



## Preparing to Use CiscoWorks Common Services

---

After installing Common Services, you must configure the server and client systems.

This chapter consists of:

- [Configuring Client Systems, page 3-2](#)
- [Accessing CiscoWorks Server, page 3-5](#)
- [Using Device Center, page 3-5](#)
- [Using Device and Credentials Repository, page 3-5](#)
- [Using Integration Utility, page 3-6](#)
- [Using CiscoView, page 3-6](#)
- [Casuser Permissions, page 3-6](#)

# Configuring Client Systems

Through the following tasks, you can configure your client system to use Common Services.

- [Setting Display Fonts, page 3-2](#)
- [Configuring Web Browser, page 3-2](#)

The system that has Common Services installed on it can be used as both the server and the client. If you are using the system as client, you must configure the web browser.

## Setting Display Fonts

For Windows, set the display to use small fonts:

- 
- Step 1** Select **Start > Settings > Control Panel**.
- The Control Panel window appears.
- Step 2** Double-click the Display icon.
- The Display Properties dialog box appears.
- Step 3** Click **Settings**, then select **Advanced**.
- If you select **Small Fonts** in the Font Size list, your display font is set correctly.
  - If you do not select **Small Fonts**, select it from the Font Size drop-down list, then click **OK**.
- The System Settings Change dialog box appears.
- Step 4** If you changed the font size, click **Yes** to restart your system.
- 

## Configuring Web Browser

To configure your web browser:

- 
- Step 1** Enable Java and JavaScript:
- In Netscape Navigator:
- Select **Edit > Preferences > Advanced**.
  - Select the Enable Java check box and click **OK**.
- In Internet Explorer:
- Select **Tools > Internet Options > Advanced**.
  - Under the Microsoft VM heading, select **Java console enabled, JIT compiler for virtual machine enabled, and Java logging enabled** and click **OK**.
- In Mozilla:
- Select **Edit > Preferences > Advanced**.
  - Under **Enable features that help interpret web pages**, select **Enable Java**.

**Step 2** Set your browser cache to at least 6 MB:

In Netscape Navigator:

- a. Select **Edit > Preferences > Advanced > Cache**.
- b. Set the cache to 6 MB and click **OK**.

In Internet Explorer:

- a. Select **Tools > Internet Options > General**, then click **Settings**.
- b. Set the cache to at least 6 MB using the **Amount of disk space to use** slide bar.
- c. Click **OK** to close the Settings dialog box and return to the Internet Options dialog box and click **OK** again.

In Mozilla:

- a. Select **Edit > Preferences > Advanced > Cache**.
- b. Under **Cache Options**, set the cache to 6 MB.

**Step 3** Configure your browser to accept all cookies:

In Netscape Navigator:

- a. Select **Edit > Preferences > Privacy & Security**.
- b. Select the Enable all cookies radio button and click **OK**.

In Internet Explorer:

- a. Select **Tools > Internet Options > Privacy**.
- b. Scroll the settings bar down to select **Accept all Cookies** and Click **OK**.

In Mozilla:

- a. Select **Edit > Preferences > Privacy & Security > Cookies**.
- b. Under **Cookies**, select Enable all cookies radio button.
- c. Click **OK** to save your preferences.

**Step 4** Configure your browser to compare each page with its cached version every time it loads a page:

In Netscape Navigator:

- a. Select **Edit > Preferences > Advanced > Cache**.
- b. Select the Every time I view the page radio button and click **OK**.

In Internet Explorer:

- a. Select **Tools > Internet Options > General** and click **Settings** under Temporary Internet files group.
- b. Select the Every visit to the page radio button and click **OK** twice.

In Mozilla:

- a. Select **Edit > Preferences > Advanced**.
- b. Select the Every time I view the page radio button and click **OK**.

You must set this option to prevent Internet Explorer from using the cached information for help links. If you do not set it, the first help link is displayed properly. However, the second time you click a link, the first page is displayed again.

In Mozilla:

- a. Select **Edit > Preferences > Advanced > Cache**.
- b. Select the Every time I view the page radio button and click **OK**.

**Step 5** Change the default timeout to 20 minute.

This is only for Internet Explorer —See the instructions on the Microsoft Support Web site.

**Step 6** Enable style sheets:

In Netscape Navigator:

- a. Select **Edit > Preferences > Composer**.
- b. Select the Use CSS styles instead of HTML elements and attributes check box and click **OK**.

In Internet Explorer:

- a. Select **Tools > Internet Options > General**, then click **Accessibility**.
- b. Make sure that the **Format documents using my style sheet** check box is not selected and click **OK** to close the Accessibility dialog box.
- c. Click **OK** again to close the Internet Options dialog box.

In Mozilla:

- a. Select **Edit > Preferences > Composer**.
- b. Select the **Use CSS styles instead of HTML elements and attributes** check box and click **OK**.

**Step 7** Change the default font to sans-serif for improved readability:

In Netscape Navigator:

- a. Select **Edit > Preferences > Appearance > Fonts**.
- b. Select a sans-serif font (for example, Arial) and a font size in the **Typeface** and **Size** selection areas and click **OK**.

The text in the browser window is redrawn using the new fonts.

In Internet Explorer:

- a. Select **Tools > Internet Options > General** and click **Fonts**.
- b. Select a sans-serif font (for example, Arial) from the **Web page font** and **Plain text font** lists and click **OK**.
- c. Click **OK** to close the dialog box.

The text in the browser window is redrawn using the new fonts.

In Mozilla:

- a. Select **Edit > Preferences > Appearance**.
- b. Select **Fonts** from the Appearance category, choose . (If no options are visible in this category, double-click **Appearance** to expand the list.)
- c. From the Fonts for drop-down list, choose a language group/script. For example, to set default fonts for West European languages/script (Latin), choose **Western**.
- d. From the Proportional drop-down list, select Sans Serif. Then select an appropriate Sans serif font from the Sans-serif drop-down list and specify the font size you want for proportional text.

**Step 8** Disable any pop up blocker utility installed on your client system.

---

If you have browser problems after configuring your browser, increase your disk cache settings. After the web browser is installed on the client system, there are no additional disk space requirements. However, because the browser uses the local disk to store cached information, make sure you have enough disk space for the amount of cached information you want to store. All Common Services information is stored on the CiscoWorks server.

## Accessing CiscoWorks Server

CiscoWorks Common Services uses port 1741 for the HTTP server and port 443 for HTTPS server (SSL).

To access the server from a client system, enter any one of these URLs in your web browser:

- If SSL is disabled and if you have installed Common Services on the default port, and enter:

```
http://server_name:1741
```

- If SSL is enabled, and if you have installed Common Services on the default port, enter:

```
https://server_name:443
```

where *server\_name* is the hostname of the server on which you installed Common Services.

The CiscoWorks Login page appears.

See the Invoking CiscoWorks Homepage and Logging in to Common Services sections in the *User Guide for CiscoWorks Common Services 3.0.5* and *CiscoWorks Common Services 3.0.3* for more information.

Also, see “[TCP and UDP Ports Information](#)” section on page 2-5.

## Using Device Center

Device Center provides a one stop place where you can see a summary for a device, and launch troubleshooting tools, management tasks, and reports for the selected device. It provides a device centric navigation paradigm, which helps you to concentrate on device centric features and information from one single location.

See the Using Device Center chapter in the *User Guide for CiscoWorks Common Services 3.0.5* and *CiscoWorks Common Services 3.0.3* for more information about launching Device Center and using the Device Center functions.

## Using Device and Credentials Repository

The Device and Credential Repository (DCR) is a common repository of devices, their attributes, and credentials. These are to be used by various network management applications, to manage devices in a management domain. The Device and Credential Admin (DCA) provides an interface to administer DCR.

It enables multiple applications to share device lists and credentials using a client-server mechanism, with secured storage and communications. The applications can read or retrieve the information. The applications can also update the information in DCR so that it could be shared with other applications.

See the Managing Device and Credentials chapter in the *User Guide for CiscoWorks Common Services 3.0.5* and *CiscoWorks Common Services 3.0.3* for more information about Adding Devices, Deleting Devices, Editing Device Credentials, Importing Devices and Credentials, Exporting Devices & Credentials, Excluding Devices, Editing Device Identity, and, Viewing Devices List.

## Using Integration Utility

The Integration Utility allows you to launch CiscoView as well as Device Center from an NMS platform even when CiscoView is running on a different system than the NMS. It also allows you to integrate other applications into NMS menu.

See *User Guide for CiscoWorks Integration Utility 1.6* for information about configuring the Integration Utility.

## Using CiscoView

CiscoView is a graphical SNMP-based device management tool that provides real-time views of networked Cisco Systems devices.

See *User Guide for CiscoView 6.1.2* and *User Guide for CiscoView 6.1.5* for information about launching and using CiscoView.

## Casuser Permissions

Casuser (casuser) is the user created by CiscoWorks installation along with the casusers group, and included into the group.

If installation fails to create casuser, you can manually create the casuser local user and casusers local group on your Windows system after the installation. To do so:

- 
- Step 1** Click **Start > Settings > Control Panel > Administrative Tools > Computer Management** on your Windows 2003 system.  
The Computer Management console opens.
  - Step 2** Click **Local Users and Groups > Users** from the Computer Management console tree.
  - Step 3** Right-click **Users** from the console tree and click **New User**.  
The New User window opens.
  - Step 4** Enter the User name as casuser and Password of the casuser.
  - Step 5** Re-enter the password in the Confirm password field.
  - Step 6** Remove the selection from the **User must change password at next logon** check box.
  - Step 7** Select the **Password never expires** option.
  - Step 8** Click **Create**.  
The casuser is displayed in the Users list.
  - Step 9** Click **Local Users and Groups > Groups** from the console tree at the left.

**Step 10** Right-click **Groups** from the console tree and click **New Group**.

The New Group window opens.

**Step 11** Enter the group name as casusers, description of the group name and click **Create**.

**Step 12** Right-click the casusers group that you have created and click **Add to Group**.

The casusers Properties window appears. This window contains the list of users who are already added to the group, if any.

**Step 13** Enter the name of the user (casuser) whom you want to be part of casusers group and click **Add**.

**Step 14** Click **OK**.

---

To install and run the CiscoWorks, make sure that:

- localSystem account and casusers group (which is created by CiscoWorks installation) have sufficient permissions to load system DLLs from system32 directory.
- The same permissions should be granted to the user who is running installation of CiscoWorks. In addition, such user must be a member of the local group administrators. Permissions for this user are required for the time of installation or uninstallation only.
- Command line utilities provided by Windows such as cmd, regedit, cacls, ping, nslookup are present in the system.
- The casuser or the casusers group must have the following privileges on the system:
  - Access this computer from the network (SeNetworkLogonRight)
  - Log on as a batch job (SeBatchLogonRight).

CiscoWorks installation creates a casuser account with the SeNetworkLogonRight and SeBatchLogonRight privileges.

These required casuser privileges may be removed whenever the server is rebooted and the local security policy settings are re-applied.

You can verify these settings from the Local Security Policies console. To do so:

- a. Go to **Start > Settings > Control Panel > Administrative Tools > Local Security Policy** to open the Local Security Policy console.
- b. Click **Local Policies > User Rights Assignments**.
- c. Open the Properties windows for Access this computer from the network and Log on as a batch job properties. Check whether the casuser is added to list of users and groups in the Properties windows.

**Note**

All CiscoWorks processes are running as localSystem, or casuser.

