Getting Started

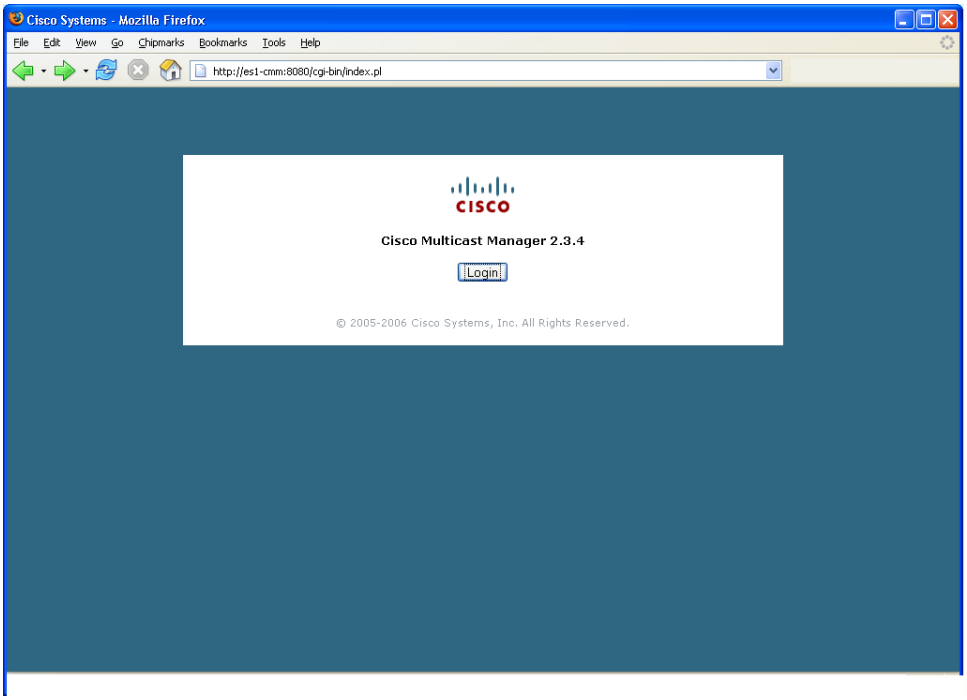
This chapter covers:

Logging Into the CMM

Note For details on stopping and starting the CMM application on Solaris and Linux, see the *Installation Guide for the Cisco Multicast Manager 2.3*.

To access CMM, enter the IP address or the name of the server where the software is installed. For example: http://172.16.0.1:8080. The default port of 8080 can be changed as described in the installation instructions.

Figure 1-1 Login Page for CMM 2.3.4



To enter CMM, click **Login**. You are prompted for a username and a password. The default CMM username is *admin*, and the default CMM password is *rmsmmt*.

Overview

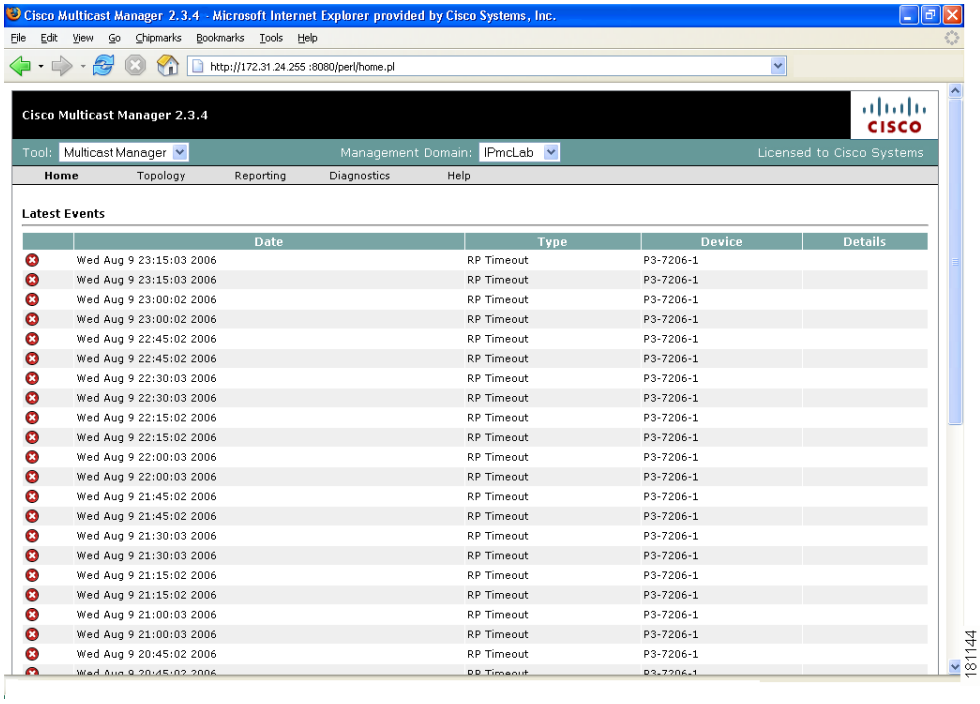
The CMM has two main tools: **Administration** and **Multicast Manager**. You can select either tool from the menu at the upper left of the CMM Web interface. You can perform the following tasks with each tool:

Tool	Tasks	Information
Administration	Manage domains	Creating a Domain, page 1-3
	Perform administrative utilities	Using Administrative Utilities, page 2-1
	Configure security	Configuring System Security, page 2-3
	Manage users	Managing Users and Passwords, page 2-4
	Perform discovery	Discovering Your Network, page 1-6
	Configure devices	Configuring Devices, page 2-6
	Configure global polling	Configuring Global Polling, page 2-12
	Manage addresses	Managing IP Addresses, page 2-16
	Configure specific polling	Configuring Specific Multicast Manager Polling, page 2-17

Tool	Tasks	Information
Multicast Manager	View events through the **Home** page	• Viewing the Multicast Manager Home Page, page 3-1 • Latest Events, page 3-5
	View **Topology**	Viewing Topology, page 3-2
	Manage **Reporting**	Managing Reports, page 3-4
	Manage **Diagnostics**	Managing Diagnostics, page 4-1
	View **Help**	Viewing User Guide Help, page 4-21

When you first log into the CMM, the Multicast Manager home page appears.

Figure 1-2 Multicast Manager Home Page



For detailed information on this window, see the "Viewing the Multicast Manager Home Page" section on page 3-1.

Creating a Domain

Before you can begin managing your networks, you must create a domain. A domain is a collection of multicast routers. Multiple domains may exist, and routers can belong to multiple domains. Using Domain Management, you can create and edit domains.

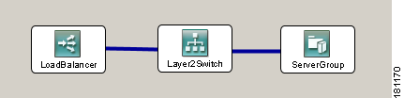
To create a domain:

Step 1 From the Multicast Manager home page, select the **Administration** tool.

Step 2 Select **Domain Management**.

Step 3 Select **add a new domain**. The System Configuration page appears.

Figure 1-3 System Configuration



Step 4 Complete the fields in the System Configuration page and click **Save** to continue and create the new domain. Click **Cancel** to exit without creating a domain.

Field	Description
Management Domain	A management domain is defined as a contiguous group of PIM neighbors sharing the same SNMP community string.
Default Read Only	SNMP read-only community string.
Default Read Write	SNMP read-write community string. This is required for retrieving and validating device configurations.
SNMP Timeout	Retry period if node does not respond. Default value is 0.8.
SNMP Retries	Number of retries to contact a node before issuing a timeout. Default value is 2.
TFTP Server	TFTP server IP address. Default is the IP address of the CMM server.

Field	Description
VTY Password	The VTY password is required if you want to issue show commands from the application. Certain features, such as querying Layer 2 switches, also require this. If TACACS is being used, then a username and password can be supplied instead of the VTY password.
Enable Password	(*Not currently used.*)
TACACS/RADIUS Username	If you are using TACACS/RADIUS then you can enter a username here. See VTY Password above. **Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands.
TACACS/RADIUS Password	If you are using TACACS/RADIUS then you can enter a password here. See VTY Password above. **Note** If you enter a TACACS/RADIUS username and password here, the application will use these values regardless of who is currently logged in. Users can also enter their own username and password when issuing show commands.
Cache TACACS Info	If this box is checked, CMM will cache the TACACS username and password until the browser is closed. This eliminates having to enter the username and password each time you issue a router command from the application.

Field	Description
Resolve Addresses	Performs DNS lookups on all sources found. The DNS name appears alongside the IP address on the “Show All Groups” screen. If the server is not configured for DNS, then DO NOT check the box. If the box is checked, you may receive a slower response, due to the fact that the application is trying to resolve names. This option is not recommended if your network contains a large number of S,Gs. The Resolve Addresses option also causes discovery to do a reverse DNS lookup on a device name. The IP address returned by DNS is then used for management purposes. Otherwise, the IP address by which the device is found is used for management purposes.
Use SG Cache	Some networks contain thousands of S,Gs. During discovery, CMM caches all the S,Gs found in the RPs. If this box is checked, CMM reads the SG cache when showing lists of sources and groups, rather then retrieving them again from the RPs in the network. The cache is automatically refreshed if RPs are being polled as described later in this document (see the “RP Polling” section on page 2-17). The cache can also be refreshed manually by clicking the **Refresh Cache** button in the Multicast Diagnostics window (see the “Show All Groups” section on page 4-1). This button appears only if you have the **Use SG Cache** option selected. It is highly recommended to use the SG cache option. If there are no RPs in the domain being discovered, then the SG cache is created by querying all the devices that have been discovered, as would be the case in a PIM Dense-Mode network. In this case, the SG cache is updated only when you click the **Refresh Cache** button.

Discovering Your Network

Note If you are upgrading from CMM 2.3, you must run discovery to access new features.

After you have created a domain, the second step in using the CMM is to discover your network using one of these choices, found within the **Discovery** menu:

- Add Router (not supported)
- Adding Layer 2 Switches to Discovery, page 1-7
- Performing Multicast Discovery, page 1-8
- Adding or Rediscovering a Single Device, page 1-10

The discovery process is multicast-specific and finds only devices that are PIM-enabled. CMM builds a database of all found devices. Discovery adds support for multiple community strings per domain, along with device-specific SNMP timeout and retries.

Note If any new routers or interfaces are added to the network, run discovery again so that the database is consistent with the network topology.

A single router may also be added or rediscovered on the network. A router being added must have a connection to a device that already exists in the database. A router that is being rediscovered is initially removed from the database, along with any neighbors that exist in the database. The router and its neighbors are then added back into the database. This option would be used if a change on a device has caused a change in the SNMP ifIndexes.

Note When possible, the snmp ifindex persist command should be used on all devices.

Adding Layer 2 Switches to Discovery

Layer 2 switches are not included in discovery and must be added manually. You can add switches individually, or you can import a list of switches in a csv file.

To add switches individually, enter the switch name or IP address and the community string, then click **Add**.

To import a list of switches:

Step 1 Create a text file by typing:

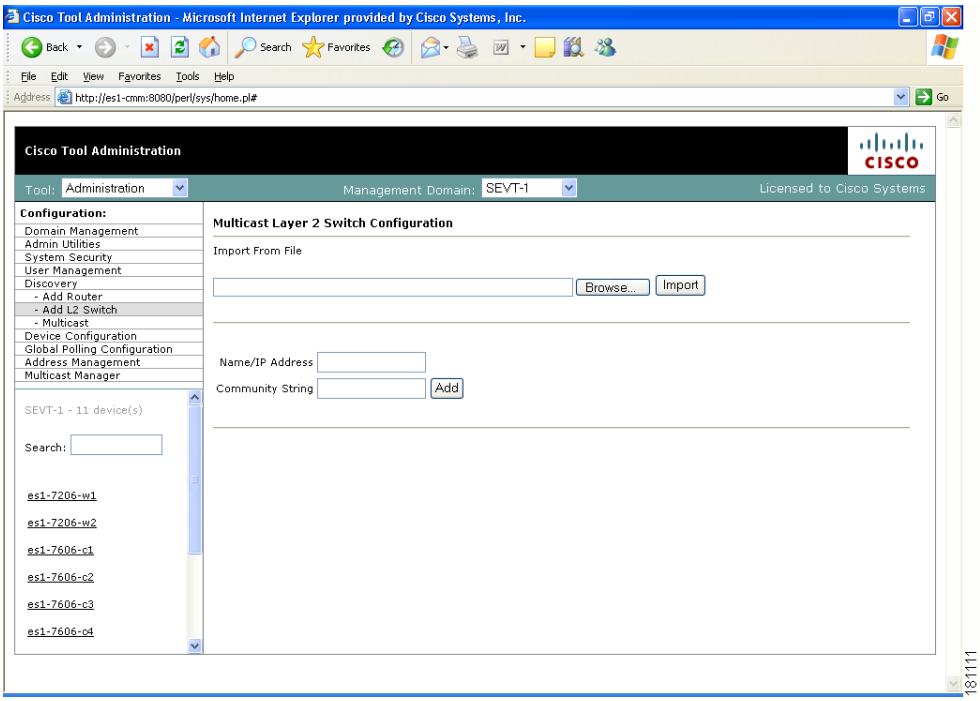
```
#import file format switch IP address or switch name
# this line will be skipped
switchA
192.168.1.1
switchC
10.10.10.1
```

Step 2 Save the file.

Step 3 Within the Administration tool, select **Discovery**.

Step 4 Select **Add L2 Switch**. The Multicast Layer 2 Switch Configuration page appears.

Figure 1-4 Multicast Layer 2 Switch Configuration



Step 5 Click **Browse**. Open the file you created.

Step 6 Click **Import**.

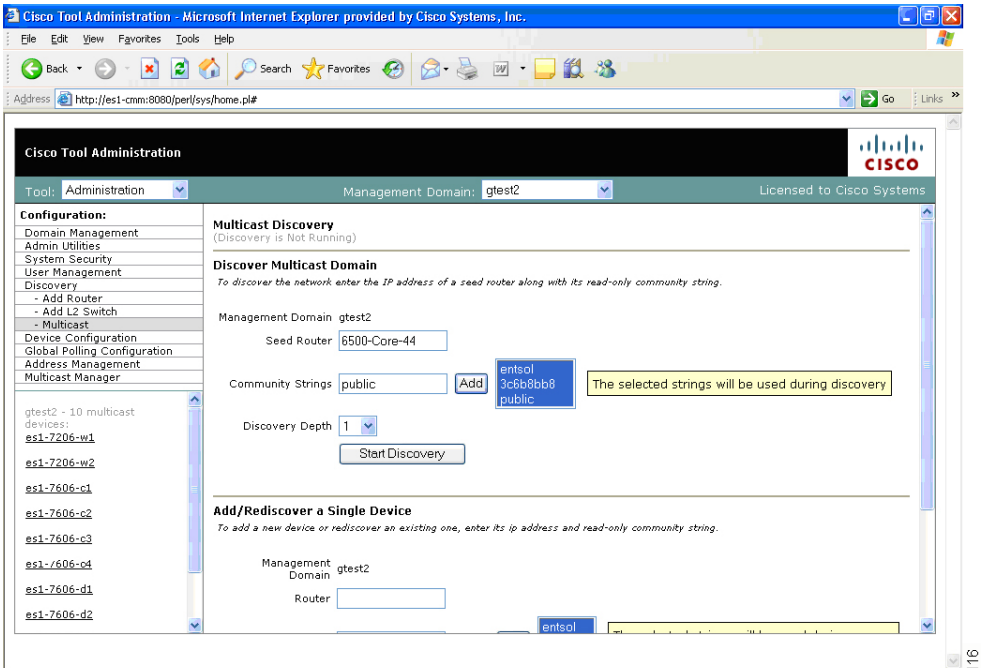
Performing Multicast Discovery

To perform a new multicast discovery:

Step 1 Within the Administration tool, select **Discovery**.

Step 2 Select **Multicast**. The Multicast Discovery page appears, with a **Management Domain** selected.

Figure 1-5 Multicast Discovery



Step 3 Complete the fields in the **Discover Multicast Domain** pane and click **Start Discovery** to continue. As routers are discovered, they appear in the browser window.

Step 4 (Optional) To view discovery progress as it is running, click **Refresh Status**.

Note For details on adding or rediscovering a single device, see Adding or Rediscovering a Single Device, page 1-10.

Field	Description
Management Domain	(Read-only) Lists the selected management domain.
Seed Router	Enter the IP address of the seed router to start discovery. If you enabled DNS when configuring the domain, enter a name.
Community Strings	You can add additional community strings if required.
Discovery Depth	Number of PIM neighbors the CMM will discover from the seed router (similar to a hop count).

CMM discovers all routers in the network that are multicast enabled and have interfaces participating in multicast routing. If the discovery fails to find any routers, or if there are routers in the network that you expected to discover but did not, check the following:

- Connectivity to the routers

- SNMP community strings on the routers
- Discovery depth setting—is it sufficient?
- SNMP ACLs on the routers

When discovery is complete, the browser window displays the time it took to discover the network and the number of devices discovered:

```
Discovery took 15 seconds
Discovered 5 routers
```

The time the discovery takes depends on the number of routers, number of interfaces, and router types.

If the discovery seems to stop at a particular router, or seems to pause, check that particular router's connectivity to its PIM neighbors. Also, check the PIM neighbor to see if it supports the PIM and IPMROUTE MIBs. Again, because the discovery is multicast-specific, unless these MIBs are supported, the device will not be included in the database. Issuing the **sh snmp mib** command on a router gives this information.

When discovery finishes, you can view the discovered routers in the lower left pane.

Adding or Rediscovering a Single Device

To add or rediscover a single device:

Step 1 Within the Administration tool, select **Discovery**.

Step 2 Select **Multicast**. The Multicast Discovery page appears (see Figure 1-5). A **Management Domain** is selected.

Step 3 Complete the fields in the **Add/Rediscover a Single Device** pane and click **Add/Rediscover** to continue. As devices are discovered, they appear in the browser window.

Field	Description
Management Domain	(Read-only) Lists the selected management domain.
Router	Enter the IP address of the device you want to discover or add.
Community Strings	You can add additional community strings if required.
This device only	Rediscovers this device and updates the current database with the new information.
One hop from this device	Discovers this router and every router within one hop, and updates the current database with the new information.