



Configuring Your Devices

In this scenario, you are a system administrator who wants to use CiscoView to configure a Catalyst 4000 series device and add IP addresses to allow other management workstations to access the same device. At the same time, you want to limit access to that particular device for other management workstations.

What You Need

Verify these prerequisites *before* starting the procedure for this scenario:

- SNMP credentials are valid.
- Permissions for IP addresses are enabled.

How to Do It—Procedures

Use the procedures in this section to:

1. [Access the Device Configuration Dialog Box.](#)
2. [Add IP Addresses for Other Management Workstations.](#)
3. [Limit Device Access.](#)

Access the Device Configuration Dialog Box

Access the Device Configuration dialog box to configure your device:

-
- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
 - Step 2** Right-click the device. The context menu appears.
 - Step 3** Select **Configure**. The Device Configuration dialog box appears.
 - Step 4** Configure your Catalyst 4000 device by entering the required information for that device in the provided categories.
 - Step 5** Click **OK**.
-

Add IP Addresses for Other Management Workstations

After you configure your device, add new IP addresses to the IP Permit List, which determines which management workstations are permitted to access this particular device.



Note IP addresses allow management workstations to access specific devices for configuration. You can add as many IP addresses to the IP address list as necessary.

-
- Step 1** From the Device Configuration dialog box, select **IP Permit** from the Category list to display the IP Permit window.
 - Step 2** Click **Create**. The Row Creation dialog box appears.
 - Step 3** Enter the appropriate IP address and IP mask.
 - Step 4** Select the appropriate access type from the list and click **OK**. The new IP address is added to the IP Permit List.
-

Limit Device Access

Limit access privileges for other management workstations and monitor unauthorized attempts to access the device.

-
- Step 1** In the IP Permit window, highlight the IP address to be deleted from the IP Permit List and click **Delete**. This disables that particular management workstation from accessing the device.
 - Step 2** To monitor unauthorized attempts to access the device, reopen the IP Permit window to view any access to the device.
-

Where You Should End Up—Verification

After you configure your device and limit access to the device by other management workstations, verify that there are no unauthorized workstations accessing the device.

-
- Step 1** Go to the bottom of the window to view the Access Attempts From Invalid IP Addresses table. This table provides information about which management workstations recently attempted to access the device, the time and date of attempted access, and a list of the invalid IP addresses that were deleted.
 - Step 2** If a deleted IP address is still attempting to access the device, notify the owner of that particular management workstation regarding any recent changes made to the owner's security level.
-

