



## Setting Up the CiscoWorks Server

---

The CiscoWorks Server includes tools required to properly set up the server to support other CiscoWorks applications. These features include:

- [Setting Up User Accounts](#)
- [Using the Pluggable Authentication Modules](#)
- [Installing the Java Plug-in](#)

### Setting Up User Accounts

Several CiscoWorks network management and application management operations are potentially disruptive to the network or to the applications themselves, and must be protected.

To prevent such operations from being used accidentally or maliciously, CiscoWorks uses a multilevel security system that only allows access to certain features to users who can authenticate themselves at the appropriate level.

CiscoWorks provides two predefined login IDs, but as an administrator you can create additional unique login IDs for users at your company:

- guest (you can specify a password during installation, user role = Help Desk)
- admin (you can specify the password during installation, user role = a combination of System Administrator, Network Administrator, Network Operator, Approver, and Help Desk)

The login named admin is the equivalent of the superuser (in UNIX) or administrator (in Windows) for CiscoWorks. This login provides access to all CiscoWorks tasks.



### Caution

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 for **admin**.

## Understanding Security Levels

System administrators determine user security levels when they are granted access to CiscoWorks. When users are granted logins to the CiscoWorks application, they are assigned one or more roles.

The user role or combination of roles, dictates which CiscoWorks applications are presented to the users on the navigation tree. [Table 3-1](#) shows security levels.

**Table 3-1 Security Levels**

Level	Description
0	Help Desk
1	Approver
2	Network Operator
4	Network Administrator
8	System Administrator
16	Export Data
32	Developer
64	Partition Administrator

Other roles are displayed, depending on your applications. For example, the additional user roles (Developer, Export Data, and Partition Administrator) are displayed in the security user account windows. These roles are available only for Management Connection and third-party developers.

To see which security levels are allowed to use the CiscoWorks applications, select **Server Configuration > Setup > Security > Permissions Report**.

The Developer and Export Data roles are not displayed in the Permissions Report.

## Performing Security Tasks

Users can perform some tasks for their own accounts, but most security tasks require system administrator role privileges. When performing these security tasks (see [Table 3-2](#)), consider the following:

- Common Services cannot recover forgotten passwords. A system administrator-level user must either change the password or delete it, and then add the user role again.
- The username *admin* is reserved and cannot be deleted.
- If you have forgotten the admin password has been, see the [Resetting Passwords](#) section.

**Table 3-2 Security Tasks**

Task	Purpose	Action
<b>All Users</b>		
View role permissions.	Displays predetermined set of applications, tools, and product features that each user role can access.	Select Server Configuration > Setup > Security > Permissions Report
Change password.	Allows users to modify their account password.	Select Server Configuration > Setup > Security > Modify My Profile

Table 3-2 Security Tasks (continued)

Task	Purpose	Action
<b>Admin Tasks</b>		
Add a user.	Creates a new username and provides appropriate user access level to CiscoWorks.	Select Server Configuration > Setup > Security > Add Users
Delete a user.	Removes a username from the list.	Select Server Configuration > Setup > Security > Modify/Delete Users
Modify a user.	Allows updates to user information, such as email address, login name, password, and access level.	Select Server Configuration > Setup > Security > Modify/Delete Users
View other logged-in users.	Displays information about currently logged in CiscoWorks users and allows users to send a broadcast message to other users.	Select Server Configuration > Setup > Security > Who Is Logged On
Modify authentication module.	Allows the authentication of new users by using another source of authentication, such as directory service.	Select Server Configuration > Setup > Security > Select Login Module

## Using the Pluggable Authentication Modules

Pluggable authentication using the CiscoWorks Server security feature allows administrators to authenticate users by another source of authentication, such as a directory service. CiscoWorks provides several standard pluggable authentication modules that allow the administrator of the CiscoWorks Server to authenticate any CiscoWorks login with NT, UNIX, TACACS+, Radius or other authentication sources.

## Understanding Fall Back Options

There are three login module fall back options. These are available on all platforms. Fall back options allow you to access the software if the login module fails, or you accidentally lock yourself or others out. [Table 3-3](#) describes the login module fall back options.

**Table 3-3 Login Module Fall Back Options**

Option	Description
Allow all CiscoWorks Local users to fall back to the CiscoWorks Local login.	All users can access CiscoWorks using the Local login if the current login module fails.
Allow only the following user(s) to fall back to the CiscoWorks Local login if preceding login fails: <i>username</i> .	Specified users can access CiscoWorks using the Local login if the current login module fails. Use commas between user names.
Allow no fall backs to the CiscoWorks Local login.	No access is allowed if the current login module fails.

It is recommended that you select the option that allows specific users to fall back to the CiscoWorks Local login if a preceding login fails. This way, if your server cannot authenticate the user, and the user has a local CiscoWorks account, the CiscoWorks Local login module authenticates the same name and password.

If authentication occurs, the user can access CiscoWorks even if their first-choice server is down. You may also want to test the new login module by having a user log in, using the new authentication module.

**Note**

The administrator needs to add users with more privileges greater than that of a guest when choosing a pluggable authentication module. If the system falls back to the local authentication choice, a full set of user IDs and passwords is necessary.

## Selecting a New Login Module

Depending on your platform, different login module features are available (see [Table 3-4](#)).

**Table 3-4 Login Module Options on Supported Platforms**

Module	Available on UNIX	Available on Windows
CiscoWorks Local	X	X
Local UNIX System	X	
Local NT System		X
MS Active Directory	X	X
Netscape Directory	X	X
Radius	X	X
TACACS+	X	X
KerberosLogin	X	X
IBM SecureWay Directory	X	X

The following procedure describes how to select a login module. For more information on selecting login modules, refer to the online help.

---

**Step 1** Select **Server Configuration > Setup > Security > Select Login Module**.

The Select Login Module window appears.

**Step 2** Select your option:

- a. To view or change the current login module configuration, click **Edit Options**.
- b. To select a different login module, select the module, then click **Next**.

The Login Module Options window appears, showing the options for the currently selected module.

The available modules are listed.

**Step 3** Enter the data into the fields and click **Finish**. To return to the previous window and modify your data, click **Back**.

After you change the login module, you do not have to restart CiscoWorks. The user who logs in next after the change automatically uses the new module. Changes to the login module are logged in the *\$NMSROOT/objects/jrun/jsm-cw2000/logs* directory for Solaris and in *NMSROOT\lib\jrun\jsm-cw2000\logs* directory for Windows.

---

**Note**

If you accidentally lock yourself out of the CiscoWorks software, see the “[Frequently Asked Questions](#)” section on page 6-5.

---

## Installing the Java Plug-in

Installing the Java Plug-in is optional. You are required to install the plug-in only if you use applications like CiscoView and Essentials. It improves the performance of the such CiscoWorks applications and allows them to use the latest Java runtime functionality. For such applications, the plug-in speeds up caching and application loading. CiscoWorks requires the Java Plug-in version 1.3.1.

Only CiscoWorks applications that have been registered during installation to use Sun’s Java Plug-in, use this plug-in.

The first time you invoke any Java Plug-in enabled window, you are alerted if the plug-in has not been installed. CiscoWorks prompts you to download and install the plug-in files, using the installation screens or the procedure displayed. The next time you start the application, CiscoWorks automatically uses the plug-in.

When you install the Java Plug-in, the follow this sequence:

- Uninstall earlier version of Java Plug-ins, if they are present in your system
- Install the Java Plug-in 1.3.1 provided with CiscoWorks (not from any other source).


**Note**

If you are using a Windows client system, you must restart the system after installing the Java Plug-in.

If you are using a UNIX client system, you must manually download and install the Java Plug-in, then restart the browser.

## Resetting Passwords

The password reset utility allows you to change the password for a local CiscoWorks user from the command line. You should have CiscoWorks Server administrative or superuser privileges to run this utility.

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

```
*** CiscoWorks user password recovery utility ***
```

```
Usage: resetpasswd [-f] <username>
```

where, -f forces password change even if Daemon Manager detection FAILS.


**Note**

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

If you execute **resetpasswd** *username* (where *username* is a valid CiscoWorks Local user), it will prompt for the new password and displays the following list:

- The password entered is not displayed for security reasons.
- Press **Backspace** to delete the last typed character.
- Press **Ctrl-U** to delete all characters.
- Press **Ctrl-C** to abort the program without changing the user password.

These keys are available on both Windows and Solaris platforms.

To run the utility, enter:

- On Solaris  
`/opt/CSCOpX/bin/resetpasswd`
- On Windows:  
`NMSROOT\bin\resetpasswd.exe`

where, `/opt/CSCOpX` and `NMSROOT` are the install directories of CiscoWorks for Solaris and Windows respectively. As `CSCOpX\bin` is added to the system path, the utility can be executed without explicitly changing to the bin directory.

■ **Resetting Passwords**