



# Interacting with the CiscoWorks Desktop

---

The CiscoWorks desktop is the interface for the CiscoWorks network management applications. The desktop is a graphical user interface (GUI) that runs on a web browser. The CiscoWorks desktop provides a set of features to help you interact with the application effectively:

- [Invoking the CiscoWorks Desktop](#)
  - [Logging In](#)
  - [Using the Desktop](#)
  - [Creating Shortcuts](#)
  - [Using Online Help](#)
  - [Changing the Web Server Port Numbers](#)



## Note

When you invoke the CiscoWorks network management application, CiscoWorks checks whether the required Java Plug-in (Java Plug-in version 1.3.1) is present on the client system. If you do not have the plug-in installed, CiscoWorks prompts you to install the plug-in. For more information, see the [“Installing the Java Plug-in”](#) section on page 3-7.

---

# Invoking the CiscoWorks Desktop

The current version of CiscoWorks uses the Java Secure Socket Extension (JSSE) 1.0.2 with the Java Plug-in 1.3.1 in SSL enabled mode. Java Plug-in is optional. This is required only for applications like CiscoView and Resource Manager Essentials (Essentials).

CiscoWorks requires JSSE 1.0.2 to be installed as a Java Plug-in add-on on the client system. This helps CiscoWorks to invoke SSL Initializer (a plug-in-enabled applet). The SSL Initializer detects whether the server is in:

Normal mode (Hypertext Transfer Protocol—HTTP)

Secure mode (Hypertext Transfer Protocol Secure—HTTPS).

## Invoking CiscoWorks Desktop in Normal Mode (HTTP)

**http://***server\_name* *port\_number*

*server name*

*port number*




---

`http://server_name:port_number/login.html`

*Also do not*

---

In normal mode (HTTP), the default TCP port for CiscoWorks Server is 1741.

On Windows, the CiscoWorks Server always uses the default port numbers in secure and normal modes.

On Solaris, if the default TCP ports (1741 and 1742) are used by other applications, you can select a different port each for secure and normal modes during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*

CiscoWorks displays the Login Manager. You can proceed by logging into CiscoWorks. For more information, see [“Logging In” section on page 2-6](#).

# Invoking CiscoWorks Desktop in SSL Enabled Mode (HTTPS)

## Step 1

https:// \_\_\_\_\_ :



---

---

a. OK

b. Yes

**Step 2**

**Finish**



**Step 3**

**Continue**

**Step 4**

- **Grant This Session**

**Deny**

**Grant always**

**More Info**

---

Downloads and installs the JSSE jar files on your system

Updates the java.policy file on your system

Prompts you to close the browser and restart the browser and CiscoWorks session.

**Step 5**



**Note**

---

---

**Step 6**

- 
- 
- 

**Grant Always**

---

# Logging In

Step 1

admin



Connect

Enter

Security > Modify My Profile

Server Configuration > Setup >

# Using the Desktop

## Buttons

- 
-

**Table 2-1 Common Navigation Tree Items**

<b>Drawer</b>	<b>Description</b>
VPN/Security Management Solution	Includes applications and tools for configuration management and administration services for MCs. <b>Note</b> This drawer is available only if Management Center (MC) applications are installed on the CiscoWorks Server.
Management Connection	Includes applications for adding external links to CiscoWorks, and a collection of links to commonly used tools on Cisco.com
Device Manager	Includes applications used for device management, such as CiscoView <b>Note</b> This drawer is available only when CiscoWorks Common Services 2.2 (including CiscoView) is installed.

## Message Window

Contents **Server Configuration > Desktop > Editing the Message Window**

## Applications Window

; other applications might display this information in a separate browser window.

## Creating Shortcuts

**Home > My Shortcuts**

# Using Online Help

- 
- 
- 
- 



Note

---

---

- 
- 

# Changing the Web Server Port Numbers

On Solaris:

```
/opt/CSCOpX/objects/web/bin/changeport
```

```
*** CiscoWorks Webserver port change utility ***
Usage: changeport <port number> [-s] [-f] [-c]
```

- <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.




---

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

---

- c—Change SSL or http ports for Common Services Web Server instead of the default CiscoWorks Web Server. This option can be used in combination with the -s and -f options.

For example, you can enter:

```
changeport 1744
```

```
changeport 1755 -s -c
```

to use 1755.

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, then that webserver process will be started as root. This is because ports lower than 1026 are allowed to be used only by root in Solaris.

However, as per 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 and do 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, then do not use the ports 80 and 443. You can use 1755 instead.

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 one 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 look like the following:

```
|
|--/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)



---

---

**`/var/adm/CSCOpX/log/changeport.log`**

**On Windows:**



**Note**

---

---

- 

- 



---

**Note**

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 execute 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 one 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 look like the following:

```
`--\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)
```



**NMSROOT\log\changeport.log**