



Interacting With CiscoWorks Homepage

CiscoWorks Homepage (CWHP) provides launch points for all Common Services features such as Home, Server, Software Center, Device and Credentials, and Groups.

CWHP also provides launch points for applications installed on the same server or a remote server, and their major functions and for other web-based products (Non-CiscoWorks products and third party/home-grown tools) residing on the same or on a different server.

CWHP has the look and feel of a portal. After you install the applications, you can see the application panels on CWHP.

CWHP supports application oriented and device oriented navigation paradigms. When you select any of the application functions on CWHP, it launches the application homepage, and the selected function is launched in application homepage content area.

CWHP is completely based on HTML, and provides intuitive navigation for you to move back-and-forth between CiscoWorks Homepage, and all other application homepages.

This chapter contains the following sections:

- [Invoking CiscoWorks Homepage](#)
- [Logging Into CiscoWorks](#)
- [Using CWHP](#)
- [Using Online Help](#)
- [Changing Web Server Port Numbers](#)

Invoking CiscoWorks Homepage

You may invoke CWHP by either:

- [Invoking CWHP in Normal Mode \(HTTP\)](#)

or

- [Invoking CWHP in SSL Enabled Mode \(HTTPS\)](#)

Invoking CWHP in Normal Mode (HTTP)

To invoke CWHP in the normal mode (HTTP), enter the URL for your CiscoWorks Server in your web browser:

```
http://server_name:port_number
```

where *server name* is the name of the CiscoWorks Server and *port number* is the TCP port used by the CiscoWorks Server, in the normal mode.

If you enter, `http://server_name:port_number/login.html` in your browser, the CiscoWorks Server will not launch. Also, do not bookmark the URL with the `login.html`.

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 443) are used by other applications, you can select different ports for secure and normal modes during CiscoWorks Server installation.

For more information, see the [Logging Into CiscoWorks](#) section, and also *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 on Solaris*.

Invoking CWHP in SSL Enabled Mode (HTTPS)

To invoke CWHP in the SSL enabled mode (HTTPS):

Step 1 Enter the URL for your CiscoWorks Server in your browser.

```
https://server_name:port_number
```

where *server name* is the name of the CiscoWorks Server and *port number* is the TCP port used by the CiscoWorks Server, when SSL is enabled (secure mode).

If you enter, `https://servername:portnumber/login.html` in your web browser, the CiscoWorks Server will not launch. Also, *do not* bookmark the URL with the `login.html`.

When SSL is enabled (HTTPS), the default TCP port for CiscoWorks Server is 443.

- On Windows, CiscoWorks Server always uses the default port numbers in secure and normal modes.
- On Solaris, if the default TCP ports (1741 and 443) are used by other applications, you can select different ports for secure and normal modes during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services 3.0.5 on Solaris*.

If you use Microsoft Internet Explorer to invoke CWHP, the browser displays a Security Alert window, indicating that you are about to view web pages over a secure connection.

- a. Click **OK** in the Security Alert window.

The Security Alert window displays the security certificate alert.

- b. Click **Yes** in the Security Alert window.

If you use Netscape Navigator to invoke CWHP, the browser displays the New Site Certificate wizard.

In the New Site Certificate wizard, you can accept the certificate for the current session or accept it till the certificate expires. To avoid going through the New Site Certificate wizard every time you invoke CWHP, you may accept the certificate till it expires.

If Common Services is running in a Plug-in environment, it displays Plug-in alert dialogs. (For example, Server Certificate details, Hostname Mismatch details).

- Step 2** Click **Yes** in the Plug-in alert dialogs to get to the Login panel.

If the server is in SSL mode and if you invoke Common Services as `http://server_name:1741`, you will be redirected to `https://server_name:443`

Logging Into CiscoWorks

If you have installed CiscoWorks Server and logging in for the first time, use the reserved *admin* user name and password.

To log in:

-
- Step 1** Enter **admin** in the User ID field, and the password for admin in the Password field of the Login Page. The CiscoWorks Server administrator can set the passwords to admin and guest users during installation. Contact the CiscoWorks Server administrator if you do not know the password.
- Step 2** Click **Login** or press **Enter**.
You are now logged into CiscoWorks Server.
- Step 3** You can change the admin password at **Common Services > Server > Security > User Management**
For more information, see Online Help.
-

Login sessions time out after two hours of inactivity. If the session is not used for two hours, you will be prompted to login again.

If you try to do any task after timeout, a message appears informing you that your session has timed out.

The Login screen replaces the current page of the current browser window. After you log in, the page you were on before re-logging in, appears.

Using CWHP

CiscoWorks Homepage is the primary user interface and the launch point for all features. After you log in to CiscoWorks, the default CiscoWorks Homepage appears.

The CWHP window consists of:

- [Common Services Panel](#)
- [Application Panels](#)
- [Device Troubleshooting Panel](#)
- [LMS Setup Center Panel](#)
- [Resources Panel](#)
- [CiscoWorks Product Updates Panel](#)
- [Tool Bar Items](#)

Common Services 3.0.5 and CiscoWorks applications use popup dialog boxes at many places.

**Note**

If you have a popup-blocker enabled in your browser, none of these popups appear. Therefore, you have to disable the popup-blocker, if you have enabled any.

Common Services Panel

The Common Services Panel displays all Common Services functions. The Common Services panel appears in a tree window.

First level items displayed in the tree window are:

- Home
- Server
- Software Center
- Device and Credentials
- Groups

**Note**

The HomePage item, which was the first level item in the tree window of Common Services Panel, is now renamed as HomePage Admin and moved as a sub item under Server item.

Application Panels

Each Application Panel in the CWHP serves as a top-level launch point for all Common Services applications installed on local or remote server.

All the applications installed appear in the CWHP in three columns.

By default, only the first level items are displayed when you login. These first level items are in collapsed mode. Lower level navigations are displayed only if you manually expand a first level item.

The title of each application panel displays the application name and it serves as a link to the relevant application homepage. Application tasks are displayed in a hierarchical manner. When you select a task from the hierarchy, it launches the application homepage in a new window.

If the corresponding application homepage already exists for some other task, the window for this task is focussed, instead of creating a new window.

To launch the URL associated with the item in the popup window, click on the label.

Supporting Applications on Another Server

CiscoWorks applications from other servers can be made to display in the same way as CiscoWorks applications from the local server.

To do this, you should import registration details of CiscoWorks applications installed on other servers. This allows you to navigate various CiscoWorks applications from same or different bundles (such as LMS), from a single homepage.

You should authenticate yourself before using applications from other server (once for each server, for each session), even if you are authenticated on the local server.

Common Services will not do the license check. Applications need to authenticate and do the license check.

For details on transparently navigating through multiple CiscoWorks Servers, see [Enabling Single Sign-On](#).

Device Troubleshooting Panel

The Device Troubleshooting panel provides a launch point to the Device Center.

For more information, see [Chapter 8, “Using Device Center”](#).

LMS Setup Center Panel

The LMS Setup Center panel provides a launch point to LMS Setup Center where you can configure the system settings for all applications in one stop. The LMS Setup Center is part of LAN Management Solution Bundle.

For more information, see [Chapter 7, “Using LMS Setup Center”](#).

Resources Panel

The Resources panel is at the top right side of the CWHP. It also serves as a top-level launch point for CiscoWorks resources, Cisco.com resources, third party application links, and web based custom tool links. This panel shows the types of resources as first level and details in the next level.



Note

CWHP provides an Admin UI to turn off this information if you are behind the firewall, or if you do not want this information to be displayed in CWHP.

CiscoWorks Product Updates Panel

The Product Updates panel is at the right side of the page. It displays informative messages about CiscoWorks product announcements, and help related topics.

If you click the More Updates link, a popup window appears with all the Cisco Product Update details.

In case the CiscoWorks server is behind a firewall, the proxy settings are used to download messages from Cisco.com. CWHP provides an Admin UI to accept the proxy settings. CWHP alerts you if any urgent messages are found.

By default, the polling interval is one minute. You can change this polling interval.

Tool Bar Items

The Tool bar buttons are at the top right side of the CWHP. The buttons are:

- Logout—Returns the browser to the Login dialog box.
- Help—Displays the Online help in a separate browser window. See [Using Online Help](#) for more information.
- About—Displays the general information about the software. The window displays license information, version and patch level, installation date and copyright information.

Using Online Help

Each CiscoWorks application includes Online help that provides procedural and conceptual information. Online help also contains:

- A search engine—Allows you to search the topics in Help, based on keywords.
- An index—Contains typical network tasks.
- A glossary.

To access Online help, click the **Help** button on the top-right corner. This opens a window that displays help contents. From this window, you can access help for all the installed CiscoWorks applications.

Changing Web Server Port Numbers

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

This section contains the following:

- [Changing Web Server Port Numbers on Solaris](#)
- [Changing Web Server Port Number on Windows](#)

Changing Web Server Port Numbers on Solaris

You can change the web server port numbers (for HTTP and HTTPS) for CiscoWorks webservers.

To change the port numbers you must login as CiscoWorks Server administrator, and run the following command at the prompt:

```
/opt/CSCOpX/MDC/Apache/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 use.

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.
```

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 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 there is any conflict, 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 run as root, and all the child processes 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 called `index.txt`. This text file contains information about the changed port, 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, as it runs. 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.

Changing Web Server Port Number on Windows

You can change the web server port numbers (for HTTP and HTTPS) for the CiscoWorks Webserver.

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

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

If you run 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 use.

For example, you can enter:

- **changeport 1744**—Changes the Common Services web server HTTP port to use 1744.

Or

- **changeport *port number* -s**—Changes the Common Services 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 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, there is no way that the utility can 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 backs up all the affected files in *CSCOpX\conf\backup*, and creates, appropriate, unique, sub-directories.

It also creates a new file called *index.txt*. This text file contains information about the changed port, 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 on the console, as it runs. 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.

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, Ciscoworks Common Services can not run on a machine, where IIS is installed and enabled.

To avoid the conflict between IIS and LMS webservers:

-
- Step 1** Disable the IIS services.
 - Step 2** Install the Ciscoworks applications with IIS services disabled.
 - Step 3** After the installation is complete, change the SSL port number of LMS webserver from 443 to some other available port number.
 - Step 4** Enable the IIS services to install HPOV or access HPOV from web interface
-