



Interacting With CiscoWorks Homepage

CiscoWorks Homepage (CWHP) provides launch points for all Common Services features. It also provides launch points for applications installed on the same server or a remote server, and their major functions.

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

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.

CWHP has the look and feel of a portal. By default, CWHP provides launch points for:

- Server
- HomePage
- Device and Credentials
- Groups

- Software Center
- Device Center

The following sections explain the CWHP features, in detail:

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

Invoking CiscoWorks Homepage

You may invoke CWHP in the normal mode (HTTP), or secure 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 on page 2-4. See also, *Installation and Setup Guide for CiscoWorks Common Services 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.

`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, when SSL is enabled (secure mode).

If you enter, `http://server_name:port_number/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 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.

Session timeout is not automatic. 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](#)
- [Resources Panel](#)
- [CiscoWorks Product Updates Panel](#)
- [Tool Bar Items](#)

Common Services 3.0 and CiscoWorks applications use popup dialog boxes at many places.

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

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

Application Panels

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

Applications 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.

For 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, RWAN, VMS), 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” section on page 3-23](#).

Supporting Traditional Applications With New Navigation

CWHP also displays the applications that are based on the traditional CiscoWorks Common Services desktop.

CWHP provides a Product Home Page, which looks similar to the traditional CiscoWorks Common Services desktop. Traditional applications are registered during installation to display their links on CWHP.

Device Troubleshooting Panel

The Device Troubleshooting panel provides a launch point to the Device Center. See [Chapter 6, “Using Device Center”](#) for details.

Resources Panel

Resources panel is on the top of the right hand 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

CiscoWorks Product Updates panel is on the right hand 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

Three buttons are available on top of the right hand side of the CWHP:

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

Configuring CWHP

The Application Registration, Link Registration, and Settings links under Homepage help you configure your CiscoWorks Homepage. They help you in:

- [Registering Applications With CWHP](#)
- [Registering Links With CWHP](#)
- [Setting Up CiscoWorks Homepage](#)

Registering Applications With CWHP

Using this feature you can register CiscoWorks applications on local or remote servers. You need to enter application instance attributes (host, port, and protocol).

Other information such as AppName, URLs available are already defined by the application in a template.

During registration you are prompted to select an application template and then register with CiscoWorks Server. The registration enables the application to be integrated with other applications based on the template definition. It also helps application launch points to be displayed on CWHP.

To register applications:

-
- Step 1** Select **Common Services > HomePage > Application Registrations**.
The Application Registration Status page appears.
- Step 2** View the list of registered applications in the Registered Applications dialog box.
-

Registering a New Application

To register a new application:

-
- Step 1** Click **Registration** in the Registered Applications dialog box.
The Choose Location for Registration page appears. A wizard guides you through the process.
- Step 2** Choose the location for registration.
You can choose to **Register from Templates** or **Import from Other servers**.
-

To register from Templates:

-
- Step 1** Select the Register from Templates radio button and click **Next**.
The Registration Through Template page appears. A list of templates appears in the Select a Template to Register dialog box.
- Step 2** Select the radio button corresponding to the Template you require and click **Next**.
The Server Attributes page appears.

- Step 3** Enter the Server attributes in the Server attributes dialog box and click **Next**.
The Registration Summary page displays the Application Registration summary window. It displays a summary the information you entered.
- Step 4** Click **Finish**.
-

Importing from other servers

You must perform the following tasks before importing application registrations from other servers. This is to ensure a secure environment for importing registrations.

- Create self signed certificates for the local and remote servers (if not already done).
- Add remote server's certificate to the local server. See [Setting up Peer Server Certificate](#) for details.
- Restart the local server.
- Create a Peer Server user on the remote server. Configure this user a System Identity user in the local server. See [Setting up Peer Server Account](#) and [Setting up System Identity Account](#) for details.

To import from other servers:

-
- Step 1** Select the Import from Servers radio button and click **Next**.
The Import Registrations page appears.
- Step 2** Enter the Server Name, Server Display Name, and the secure Port Number in the Import Server's Attributes dialog box.
- Step 3** Click **Next**.
The Import Registrations Summary window displays a summary of the information you entered.
- Step 4** Click **Finish**.
-

Unregistering an Application

To unregister an application:

-
- Step 1** Select **Common Services > HomePage > Application Registrations**.
The Application Registration Status page appears. You can view the list of registered applications in the Registered Applications dialog box.
- Step 2** Select the radio button corresponding to the Application you want to unregister, and click **Unregister**.
The Applications to be Unregistered window appears with the details of the Application unregistered.
- Step 3** Click **Confirm**.
-

Registering Links With CWHP

You can add additional links to CiscoWorks Homepage for Custom tools and home grown tools, and third party applications such as HPOV. The links appear under the Third Party or Custom Tools, as you specify.

To register links with CiscoWorks Homepage:

-
- Step 1** Select **Common Services > HomePage > Links Registration**.
The Links Registration Status page appears.
- Step 2** Click **Registration**.
The Enter Link Attributes dialog box appears.
- Step 3** Enter the Link Name and the URL.
Select the radio button corresponding to Third Party or Custom Tools to set the display location.
- Step 4** Click **OK**.
-

Unregistering a Link

To unregister a link:

-
- Step 1** Select **Common Services > HomePage > Links Registration**.
The Links Registration Status page appears.
 - Step 2** Select the check box corresponding to the link you need to unregister.
 - Step 3** Click **Unregister**.
-

Setting Up CiscoWorks Homepage

You can configure or change the CiscoWorks Homepage settings.

To modify CiscoWorks Homepage settings:

-
- Step 1** Select **Common Services > HomePage > Settings**.
The Homepage Settings page displays the Homepage Settings dialog box.
 - Step 2** Enter a name for the CiscoWorks Server in the Change Homepage Server Name field.
You can use this name in the Provider Group name in the Common Services Groups UI. See [“System-defined and User-defined Groups”](#) section on page 5-3 for details on Provider Group.
 - Step 3** Select the Hide External Resources check box to hide the Resources and CiscoWorks Product Updates panels in the Homepage.
 - Step 4** Enter the display name you want for Third Party tools in the Custom Name for Third Party field.
 - Step 5** Enter the display name you want for Custom tools/homegrown tools in the Custom Name for Custom Tools field.

Step 6 Select a value from the Urgent Messages Polling Interval drop-down list to set the polling interval for messages.

The time you set here decides the polling interval for disk watcher messages and messages you want to broadcast using the Notify Users features.

To disable this feature, select **DISABLE** from the drop-down list.

Disk watcher is a utility that monitors the file system. If the file system size goes above 90 percent, it displays an alert to logged in CiscoWorks users. You can use this to monitor critical file systems.

To know more about the Notify Users feature, see [“Messaging Online Users” section on page 3-80](#).

Step 7 Click **Update**.

You can update any one of the above settings by clicking update.

If you have changed the Homepage Server Name, a popup window appears prompting you to confirm whether you want to use this name in Provider Group name.

- Click **OK** if you want the name to be suffixed to the Provider Group name.
 - You need to restart Daemon Manager for the Provider Group name change to take effect. See [“Using Daemon Manager” section on page 3-60](#) for details on restarting Daemon Manager.
-

Using Online Help

Each CiscoWorks application includes online help that provides procedural and conceptual information to assist you in using CiscoWorks.

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 CiscoWorks applications installed.

Changing Web Server Port Numbers

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 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 web servers, 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 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.

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:

```
CSCOpX\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 `CSCOp\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.

