop crmdmgtd`

Enter `net start crmdmgtd`

On Solaris:

Enter `/etc/init.d/dmgtd stop`

Enter `/etc/init.d/dmgtd start`

---

**Q.** How do I change web server port numbers?

**A.** To change the web server port numbers, you must execute separate commands for both Windows and Solaris.

**On Solaris:**

You can change the web server port numbers for the webservers. You can also change both the HTTP and HTTPS port numbers. To change the port numbers you must login as CiscoWorks Server administrator, and run the following command at the prompt:

`NMSROOT/MDC/Adobe/bin/changeport`

If you run this command without any command line parameter, CiscoWorks displays:

```
*** CiscoWorks Webserver port change utility ***
```

```
Usage: changeport <port number> [-s] [-f]
```

where

*port number*—The new port number that should be used

**-s**—Changes the SSL port instead of the default HTTP port

**-f**—Forces port change even if Daemon Manager detection FAILS.




---

**Note** Do not use this option by default. Use it only when CiscoWorks instructs you to.

---

For example, you can enter:

`changeport 1744`—Changes the CiscoWorks web server HTTP port to use 1744.

Or,

**changeport** *port number* **-s**—Changes the CiscoWorks web server HTTPS port to use the specified port number.

The restrictions that apply to the specified port number are:

- Port numbers less than 1025 are not allowed except 80 (HTTP) and 443 (HTTPS). Also port 80 is not allowed for SSL port and port 443 is not allowed for HTTP port.
- The specified port should not be used by any other service or daemon. The utility checks for active listening ports and ports listed in /etc/services. If any conflict is found it rejects the specified port.
- The port number must be a numeric value in the range 1026 – 65000. Values outside this range and non-numeric values are not allowed.
- If port 80 or 443 is specified for any of the webservers, that webserver process is started as root. This is because ports lower than 1026 are allowed to be used only by root in Solaris.

However, according to Apache behavior, only the main webserver process runs as root, and all the child processes will run as casuser:casusers. Only the child processes serve the external requests.

The main process which runs as root monitors the child processes. It does not accept any HTTP requests. Owing to this, Apache ensures that a root process is not exposed to the external world and thus ensures security.

- If you do not want CiscoWorks processes to run as root, do not use the ports 80 and 443.

When you execute the utility with the appropriate options, it displays messages on the tasks it performs.

This utility lists out all the files that are being updated. Before updating, the utility will back up all the affected files in /opt/CSCOpX/conf/backup and creates appropriate unique sub-directories.

It also creates a new file index.txt. This text file contains information about the changed port and a list of all the files that are backed up and their actual location in the CiscoWorks directory.

A sample backup may be similar to:

```

/opt
├── /CSCOPx
│ ├── /conf
│ │ └── /backup
│ │ ├── --README.txt (Note the purpose of this directory as it is initially empty)
│ │ └── --AAAtpaG03_Ciscobak (Autogenerated unique backup directory).
│ │ ├── --index.txt (The backup file list)
│ │ ├── --httpd.conf (Webserver config file)
│ │ ├── --md.properties (CiscoWorks config elements)
│ │ ├── --mdc_web.xml (Common Services application config file)
│ │ ├── --regdaemon.key (Common Services config registry key file)
│ │ ├── --regdaemon.xml (Common Services config registry data file)
│ │ ├── --rootapps.conf (CiscoWorks daemons using privileged ports)
│ │ ├── --services (The system /etc/services file)
│ │ ├── --ssl.properties (CiscoWorks config elements for SSL mode)
│ │ └── --vms_web.xml (Common Services application config file)

```



#### Note

All the above files and the unique directories are stored with read only permission to casuser:casusers. To ensure the security of the backup files, only the CiscoWorks Server administrator has write permissions.

The change port utility displays messages to the console during execution. These messages contain information about the directory where the backup files are being stored. These messages are also logged to a file, changeport.log

This file is saved to the directory:

```
/var/adm/CSCOPx/log/changeport.log
```

This file contains the date and time stamps to indicate when the log entries were created.

#### On Windows:

You can change the web server port numbers for the Common Services Webserver. You can also change both the HTTP and HTTPS port numbers.

To change the port numbers you must have administrative privileges. Run the following command at the prompt:

```
NMSROOT\MDC\Apache\changeport.exe
```

If you execute this utility without any command line parameter, CiscoWorks displays the following usage text:

```

*** Common Services Webserver port change utility ***
Usage: changeport <port number> [-s] [-f]

```

where:

- port number*—The new port number that should be used
- s**—Change the SSL port instead of the default HTTP port
- f**—Force port change even if Daemon Manager detection fails.



---

**Note** Do not use this option by default. Use it only when CiscoWorks instructs you to.

---

For example, you can enter:

**changeport 1744**—To change the CiscoWorks web server HTTP port to use 1744.

Or,

**changeport *port number* -s**—Changes the CiscoWorks web server HTTPS port to use the specified port number.



**Note**

---

If you change the port after installation, CiscoWorks will not launch from Start menu (**Start > Programs > CiscoWorks > CiscoWorks**). You have to manually invoke the browser and specify the URL, with the changed port number.

---

The restrictions that apply to the specified port number are:

- Port numbers less than 1025 are not allowed except 80 (HTTP) and 443 (HTTPS). Also port 80 is not allowed for HTTPS port and port 443 is not allowed for HTTP port.
- The specified port should not be used by any other service or daemon. The utility checks for active listening ports and if any conflict is found the utility rejects the specified port.

There is no reliable way to determine whether any other service or application is using a specified port. If the service or application is running and actively listening on a port, it can be easily detected.

However, if the service is currently stopped, the utility cannot determine what port it uses. This is because on Windows there is no common port registry equivalent to */etc/services* as in UNIX.

The port number must be a numeric value in the range 1026 – 65000. Values outside this range and non-numeric values are not allowed.

When you run the utility with the appropriate options, it displays messages on the actions it is performing.

It lists out all the files that are being updated. Before updating, the utility will back up all the affected files in *CSCOPx\conf\backup* and creates appropriate unique sub-directories.

It also creates a new file *index.txt*, which contains information about the changed port and a list of all the files that are backed up and their actual location in the CiscoWorks directory.

A sample backup may be similar to:

```
[drive:]
|--\Program Files
 |--\CSCOpX
 |--\conf
 |--\backup
 |--README.txt (Notes the purpose of this dir as it is initially empty)
 |--\skc03._Ciscobak (Autogenerated unique backup directory).
 |--index.txt (The backup file list)
 |--httpd.conf (Webserver config file)
 |--md.properties (CiscoWorks config elements)
 |--mdc_web.xml (Common Services application config file)
 |--regdaemon.key (Common Services config registry key file)
 |--regdaemon.xml (Common Services config registry data file)
 |--ssl.properties (CiscoWorks config elements for SSL mode)
 |--vms_web.xml (Common Services application config file)
```


**Note**

All the above files and the unique directories are stored with read only permissions. Only the administrator and casuser have write permissions, to ensure the security of the backup files.

The change port utility displays messages to the console during execution. These messages contain information about the directory where the backup files are being stored. These messages are also logged to a file, changeport.log.

This file is saved to the directory:

*NMSROOT*\log\changeport.log

This log file contains the date and time stamps to indicate when the log entries were created.

**Q.** Ho do I increase Tomcat heap size?

**A.** To increase Tomcat heap size:

**Step 1** Stop Daemon Manager.

- On Solaris:  
Run `/etc/init.d/dmgttd stop`
- On Windows:  
Run `net stop CRMdmgttd`

**Step 2** Run `NMSROOT/bin/perl NMSROOT/bin/ModifyTomcatHeap.pl max heap in MB`

**Step 3** Start Daemon Manager.

- On Solaris:  
Run `/etc/init.d/dmgttd stop`

- On Windows:

Run `net start CRMdmgtd`

---

If Tomcat is already configured for higher memory than what you specify when you run the command, it displays message stating this, and exits.

**Q.** How do I enable debugging in MICE?

**A.** To enable debugging in MICE:

---

**Step 1** Go to `NMSROOT/MDC/tomcat/webapps/classic/WEB-INF/web.xml`.

You have to edit the following section of the file:

```
<context-param>
<param-name>DEBUG</param-name>
<param-value>>false</param-value>
<description>mice debug enabling</description>
</context-param>
```

**Step 2** Change `<param-value>false</param-value>` to

```
<param-value>>true</param-value>
```

---

**Q.** What does cmf stand for?

**A.** The cmf acronym stands for Common Management Foundation. This phrase describes the set of management services provided by the CiscoWorks Server. cmf is synonymous with Common Services.

**Q.** Why does the Apache process not come up after installation or why does the process go down suddenly?

**A.** The reason could be a problem with the Apache configuration syntax or the validity of the server certificate. You should first check the Apache configuration syntax.

To do this:

On Windows:

Go to `NMSROOT\MDC\Apache` and run the command `Apache.exe -t -d .`

---



**Note**

Do not omit the `.`

---

On Solaris:

Go to `NMSROOT/MDC/Apache/bin` and run the command `./web_server -t`

If the Apache configuration syntax is fine, you will see the message

```
Syntax OK
```

If the Apache configuration syntax is fine, check the validity of the Server Certificate using the SSL Utility Script.

To do this:

---

**Step 1** Navigate to the directory where the SSL Utility Script is located.

On Windows:

- a. Go to *NMSROOT\MDC\Apache*
- b. Enter *NMSROOT\bin\perl SSLUtil.pl*

On Solaris:

- a. Go to *NMSROOT/MDC/Apache/bin*
- b. Enter *NMSROOT/bin/perl SSLUtil.pl*

After you have entered this command, the system displays a set of options.

**Step 2** Select the fourth option Verify the input Certificate/Certificate Chain by entering 4.

**Step 3** Enter the location of the server certificate *NMSROOT/MDC/Apache/conf/ssl/server.crt*

The script verifies if the server certificate is valid. If the script reports errors during validation and verification, you have to regenerate the certificate by running *signTool.pl* from the above directory.

**Step 4** Enter *NMSROOT/bin/perl signTool.pl [-SSL=true | -SSL=false]*



**Note**

---

*NMSROOT* is the directory where CiscoWorks is installed.

---

**Q.** Why task-2-role mapping is not synchronized between the ACS server and the CiscoWorks server, sometimes?

**A.** CAM provides user cache. This cache is not per session, and may become stable when User privileges changes on the ACS server. The user should explicitly logout from the browser session, when the privileges changes.

If the browser window is closed without logging out properly, the user cache may not be cleared and the task-2-role mapping may not be synchronized between the ACS server and the CiscoWorks server .

**Q.** What does a diskWatcher process do?

**A.** The diskWatcher process monitors disk space availability on the CiscoWorks server.

This process calculates the disk space information of a drive (in Windows machine) or a file system (in Solaris machine) at regular intervals and stores them in *diskwatcher.log* file.

Disk spaces are calculated at an interval of approximately one hour in both Windows and Solaris machines.

In Solaris machine, the disk spaces are calculated for */var*, */tmp* and */opt* file systems. Disk spaces of */opt* file system is calculated in the first 30 minutes of every one hour time interval. The disk spaces of */var* file system and */tmp* file system are calculated in the next 15 minutes and the last 15 minutes of an approximate one hour time interval.

This process also alerts the users by displaying a popup window when the disk space is less than the threshold limit (10% approximately), and records the alert information in the system log files.

The popup message details are recorded in *diskwatcher.log* and *syslog.log* files in Windows machines. They are stored in *diskwatcher.log* and *daemons.log* files in Solaris machines.

- Q.** How do I avoid the SSL port conflict between HPOV and Common Services servers and run them both on the same system?
- A.** If you are using HPOV as your third party NMS application, you would require the IIS service be enabled for HPOV to install and run. The IIS webserver runs on SSL port 443, which is the default port for LMS webserver. Since LMS web server and IIS web server conflicting on SSL port 443, bCiscoverks Common Services can not run on a machine, where IIS is installed and enabled.

To avoid the conflict between both the webservers:

- a. Disable the IIS services.
- b. Install the Ciscoworks applications with IIS Services disabled.
- c. After the installation is complete, change the SSL port number of LMS webserver from 443 to some other available port number.
- d. Enable the IIS services to install HPOV or access HPOV from web interface

# Troubleshooting Suggestions

Use the suggestions in [Table 10-4](#) to resolve errors or other problems with the CiscoWorks Server.

**Table 10-4** Troubleshooting Suggestions

Symptom	Probable Cause	Possible Solutions
Authorization required. Please log in with your username and password.	Incompatible browser causing cookie failure (unable to retrieve cookie).	Verify that you have <b>Accept all cookies</b> enabled. Refer to the installation documentation for supported Internet Explorer and Netscape Navigator software and setup procedures.
Daemon Manager could not start. The port is in use.	The operating system has not yet reallocated the port.	Make sure all CiscoWorks processes are terminated ( <code>/usr/ucb/ps -auxww   grep CSCO</code> ). Wait five to ten minutes, then try to restart the Daemon Manager.
User has forgotten his password.	Common Services cannot recover forgotten passwords.	A system administrator-level user must either change the password or delete and then add the user again.
You are logged out of the CiscoWorks Server.	Changes in the login module configuration file might not be correct.  Authentication server might be down and there were no fallback logins set.	<ol style="list-style-type: none"> <li>Log on as root.</li> <li>On Windows: Run <code>NMSROOT/bin/ResetLoginModule.pl</code> On Solaris: Run <code>opt/CSCOpX/bin/ResetLoginModule.pl</code></li> <li>Restart Daemon Manager.</li> </ol>
The Log File Status window displays files that exceed their limit.	Files need to be backed up so that file size will be reset to zero.	<ol style="list-style-type: none"> <li>Stop all processes.</li> <li>Enter the log file maintenance command: <ol style="list-style-type: none"> <li>On UNIX: <code>NMSROOT/cgi-bin/admin/</code></li> <li>On Windows: <code>NMSROOT\cgi-bin\admin\</code></li> </ol> </li> <li>Restart all processes.</li> </ol>
Error message in the logfile: Connection Refused. Check the Device is SSH supported or not.	Device is not SSH enabled or the server is not authorized to initiate SSH connection.	<ol style="list-style-type: none"> <li>Check whether the device is up or not.</li> <li>Try connecting to the device with a commercial SSH client. If you are able to connect, go to step 3. If you are not able to connect, check whether the device is running SSH enabled (K2 or K9) image. <ul style="list-style-type: none"> <li>If it is not the correct image, download the appropriate image to the device.</li> <li>If you have the correct image, then see whether you have created RSA key pairs in the device. Creating RSA keys will enable SSH in the device.</li> </ul> </li> <li>Check whether your server or network is authorized to initiate SSH connections to device.</li> </ol>

**Table 10-4** Troubleshooting Suggestions (continued)

Symptom	Probable Cause	Possible Solutions
<p>After installation, while starting the daemon manager, the following error message is displayed:</p> <pre>Found Non-SSL compliant Applications. Please disable SSL and then start the Daemon Manager</pre> <p>(Solaris only)</p>	<p>Found Non-SSL compliant products that do not function in SSL enabled mode.</p>	<p>Disable SSL from CLI and then start the daemon manager.</p>
<p>After installation, while starting the daemon manager, the following error message is displayed:</p> <pre>Service Not responded in a timely fashion</pre>	<p>Found Non-SSL compliant products that do not function in SSL enabled mode.</p>	<p>Disable SSL from CLI and then start the daemon manager.</p>

