



Administering Campus Manager

Network administrators can perform administrative tasks on Campus Manager applications using the Administration module. This chapter contains:

- [Understanding Campus Manager Administration, page 4-1](#)
- [Using Daemon Manager, page 4-2](#)
- [Using Campus Manager Administration, page 4-3](#)
- [Administration Command Line Interface, page 4-53](#)
- [Security, page 4-56](#)
- [Frequently Asked Question, page 4-56](#)

Understanding Campus Manager Administration

You can set up Device Discovery, Data Collection, and User Tracking acquisition using the Administration module of Campus Manager.

The Administration module also allows you to:

- Configure discrepancy reporting for the discrepancies.
- Specify any discrepancies for which you need to generate syslog messages.
- Administer Groups.
- Schedule Path Analysis traces.

Using Daemon Manager

The Daemon Manager provides the following services:

- Maintains the startup dependencies among processes.
- Starts and stops processes based on their dependency relationships.
- Restarts processes if an abnormal termination is detected.
- Monitors the status of processes.

The Daemon Manager is useful to applications that have long-running processes that must be monitored and restarted, if necessary. It is also used to start processes in a dependency sequence, and to start transient jobs.

Restarting Daemon Manager on Solaris

To restart Daemon Manager on Solaris:

-
- Step 1** Log in as root.
- Step 2** To stop the Daemon Manager, enter:
- ```
/etc/init.d/dmgttd stop
```
- Step 3** To start the Daemon Manager, enter:
- ```
/etc/init.d/dmgttd start
```
-

Restarting Daemon Manager on Windows

To restart Daemon Manager on Windows:

-
- Step 1** Go to Command Prompt.
- Step 2** To stop the Daemon Manager, enter:
- ```
net stop crmdmgttd
```

**Step 3** To start the Daemon Manager, enter:

```
net start crmdmgt
```

---

**Note**

Do not start the Daemon Manager immediately after you stop it. The ports used by Daemon Manager will be in use for a while even after the Daemon Manager is stopped. Wait for sometime before you start the Daemon Manager.

---

If the System resources are less than the required resources to install the application, Daemon Manager restart displays warning messages that are logged into syslog.log.

## Using Campus Manager Administration

Use the administrative functions of Campus Manager to:

- View the Admin Dashboard. For more details, see [Viewing Campus Manager Administration Dashboard, page 4-5](#).
- Setup Device Discovery
  - View the summary of Device Discovery Settings. For details, see [Viewing Summary of Device Discovery Settings, page 4-6](#).
  - Specify the seed device and the IP address range, For details, see [Specifying Seed Device and IP Address Range, page 4-9](#).
  - Modify the Discovery Schedule. For details, see [Modifying Discovery Schedule, page 4-14](#).

- Specify the debugging options. For details, see [Setting Debugging Options for Device Discovery, page 4-15](#)
- Modify SNMP settings. For details, see [Administration Command Line Interface, page 4-53](#).
- Setup Data Collection
  - View a summary of Data Collection settings. For details, see [Viewing Summary of Data Collection Settings, page 4-18](#)
  - Modify Data Collection schedule. For details, see [Scheduling Data Collection, page 4-20](#).
  - Specify Data Collection filters. For details, see [Setting up Data Collection Filters, page 4-22](#)
  - Set Data Collection debugging options. For details, see [Setting up Debugging Options for Data Collection, page 4-25](#)
- Administer User Tracking. For details, see [Using User Tracking Administration, page 4-29](#)
- Manage Groups. For details, see [Understanding Groups, page 4-29](#)
- Configure Network Discrepancies settings. For details, see [Configuring Discrepancy Reporting and Syslog Message Generation, page 4-45](#).
- Schedule Path Analysis traces. For details, see [Scheduling Jobs for Path Analysis, page 4-46](#).
- View reports on ANI server analysis, Device Discovery, Data Collection, and device support. For details, see [Using Administration Reports, page 4-49](#).

This section contains:

- [Viewing Campus Manager Administration Dashboard, page 4-5](#)
- [Using Device Discovery Administration, page 4-6](#)
- [Using Campus Data Collection Administration, page 4-17](#)
- [Using User Tracking Administration, page 4-29](#)
- [Understanding Groups, page 4-29](#)

## Viewing Campus Manager Administration Dashboard

You can view the status of Device Discovery, Data Collection, and User Tracking Acquisition in the Campus Administration dashboard. You can also view a brief description of the steps involved in configuring Campus Manager.

To view the Campus Administration dashboard, start **Campus Manager > Administration**. The Campus Manager Administration dashboard appears.

[Table 4-1](#) describes the fields in the Current Status table.

**Table 4-1** *Fields in the Current Status Table*

| Field                | Description                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Operation            | Campus Manager applications—Device Discovery, Data Collection, User Tracking Acquisition                                        |
| Last Completion Time | Date and time when the operation was last completed                                                                             |
| Result               | Click on the respective hyperlinks, you will get reports on Device Discovery, Data Collection, and User Tracking quick reports. |
| Status               | Status of the Operation—Running or Idle                                                                                         |
| Action               | Click on the respective hyperlinks to start Device Discovery, Data Collection, or User Tracking Acquisition.                    |

The Configure Campus Manager table gives a brief description of the steps required for configuring Campus Manager.

You can use the hyperlinks in this table to perform the following tasks:

- Modify SNMP settings
- Specify seed device and IP address range for Device Discovery
- Modify Device Discovery Schedule
- Specify Data Collection filters
- Schedule Data Collection
- Start User Tracking Administration

Click the Refresh icon to get the updated status.

## Using Device Discovery Administration

The Device Discovery option of the Admin tab in the Campus Manager Administration window allows you to:

- View a summary of Device Discovery settings. For more details, see “[Viewing Summary of Device Discovery Settings](#)” section on page 4-6.
- Modify SNMP settings. For more details, see “[Setting SNMP Credentials](#)” section on page 4-7.
- Specify the seed device and IP address range. For more details, see “[Specifying Seed Device and IP Address Range](#)” section on page 4-9.
- Modify Device Discovery schedule. For more details, see “[Modifying Discovery Schedule](#)” section on page 4-14.
- Specify the Device Discovery debugging options. For more details, see “[Setting Debugging Options for Device Discovery](#)” section on page 4-15.

You can click the Go to Campus Administration hyperlink from any screen to go to the Campus Administration dashboard.

[www.cisco.com](http://www.cisco.com)

## Viewing Summary of Device Discovery Settings

You can view a summary of the Device Discovery settings using the Device Discovery option in the Admin tab of Campus Manager Administration window.

To view a summary of Device Discovery settings:

---

**Step 1** Select **Campus Manager > Administration**.

The Campus Administration window appears.

**Step 2** Select **Admin > Device Discovery**.

The Device Discovery Settings Summary page appears.

[Table 4-2](#) describes the fields that appear in the Device Discovery Settings Summary page.

**Table 4-2** *Discovery Settings Summary*

| <b>Field</b>           | <b>Description</b>                                                                                                                 |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| SNMP                   | Click <b>View Details</b> to view the SNMP settings. You can add new SNMP community strings, and edit or delete existing settings. |
| Use LoopBack Address   | If True, the preferred management address is obtained by searching for the address assigned to the Loopback interface.             |
| ResolveByName          | If True, name resolution using device name is enabled                                                                              |
| ResolveBySysName       | If True, name resolution using sysname is enabled                                                                                  |
| Jump Router Boundaries | If True, discovery beyond router boundaries is enabled.                                                                            |
| Reverse DNS Lookup     | If True, name resolution using reverse DNS lookup is enabled.                                                                      |
| Seed Device            | Click <b>View Details</b> to view the Device Discovery Settings page. You can use this page to configure the seed device(s).       |
| IP Address Range       | The IP address range specified for discovery.                                                                                      |
| Discovery Schedule     | Click <b>View Details</b> to view the discovery schedule. You can add a new schedule, and edit or delete existing schedules.       |

## Setting SNMP Credentials

You can modify SNMPv2 and SNMPv3 credentials using the **Discovery > SNMP Settings** option from the Admin tab in the Campus Manager Administration window.

You must set the write community before you start using the configuration features in Campus Manager. To set the write community, select **Common Services > Device and Credentials > Device Management** from the CiscoWorks homepage.

To modify SNMP settings:

- Step 1** Select **Campus Manager > Administration**.  
The Campus Administration window appears.
- Step 2** Select **Admin > Device Discovery > SNMP Settings**.  
The Modify SNMP Setting window appears.  
Modify the SNMP settings as given in [Table 4-3](#).

**Table 4-3** *Modify SNMP Settings*

| Fields                            | Description                                                                                                                              | Usage Notes                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMPV2,<br>SNMPV3                 | Select the appropriate radio button for the version of the Simple Network Management Protocol for which you want to modify the settings. | Selecting the radio button displays the fields appropriate to the SNMP version selected.                                                                                                                     |
| <b>SNMPV2</b>                     |                                                                                                                                          |                                                                                                                                                                                                              |
| Enable Multiple Community Strings | Select this to enable multiple community strings.                                                                                        | You can provide multiple community strings for the same IP address range. Each string is tried for reachability until the correct string is found.<br><br>For example, 10.*.*.* public1 and 10.*.*.* public2 |
| Encrypt Community Strings         | Select this to enable encryption of community strings                                                                                    | Community strings are stored in the system in the encrypted format.                                                                                                                                          |
| Target                            | Target device.                                                                                                                           | None.                                                                                                                                                                                                        |
| Read Community                    | Read community string.                                                                                                                   | None.                                                                                                                                                                                                        |
| Time Outs                         | Time period after which the query times out.                                                                                             | If time out is increased, discovery time could also increase.                                                                                                                                                |
| Retries                           | Number of attempts.                                                                                                                      | None.                                                                                                                                                                                                        |
| Comments                          | Remarks, if any.                                                                                                                         | None.                                                                                                                                                                                                        |

**Table 4-3**      **Modify SNMP Settings (continued)**

| Fields                                         | Description                                                        | Usage Notes                                                   |
|------------------------------------------------|--------------------------------------------------------------------|---------------------------------------------------------------|
| <b>SNMPV3</b>                                  |                                                                    |                                                               |
| Encrypt the fields except Retries and Timeouts | Select this to encrypt all fields except Retries and Timeouts.     | None.                                                         |
| Target                                         | Target device.                                                     | None.                                                         |
| UserName                                       | Name of the user who has access to views configured on the device. | None.                                                         |
| Password                                       | Password of the user.                                              | None.                                                         |
| Time Outs                                      | Time period after which the query times out.                       | If time out is increased, discovery time could also increase. |
| Retries                                        | Number of attempts.                                                | None.                                                         |
| Authentication                                 | Method of authentication.                                          | The method of authentication is SHA-1 or MD5.                 |
| Comments                                       | Remarks, if any.                                                   | None.                                                         |

- Step 3** Do one of the following:
- Click **Add** to add community strings.
  - Select a row and click **Edit** to edit the community strings.
  - Select a row and click **Delete** to delete the community string.
- Click **OK** to save the changes or click **Cancel** to exit.

- Step 4** Click **Apply**.

## Specifying Seed Device and IP Address Range

You can specify the seed device and IP Address Range using the **Device Discovery > Discovery Settings** option in the Admin tab of Campus Manager Administration window.

The seed device is the starting point from which Campus Manager discovers the network and its neighbors.

The seed device must be a Cisco device. It should be a core switch and not a router. Although you can specify a router IP address, you might experience problems with network discovery.

Ideally a seed device must include the Cisco Catalyst 5000 series, Cisco Catalyst 5500 series, and Cisco Catalyst 8510 series devices. If you must use a router as the seed device, make sure you select the Jump Router Boundaries option.

To specify Device Discovery settings:

**Step 1** Click **Campus Manager > Administration**.

The Campus Administration window appears.

**Step 2** Click **Admin > Device Discovery > Discovery Settings**.

The Device Discovery Settings dialog box appears.

**Step 3** Specify the seed device and the IP address range as described in [Table 4-4](#).

**Table 4-4** *Device Discovery Settings*

| Field                  | Description                                                                                                                               | Usage Notes                                                                                                                                                                                                                                                                                                                          |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jump Router Boundaries | Select this option to extend discovery beyond the boundaries set by routers on your network.                                              | Be cautious about enabling discovery to occur beyond router boundaries.<br><br>Discovery could take much longer if you do not selectively choose the boundaries by excluding specific IP addresses.                                                                                                                                  |
| Use Reverse DNS Lookup | Select this option to use DNS for Device Discovery.<br><br>When you check this checkbox, the Preferred Management IP options are enabled. | Device Discovery uses Domain Name Services (DNS), if available, to perform device name lookups. If Device Discovery has problems resolving DNS names, discovery might take longer.<br><br>Therefore, if you do not use DNS in your network, or if you are experiencing problems with DNS, consider disabling the reverse DNS lookup. |

**Table 4-4**      **Device Discovery Settings (continued)**

| Field                          | Description                                                                                                                                                                                                                                          | Usage Notes                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Preferred Management IP</b> |                                                                                                                                                                                                                                                      |                                                                                                               |
| Use LoopBack Address           | Select this option to resolve name server by loopback address.<br><br>If the device has IP for LoopBack Interface, the device is managed in this IP Address.<br><br>If there are multiple Loopback IPs, one of them is used for managing the device. | The preferred management address is obtained by searching for the address assigned to the Loopback interface. |
| Resolve By Name                | Select this option if you have configured the device with DNS Name. This name is fetched from DNS during discovery                                                                                                                                   | The preferred management address is obtained by resolving the name using the device name.                     |
| Resolve By Sysname             | Select this option to contact the DNS Server to pick up the device hostname.                                                                                                                                                                         | The preferred management address is obtained by resolving the name using the Sysname.                         |

**Table 4-4**      **Device Discovery Settings (continued)**

| Field              | Description                                                                                                                                                 | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Seed Device</b> |                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Seed Device        | <p>Seed devices are devices used to initiate network discovery.</p> <p>Click <b>Configure</b> to enter the IP address or host name of the seed devices.</p> | <p>Click <b>Browse</b> to enter seed devices in a file.</p> <p>The seed devices stored in the file have to be separated by a carriage return. Only one seed device can be stored in each line in the file.</p> <p>For example, the seed devices in the file can be entered as:</p> <pre>172.20.5.6 172.20.118.130 10.77.209.209 172.20.99.2 10.77.210.101 10.77.210.103</pre> <p>Click <b>Add</b> to add new rows, to enter seed device.</p> <p>If you limit discovery by IP addresses, and these address are separated by addresses that are not in the included list, you must add a seed device for each set of addresses.</p> <p>Click <b>OK</b> to save the seed device.</p> |

Table 4-4 Device Discovery Settings (continued)

| Field                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IP Address Range</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IP Address Range        | <p>You can limit discovery by IP addresses in your network:</p> <p>Click <b>Configure</b> to enter the IP Address ranges.</p> <ol style="list-style-type: none"> <li>From the drop-down list box, select either of these options: <ul style="list-style-type: none"> <li>Discover devices in IP address range.</li> </ul> </li> <li>Or <ul style="list-style-type: none"> <li>Do not discover devices in IP address range.</li> </ul> </li> </ol> <ol style="list-style-type: none"> <li>Enter an IP address or a range of IP addresses to limit discovery. Use standard IP addressing format (4 octets separated by periods) where any octet is: <ul style="list-style-type: none"> <li>IP address—Number between 0 and 255<br/>172.20.4.9</li> <li>Wild card—Asterisk (*) denoting all numbers from 0-255, inclusive<br/>172.*.4.9</li> <li>Range—[begin-end], where <i>begin</i> and <i>end</i> are numbers between 0-255; <i>begin</i> is less than <i>end</i>.<br/>172.[4-55].4.9</li> </ul> </li> </ol> <ol style="list-style-type: none"> <li>Click <b>OK</b> to save the IP address range.</li> </ol> | <p>Establishing IP address boundaries prevents discovery from occurring outside of these boundaries. You can enter multiple IP Address ranges.</p> <p>You can only exclude or include IP addresses or ranges; you cannot do both.</p> <p>For example, you cannot enter IP addresses A and B to be discovered and IP address C to not be discovered. You can either include IP addresses A and B, or exclude IP address C.</p> |

**Step 4** Click **Apply**.

The settings are saved.

**Step 5** Click either:

- **OK** to start Device Discovery immediately.

Or

- **Cancel** if you do not want to start Device Discovery immediately.
- 

## Modifying Discovery Schedule

You can modify the day, time, and frequency of discovery using **Device Discovery > Schedule Discovery** of the Admin option in Campus Manager Administration.

To modify the discovery schedule:

---

**Step 1** Click **Campus Manager > Administration**.

The Campus Administration window appears.

**Step 2** Click **Admin > Device Discovery > Schedule Discovery**.

The Schedule Discovery dialog box appears.

**Step 3** You can add, delete, or edit an existing schedule.

- Click **Add** if you want to add a new Discovery Schedule.
- Click **Delete** if you want to delete a Discovery Schedule.
- Click **Edit** if you want to modify an existing schedule. Modify the discovery schedule settings as described in [Table 4-5](#).

**Table 4-5**      **Discovery Schedule**

| Field              | Description                                                        | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Days, Hour, Min    | Days on which and the time at which discovery is scheduled.        | <p>Optimum discovery schedule depends on the size of network and frequency of network changes.</p> <p>The default discovery schedule is every 4 hours, on the 4-hour mark, daily: 3.00, 7.00 11.00, 15.00, 19.00, 23.00. Time is in the 24-hour format.</p> <p>You can add new schedules and edit or delete existing schedules.</p> <ul style="list-style-type: none"> <li>• Select a schedule and click <b>Edit</b> to edit the schedule.</li> <li>• Select a schedule and click <b>Delete</b> to delete the schedule.</li> <li>• Click <b>Add</b> to add a new schedule</li> </ul> <p>Click <b>OK</b> after adding or editing a schedule to save changes.</p> |
| Recurrence Pattern | Select the days of the week on which discovery is to be scheduled. | This field is available only when you add or edit a schedule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Step 4**      Click **Apply** to save these changes.

---

Discovery must occur frequently enough to capture changes to the network within a reasonable amount of time. This frequency is dependent on the frequency of changes to your network.

## Setting Debugging Options for Device Discovery

You can specify the trace, debugging and logging options for Device Discovery using the **Device Discovery > Discovery Debugging Options** option in the Admin tab of Campus Manager Administration window.

To set the debugging options:

- 
- Step 1** Select **Campus Manager > Administration**.  
The Campus Manager Administration window appears.
- Step 2** Click **Admin > Device Discovery > Debugging Options**.  
The Discovery Debugging Options dialog box appears.
- Step 3** Modify the debugging options as specified in [Table 4-6](#).

**Table 4-6** *Debugging Options Field Description*

| Field                                | Description                                                                      | Usage Notes                                                                                                                                                     |
|--------------------------------------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Debug</b>                  |                                                                                  |                                                                                                                                                                 |
| Modules                              | Specify the modules on which debug is to be enabled.                             | Click <b>Select</b> to view the available modules and select the modules in which debug is to be enabled.<br><b>Select</b> is enabled only if Debug is enabled. |
| File Name                            | Name of the log file in which the trace messages are to be recorded.             |                                                                                                                                                                 |
| Maximum File Size (lines)            | Maximum size of the file in lines                                                | The default file size is set to 10,000 lines.                                                                                                                   |
| <b>Enable Device Level Debugging</b> |                                                                                  |                                                                                                                                                                 |
| Device IP(s)                         | IP addresses of devices for which discovery debugging messages are to be logged. | This field is enabled only when the device level debugging option is enabled.<br>You can enter multiple IP addresses, separated by commas.                      |

- Step 4** Click **Apply**.
-

### Selecting Modules

Table 4-7 describes the debug modules available for Device Discovery in Campus Manager.

**Table 4-7**      *Device Discovery Debug Modules*

| Service Module | Description                                                                                                                                                                                                                                                                                |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frontend       | Provides framework for Campus Manager features. Enable debugging for this module only when requested by TAC. This is because enabling debugging for this module creates huge logs.                                                                                                         |
| framework      | <ul style="list-style-type: none"> <li>Constructs and maintains data in the memory.</li> <li>Provides framework for Campus Manager features.</li> </ul> Enable debugging for this module only when requested by TAC. This is because enabling debugging for this module creates huge logs. |
| devdiscovery   | Performs Device discovery of your network. Enable debugging for this module if you have any issues related to Device Discovery.                                                                                                                                                            |
| devices        | Provides specific information, if any, available for device categories.                                                                                                                                                                                                                    |

Click **OK** to save the selected modules or click **Cancel** to exit.

## Using Campus Data Collection Administration

You must run Data Collection for Campus Manager to manage devices. Using the Administration module of Campus Manager you can:

- View the summary of Data Collection settings. For details, see [“Viewing Summary of Data Collection Settings” section on page 4-18](#).
- Modify SNMP Timeouts and Retries. For details, see [“Modifying SNMP Timeouts and Retries” section on page 4-19](#).

- Schedule Data Collection. For details, see [“Scheduling Data Collection” section on page 4-20](#).
- Specify Data Collection filters. For details, see [“Setting up Data Collection Filters” section on page 4-22](#).
- Specify the Data Collection debugging options. For details, see [“Setting up Debugging Options for Data Collection” section on page 4-25](#).

You can click the Go to Campus Administration hyperlink from any screen to go to the Campus Administration dashboard.

## Viewing Summary of Data Collection Settings

You can view a summary of the Data Collection settings using the Campus Data Collection option in the Admin tab of Campus Administration window.

To view a summary of Data Collection settings:

---

**Step 1** Select **Campus Manager > Administration**.

The Campus Administration window appears.

**Step 2** Select **Admin > Campus Data Collection**.

The Data Collection Settings Summary dialog box appears.

[Table 4-8](#) describes the fields that appear in the Data Collection Settings dialog box.

**Table 4-8 Data Collection Settings Summary**

| <b>Field</b>             | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VTP Domains              | VTP domains that are to be used as the filtering criteria for Data Collection.                                                                                                                                                                                                                                                                                                               |
| IP Address Range         | IP address range that is to be used as the filtering criteria for Data Collection.                                                                                                                                                                                                                                                                                                           |
| Poll Interval            | Periodicity for polling the network. Polling Interval is in the format HH:MM:SS, where HH is the hour; MM is the minutes; SS is the seconds.<br><br>Polling is done to see updated devices and link information without running Data Collection. The default poll interval is 2 hours. You can change this value in <b>Admin &gt; Campus Data Collection &gt; Schedule Data Collection</b> . |
| Data Collection Schedule | Click <b>View Details</b> to view the Data Collection Schedule details. You can add a new schedule and edit or delete existing schedules.                                                                                                                                                                                                                                                    |

## Modifying SNMP Timeouts and Retries

You can modify SNMP timeouts and retries using the **Campus Data Collection > SNMP Timeouts & Retries** option of the Admin tab in Campus Manager Administration window.

To modify SNMP timeouts and retries:

- 
- Step 1** Select **Campus Manager > Administration**.  
The Campus Manager Administration window appears.
- Step 2** Select **Admin > Campus Data Collection > SNMP Timeouts & Retries**.  
The SNMP Timeouts & Retries dialog box appears.  
Modify the SNMP settings as given in [Table 4-9](#).

**Table 4-9** *Modify Data Collection SNMP Timeouts and Retries*

| Field    | Description                                                                                                                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------|
| Target   | IP address of the target device. For example, 10.*.*.*                                                                                 |
| Timeouts | Time period after which the query times out. If Time out is increased, discovery time could also increase. Enter the value in seconds. |
| Retries  | Number of attempts. The allowed range is 0-8.                                                                                          |

**Step 3** Click **Add** to add SNMP settings.

**Step 4** Select a row and either:

- Click **Edit** to edit the timeouts and retries values.

Or

- Click **Delete** to delete the timeouts and retries values.

Click **OK** to save the changes or click **Cancel** to exit.

**Step 5** Click **Apply**.

## Scheduling Data Collection

You can schedule the day, time, and frequency of Data Collection and status polling using the **Campus Data Collection > Schedule Data Collection** option of the Admin tab in Campus Administration window.

To schedule Data Collection:

**Step 1** Select **Campus Manager > Administration**.

The Campus Manager Administration window appears.

**Step 2** Select **Admin > Campus Data Collection > Schedule Data Collection**.

The Schedule Data Collection dialog box appears.

**Step 3** Modify the Data Collection settings as described in [Table 4-10](#).

**Table 4-10 Data Collection Schedule Settings**

| Field                | Description                                                                                                                                                       | Usage Notes                                                                                                                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Poll Interval</b> |                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                 |
| Poll Interval        | Periodicity for polling the network. Polling Interval is in the format HH:MM:SS, where <i>HH</i> is the hour; <i>MM</i> is the minutes; <i>SS</i> is the seconds. | <p>Polling is done to see updated devices and link information without running Data Collection.</p> <p>Polling is enabled by default. The default poll interval is 2 hours.</p>                                                                                                                 |
| <b>Schedule</b>      |                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                 |
| Days, Hour, Min      | Days on which and the time at which Data Collection is scheduled.                                                                                                 | <p>The optimum Data Collection schedule depends on the size of the network and the frequency of network changes.</p> <p>The default Data Collection schedule is every 4 hours, on the 4-hour mark, daily: 04.00, 08.00, 12.00, 16.00, 20.00, 24.00 Note that time is in the 24-hour format.</p> |
| Recurrence Pattern   | Select the days of the week on which Data Collection is to be scheduled.                                                                                          | This field is available only when you are adding or editing a schedule.                                                                                                                                                                                                                         |

- Step 4** Select a schedule and click **Edit** to edit the schedule.
- Step 5** Select a schedule and click **Delete** to delete the schedule.
- Step 6** Click **Add** to add a new schedule.
- Step 7** Click **OK** to save the changes or click **Cancel** to exit.

### Best Practices

Be cautious while scheduling Data Collection:

- Data collection consumes significant resources on the network management system.
- Use the Polling option to see updated device and link status without running Data Collection.

## Setting up Data Collection Filters

You can specify VTP Domains and IP Address ranges for Data Collection using the **Campus Data Collection > Data Collection Filters** option in the Admin tab of Campus Manager Administration window.

To set up Data Collection filters:

- 
- Step 1** Select **Campus Manager > Administration**.  
The Campus Manager Administration window appears.
  - Step 2** Select **Admin > Campus Data Collection > Data Collection Filters**.  
The Data Collection Filter Settings dialog box appears.
  - Step 3** Click **Configure** to activate the filter.  
Corresponding filter window appears.
  - Step 4** Specify the Data Collection filters as described in [Table 4-11](#).

Table 4-11 Data Collection Filters

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                             | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filter Options</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| VTP Domain            | <p>Select this radio button and click <b>Configure</b> to limit Data Collection using VTP domains:</p> <ol style="list-style-type: none"> <li>From the drop-down list box, select either of these options: <ul style="list-style-type: none"> <li>Manage devices in specified VTP domains.</li> <li>Do not manage devices in specified VTP domains.</li> </ul> </li> <li>Enter the VTP domains that are to be used to limit Data Collection.</li> </ol> | <p>Specifying VLAN Trunk Protocol (VTP) boundaries prevents Data Collection from occurring outside of these boundaries.</p> <p>You can enter multiple VTP domains.</p> <p>You can only exclude or include domains; you cannot do both.</p> <p>For example, you cannot enter domains A and B to be included for Data Collection and domain C to be excluded.</p> <p>You can either include domains A and B, or exclude domain C.</p> <ol style="list-style-type: none"> <li>Click <b>Add</b> to add a VTP domain.</li> <li>Select a VTP domain and click <b>Delete</b> to delete the VTP domain.</li> <li>Click <b>OK</b> to save changes.</li> </ol> |

Table 4-11 Data Collection Filters (continued)

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Addresses | <p>Select this radio button and click <b>Configure</b> to limit Data Collection using IP addresses:</p> <ol style="list-style-type: none"> <li>1. From the drop-down list box, select <i>one</i> of these options: <ul style="list-style-type: none"> <li>– Manage devices in specified IP address range.</li> <li>– Do not manage devices in specified IP address range.</li> </ul> </li> <li>2. Enter an IP address or a range of IP addresses to limit Data Collection.</li> </ol> <p>Use standard IP addressing format (4 octets separated by periods) in which any octet can be:</p> <ul style="list-style-type: none"> <li>– IP address—Number between 0 and 255<br/>172.20.4.9</li> <li>– Wild card—Asterisk (*) denoting all numbers from 0-255, inclusive<br/>172.*.4.9</li> <li>– Range—[<i>begin-end</i>], where <i>begin</i> and <i>end</i> are numbers between 0-255 and <i>begin</i> is less than <i>end</i><br/>172.[4-55].4.9</li> </ul> | <p>Specifying IP address boundaries prevents Data Collection from occurring outside of these boundaries.</p> <p>The filter you set applies to the existing devices in Campus Manager server.</p> <p>You can only exclude or include IP addresses or ranges; you cannot do both.</p> <p>For example, you cannot enter IP addresses A and B to be included for Data Collection and IP address C to be excluded.</p> <p>You can either include IP addresses A and B, or exclude IP address C.</p> <ol style="list-style-type: none"> <li>1. Click <b>Add</b> to add an IP Address Range.</li> <li>2. Select an IP Address Range and click <b>Delete</b> to delete the IP Address Range.</li> <li>3. Click <b>OK</b> to save changes.</li> </ol> |

**Step 5** Click **OK** to start Data Collection or click **Cancel** to apply the changes and quit.

## Setting up Debugging Options for Data Collection

You can set the trace, and debugging, for Data Collection using the **Campus Data Collection > Debugging Options** option in the Admin tab of Campus Administration window.

To set the debugging options:

- 
- Step 1** Select **Campus Manager > Administration**.  
The Campus Administration window appears.
- Step 2** Select **Admin > Campus Data Collection > Debugging Options**.  
The Data Collection Debugging Options dialog box appears.  
Modify the debugging options as specified in [Table 4-12](#).

**Table 4-12** Data Collection Debugging Options

| Field                                | Description                                                            | Usage Notes                                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable Debug</b>                  |                                                                        |                                                                                                                                                          |
| Modules                              | Specify the modules on which debug is to be enabled.                   | Click <b>Select</b> to view the available modules and select the modules in which debug is to be enabled.<br>Select is enabled only if Debug is enabled. |
| File Name                            | Name of the log file in which the trace messages are to be recorded.   |                                                                                                                                                          |
| Maximum File Size (lines)            | Maximum size of the file in lines                                      |                                                                                                                                                          |
| <b>Enable Device Level Debugging</b> |                                                                        |                                                                                                                                                          |
| Device IP(s)                         | IP addresses of devices for which debugging messages are to be logged. | This field is enabled only when the device level debugging option is enabled.                                                                            |

- Step 3** Click **Apply**.
-

### Selecting Modules

Table 4-13 describes the debug modules available for Data Collection in Campus Manager.

**Table 4-13 Data Collection Debug Modules**

| Module    | Description                                                                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| framework | <ul style="list-style-type: none"> <li>Constructs and maintains data in the memory.</li> <li>Provides framework for Campus Manager features.</li> </ul> <p>Enable debugging for this module only when requested by TAC. This is because enabling debugging for this module creates huge logs.</p>                    |
| core      | <ul style="list-style-type: none"> <li>Provides basic device information</li> <li>Collects CDP information</li> </ul> <p>Enable debugging for this module if you encounter issues with basic device information such as CDP and manageability.</p>                                                                   |
| corex     | <p>Provides detailed Device Discovery, including modules and port information</p> <p>Enable debugging for this module if you encounter issues with modules, and port details.</p>                                                                                                                                    |
| topo      | <p>Provides network topology computation and layouts.</p> <p>Enable debugging for this module if you encounter issues with Topology computation of devices.</p> <p>In addition to topo, we recommend that you enable debugging for core and corex modules when you are troubleshooting Topology Services issues.</p> |
| vlan      | <ul style="list-style-type: none"> <li>Discovers VTP domains, VLANs, port-in-VLAN configurations</li> <li>Performs VLAN configuration tasks</li> <li>Determines Spanning Tree state</li> </ul> <p>Enable debugging for this module if you encounter issues with VTP, VLAN reports, and configuration.</p>            |

**Table 4-13 Data Collection Debug Modules (continued)**

| <b>Module</b>     | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccm               | <p>Discovers Cisco CallManager (CCM).</p> <p>Enable debugging for this module if you encounter issues with data collected for CCM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| vmppadmin         | <ul style="list-style-type: none"> <li>• Discovers end-user hosts on the network</li> <li>• Records end-user host information in the ANI database</li> <li>• Manages requests for scheduling user and host discoveries, ping sweeps, database queries, and updates to user and notes information</li> <li>• Provides subnet to VLAN mapping information to path service module</li> </ul> <p>Enable debugging for this module if you encounter issues with User Tracking.</p> <p>In addition to vmppadmin, we recommend that you enable debugging for core and corex modules when you are troubleshooting User Tracking issues.</p> |
| lane              | <ul style="list-style-type: none"> <li>• Discovers individual LANE components (LECS, LES/BUS &amp; LEC) for both Ethernet and Token Ring networks</li> <li>• Discovers LEC to VLAN index mapping (used for ATM-VLAN to VLAN mapping)</li> <li>• Determines logical ATM-VLANs from the discovered individual LANE components</li> <li>• Determines ATM-VLAN to Ethernet and Token Ring VLAN associations</li> </ul> <p>Enable debugging for this module if you encounter issues with LAN Emulation reports and configuration.</p>                                                                                                    |
| laneconfiguration | Performs LANE configuration tasks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 4-13 Data Collection Debug Modules (continued)**

| <b>Module</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                    |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dcrp          | <p>Provides computation of network discrepancies.</p> <p>Enable debugging for this module if you encounter issues in Discrepancy reports.</p> <p>In addition to dcrp, we recommend that you enable debugging for core and corex modules when you are troubleshooting Discrepancy Reporting issues.</p>                                |
| status        | <p>Enables status polling on previously discovered devices.</p> <p>Enable debugging for this module if you encounter issues with device and link status polling.</p>                                                                                                                                                                  |
| path          | <p>Determines the path between a pair of endpoints.</p> <p>Enable debugging for this module if you encounter issues in Path Tracing.</p> <p>In addition to path, we recommend that you enable debugging for core and corex modules when you are troubleshooting Path Tracing issues.</p>                                              |
| atm           | <p>Performs ATM-related configurations, such as:</p> <ul style="list-style-type: none"> <li>• SPVC provisioning</li> <li>• ATM RMON configuration and data polling</li> <li>• OamPing</li> <li>• ATM interface configuration</li> </ul> <p>Enable debugging for this module if you encounter issues in ATM reports and debugging.</p> |
| apps          | <p>Discovers application hosts such as MCS.</p> <p>Enable debugging for this module if you encounter issues with data collected on application hosts.</p>                                                                                                                                                                             |
| stp           | <p>Discovers all STP related information from the network.</p> <p>Enable debugging for this module if you encounter issues with STP reports and configuration.</p>                                                                                                                                                                    |

**Table 4-13 Data Collection Debug Modules (continued)**

| Module   | Description                                                                                                                                                                                                                                                            |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| stpeng   | <ul style="list-style-type: none"> <li>Performs STP configuration tasks</li> <li>Provides basic STP analysis for migration from one STP type to another</li> </ul> <p>Enable debugging for this module if you encounter issues with STP reports and configuration.</p> |
| frontend | <p>Provides framework for Campus Manager features. Enable debugging for this module only when requested by TAC. This is because enabling debugging for this module creates huge logs.</p>                                                                              |
| devices  | <p>Provides specific information, if any, available for device categories.</p> <p>Enable debugging for this module if you encounter issues specific to a particular device type.</p>                                                                                   |

Click **OK** to save the selected modules or click **Cancel** to exit.

## Using User Tracking Administration

You can perform administrative tasks using User Tracking Administration. For more details, see [Using User Tracking Administration, page 6-4](#).

## Understanding Groups

A Group can be thought of as a convenience view that allows you to view a subset of the entire network based on the group rule defined while creating the view.

These views, which are subsets of the Layer 2 views, can be accessed by a user or a set of users. These custom views are generated using a Campus Manager feature called Grouping Services, which helps manage groups of devices.

Grouping Services determines the membership of a group by interpreting and applying the rule associated with the group.

Hence, Topology Groups provides multiple benefits. It allows you to:

- Identify, and view a set of objects corresponding to a view.
- Create and manage views.
- Define convenience views which are a subset of the Layer 2 map.

See the following sections for a better understanding of Topology Groups concepts:

- [Concept of a Group, page 4-30](#)
- [Membership Update, page 4-43](#)
- [Rules Editor, page 4-36](#)

### Concept of a Group

A group is a named set of devices. The group is characterized by a set of properties such as a name, description, type, access permission, and so on. Most importantly, a group has an associated rule. The rule determines the membership of a group, which may change whenever the rule is evaluated.

Groups manage groups in a hierarchical organization and supports subgrouping. Two predefined top level parent groups are available when you install Campus Manager:

- [System Defined Groups, page 4-31](#)
- [User Defined Groups, page 4-31](#)

These groups are provided as a way to categorize groups at your site, and each of these contains a list of all the devices in the Campus Manager Database.

The Groups under **Administration > Groups** and that under **Topology Services > Topology Groups** follow the same hierarchy.

After you create a Group through **Administration > Groups**, you must reopen the Topology Services to view the changes.

By default, only the *admin* user has necessary privileges to create groups under System Defined Groups. However, the *admin* user can edit the group to provide write access to other users. Access permissions are maintained on a username basis, not a role basis.

If you possess appropriate permissions, you can create subgroups under groups. Hence, each child group is a subgroup of a parent group.

Note the following:

- The membership of a child group will be a subset of its immediate parent group.
- Changes in the properties of a parent group—Name, Rule, Evaluation Type, Access Permissions, impacts all child groups under it.
- When you remove a group, all child groups under it are also removed.
- When a user is removed from the Campus Manager list of users, the groups created by the user are not removed.

## System Defined Groups

A System Defined Group is a top-level container for standard groups that are accessible to and used by most Campus Manager users. By default, only the Campus Manager admin user has necessary privilege to create groups under the System Defined Groups folder.

A user must have write permission to a group in order to create a child group under it. Although by default, only the Campus Manager admin user has write permission to System Defined Groups, the admin user can grant write privilege to other users by editing the access permission to System Defined Groups.

A system administrator will typically define and configure their own System Defined Groups based on the partitioning requirements of the network.

The admin may choose to partition views based on any of the attributes that can be grouped. However, IP address, device name, sysLocation, and subnet will be common selections.

## User Defined Groups

A User Defined Group is a top-level container where individual Campus Manager users can create their own groups. Typically, the groups under User Defined Groups would be used and accessible to the user who created the group, and perhaps a small group of additional users, or these groups may be transient in nature.

For example, if Joe Smith wants to create a group that contains all devices where he is the System Contact, and he uses the following rule to form this group:

```
:Campus:OGS:Device.SystemContact equals "Joe Smith" OR
:Campus:OGS:Device.SystemContact equals "jsmith"
```

## Dynamic Group

A Dynamic group is a group for which the membership list is always up-to-date. Whenever you view a dynamic group, it always displays the latest group membership list.

## Static Group

A Static group is a group for which the membership is refreshed only when you explicitly request it. Between re-evaluations, the Group Server stores the membership list and group definition of the static group.

## Overview of Subnet Based Groups

Subnet based groups are automatically created when devices are managed. Subnet based groups help you work on smaller subsets of devices that are logically grouped. They are automatically deleted when all the devices in a subnet are deleted.

## Accessing Subnet Based Groups

From the CiscoWorks Homepage, select **Administration > Groups**.

This displays the Groups Administration and Configuration page. The Group Selector field will already have two names, System Defined Groups and User Defined Groups. The Subnet Based Groups are created under System Defined Groups.

## Understanding Subnet Based Groups

The Subnet based groups use the following name format:

```
Subnet -- Subnet Mask.
```

The rule expression has the following components:

```
Class.attribute operator "value"
```

For example,

```
:Campus:OGS:Device.IP.Subnet equals "172.20.104.192" AND
:Campus:OGS:Device.IP.SubnetMask equals "255.255.255.240"
```

The rule above will select all devices of subnet 172.20.104.192 and subnet mask 255.255.255.240.

## Creating Groups Based on Subnet

For example, the following rules might be used to create two groups based on the IP address subnet:

```
:Campus:OGS:Device.IP.Subnet equals "172.29.252.32"
:Campus:OGS:Device.IP.Subnet equals "172.29.252.64"
```

The examples provided here are simple; however the Grouping Service allows arbitrarily complex rules to be formed by combining rule expressions with AND, OR or the EXCLUDE operators. This gives the administrator the power and flexibility to create view partitions tailored to the needs of their site.

## Using Groups

From the CiscoWorks Homepage, select **Campus Manager > Administration > Topology Groups**. The Campus Manager Administration page appears.

The main tasks that you can perform using Topology Groups administration are:

- [Creating Groups, page 4-34](#)
- [Modifying Groups, page 4-43](#)
- [Viewing Group Details, page 4-44](#)
- [Recomputing Group Membership, page 4-45](#)

All actions begin from the Topology Groups administration page, unless otherwise specified.

Access control to groups is controlled on a username basis.

By default, read permission is granted to System Defined Groups, and read and write permissions are granted to User Defined Groups.

Usually, the admin user creates groups that are to be generally shared among users under the System Defined Groups folder. For example, the admin may wish to create device groupings based on IP address, subnet, location or contact.

The User Defined Groups folder is meant to hold a users private group and/or groups that are more transient in nature.

By default, read permission will be granted to System Defined Groups and read, write, and evaluate permissions will be granted to User Defined Groups.

## Creating Groups

You can create groups under System Defined Groups and User Defined Groups. This involves:

- [Creating Group Properties, page 4-34](#)
- [Creating Group Rule, page 4-39](#)
- [Creating Memberships, page 4-41](#)

## Creating Group Properties

Access to group creation is based on permission levels. You can create groups under User Defined Groups.

By default, only the CiscoWorks admin user can create groups under System Defined Groups; however, the admin user can modify the access permission to the System Defined Group to enable edit privilege (that is, create permission) to other Campus Manager user names.

To create Group Properties:

**Step 1** Select **Campus Manager > Administration > Groups**.

The Group Management window appears.

**Step 2** Click **Create**.

In the Properties: Create window that opens.

**Step 3** Enter the following details:

**Table 4-14** *Creating Properties Field Description*

| <b>Field</b>               | <b>Usage Notes</b>                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name                 | The group name should be unique within the parent group. However, it need not be so across groups. The same group name cannot be used in the same group hierarchy.                                                                                                                                                                                      |
| Copy Attributes from Group | <ol style="list-style-type: none"> <li>1. Click <b>Select Group</b> to copy attributes from a previously selected defined group.<br/>The Replicate Attributes dialog box appears.</li> <li>2. Select the devices from the Replicate Attributes dialog box.</li> <li>3. Click <b>OK</b> to select the devices or click <b>Cancel</b> to exit.</li> </ol> |
| Parent Group               | <ol style="list-style-type: none"> <li>1. Click <b>Change Parent</b> to change the parent group under which you want to define the group.</li> <li>2. Select the devices from the Select Parent window.</li> <li>3. Click <b>OK</b> to select the devices or click <b>Cancel</b> to exit.</li> </ol>                                                    |
| Description                | You can enter a detailed description of the group identifying its characteristics in this field.                                                                                                                                                                                                                                                        |

**Table 4-14** *Creating Properties Field Description (continued)*

| Field             | Usage Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Membership Update | <p>Select a membership update mode.</p> <ul style="list-style-type: none"> <li>• Automatic—The membership of the group is automatically recomputed each time the group is invoked.</li> <li>• Only Upon User Request—The membership of the group is recomputed only when an explicit request is made, using the Refresh option.</li> </ul> <p>If you select Automatic, the group will be a Dynamic group.</p> <p>If you select Only Upon User Request, the group will be a Static group.</p> |
| Visibility Scope  | <p>Select the mode of visibility.</p> <ul style="list-style-type: none"> <li>• Private</li> <li>• Public</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |

**Step 4** Click **Next**.

The Rules window appears. For entering the details in the Rules: Create dialog box, see [Creating Group Rule, page 4-39](#).

## Rules Editor

Every group is defined by a set of rules. You may select an item from the drop-down menus, enter a rule in the free-form **Rule Text** area, or use a combination of the two.

A rule set contains a Boolean combination of individual rule expressions. A rule expression is made of the following components:

### Object type

The type of devices which form the group. Rules are evaluated on the list of devices discovered. Campus Manager supports only one object type:

: Campus : OGS : Device

### Variable

Any of the attributes of a device. The following variables are available:

- DiscoveryStatus
- HostName
- ImageVersion
- IP.Subnet
- IP.SubnetMask
- SingleIpAddress
- SysName
- SysObjectID
- SystemContact
- SystemLocation

### Operator

The operator used in forming a rule. The following operators are available:

- equals
- contains

When the variable *DiscoveryStatus* is used, only one operator is available, which is, = (equals sign).

### Value

A free flow operand forming the last part of the rule.

When the variable *DiscoveryStatus* is used, only the following values are available:

- Never\_Reachable
- Reachable
- Currently\_Unreachable

## Example of Rule

Let us consider a scenario where you need to define a rule for a set of devices in the State Street Campus. The Campus Manager has devices at two locations: Bldg 1 Devices and Bldg 2 Devices.

In this scenario, we will create rules for the System Defined Groups and the User Defined Groups.

### Rule for a System Defined Group

- To create a System Defined Group whose member devices are located in Bldg. 1 Devices, the group rule is:

```
:Campus:OGS:Device.SystemLocation equals "Bldg 1 Devices"
```

where

Variable is *SystemLocation*

Operator is *equals*

Value is Bldg 1 Devices

- Similarly, to create a System Defined Group whose member device IP addresses is 172.20.121.10, the group rule is:

```
:Campus:OGS:Device.IpAddress equals "172.20.121.10"
```

In addition you can use the *contains* operator to match a value anywhere in the attribute:

```
:Campus:OGS:Device.IpAddress contains "10"
```

The above rule, will match devices with IP address like 172.20.10.3, 172.25.3.101 etc.

### Rule for a User Defined Group

- To create an User Defined group whose member devices are labelled *Lab Test Setup*, the group rule is:

```
:Campus:OGS:Device.DeviceLabel equals "Lab Test Setup"
```

where

Variable is *DeviceLabel*

Operator is *equals*

Value is *Lab Test Setup*

- Similarly, to create an User Defined group whose member devices have a common system contact person, *J Smith Devices*, the group rule is:

```
:Campus:OGS:Device.DeviceLabel equals "J Smith Devices"
```

### A Composite Rule

A Boolean set of such rules form a composite rule. In the example, to create a group whose member devices are labelled *Lab Test Setup*, have a common system contact person, *J Smith Devices*, the composite rule is:

```
:Campus:OGS:Device.DeviceLabel equals "Lab Test Setup" AND
:Campus:OGS:Device.SystemContact equals "J Smith Devices"
```

## Creating Group Rule

After entering the details for creating properties for the Group, you must create rules for the Group. To create rules for the Group, either you must use the parameters specified, or manually enter the rule text.

To create rules using parameters:

**Step 1** In the Rules window, enter the details in the Rule Expression area.

[Table 4-15](#) describes the fields in the Rule Expression area.

**Table 4-15 Rules: Create Field Description**

| Field       | Description                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —           | Select the Boolean expression. <ul style="list-style-type: none"> <li>• OR</li> <li>• AND</li> <li>• EXCLUDE</li> </ul>                                                                                                                                                                                                                                                                                   |
| Object Type | The type of devices that form the group. Rules are evaluated on the list of devices discovered.<br><br>Campus Manager supports only one object type:<br>:Campus:OGS:Device                                                                                                                                                                                                                                |
| Variable    | Attribute of a device. The available variables are: <ul style="list-style-type: none"> <li>• DiscoveryStatus</li> <li>• HostName</li> <li>• ImageVersion</li> <li>• IP Subnet</li> <li>• IP SubnetMask</li> <li>• SingleIpAddress</li> <li>• SysName</li> <li>• SysObjectID</li> <li>• SystemContact</li> <li>• SystemLocation</li> </ul> For more details, see <a href="#">Rules Editor, page 4-36</a> . |

**Table 4-15 Rules: Create Field Description (continued)**

| Field    | Description                                                                                                                                                                                                                                                                                                                                                  |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operator | <p>Operator used in forming a rule. The available operators are:</p> <ul style="list-style-type: none"> <li>• equals</li> <li>• contains</li> </ul> <p>When you use the variable SingleIpAddress, only one operator is available: <b>equals</b></p> <p>When the variable DiscoveryStatus is used, only one operator is available:</p> <p>= (equals sign)</p> |
| Value    | Enter the desired value for the variable you have selected.                                                                                                                                                                                                                                                                                                  |

**Step 2** Click **Add Rule Expression**.

The Rule Text field shows the rule you are creating.

You can also enter the rules directly in the Rule Text field.

**Step 3** Click **Check Syntax** to validate the rules syntax entered.**Step 4** Click **View Parent Rules** to view rules defined for the parent Groups.**Step 5** Click **Next** to create Memberships to specify the devices available to the group.

For entering details for creating Memberships, see [Creating Memberships, page 4-41](#).

## Creating Memberships

You can create memberships to specify the devices available to the group. The devices appear in Available Objects From Parent Group or Objects Matching Membership Criteria, based on the properties and rules you specified in the previous steps.

Available Objects From Parent Group is the set of objects in the parent group not selected by the child group's rule.

To add the selected devices from the Available Objects From Parent Group list to the Objects Matching Membership Criteria list:

**Step 1** Select one or more IP addresses of the devices from the Available Objects From Parent Group list on the left pane.

**Step 2** Click **Add**.

The devices appear in Objects Matching Membership Criteria list, based on the properties and rules you specified in the previous steps.

If you want to remove devices from the Objects Matching Membership Criteria list, select the device from the list of Objects Matching Membership Criteria, and click **Remove**.

**Step 3** Click **Next** to view the summary of the details of the newly created group.

[Table 4-16](#) describes the entries in the Summary: Create table.

**Table 4-16** *Create Group Summary Entry Description*

| Entry             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Name        | Name of the Group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Parent Group      | Name of the Parent Group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Description       | Description for the Group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Membership Update | <p>Select a membership update mode.</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b>—The membership of the group is automatically recomputed each time the group is invoked.</li> <li>• <b>Only Upon User Request</b>—The membership of the group is recomputed only when an explicit request is made, using the Refresh option.</li> </ul> <p>If you select Automatic, the group will be a Dynamic group.</p> <p>If you select Only Upon User Request, the group will be a Static group.</p> |
| Rules             | Rule you entered for the Group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Visibility Scope  | Visibility scope that you selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 4** Click either:

- **Finish** to create the Group,

or

- **Cancel** to exit the wizard and go back to the Group Management window.
- 

## Membership Update

The membership of a group is governed by the rule associated with a group. The changes in the membership is reflected in the Network Topology View of the group. To view a topology view, select **Campus Manager > Topology Views**.

Moreover, while groups with evaluation type Automatic have membership that is current, groups with evaluation type Only Upon User Request retain the membership at creation time or on subsequent re-evaluation.

Two modes of membership updates are available:

- Automatic

The membership of a group is recomputed automatically on a periodic basis.

If the node or view has been displayed, you must close all of Topology Services and re-open it to display the revised group membership.

- Only Upon User Request

The membership of the group is recomputed only when an explicit request is made, using the Refresh option. For more information on the Refresh option, see [Recomputing Group Membership, page 4-45](#).

## Modifying Groups

You can modify most attributes of a group in the edit mode, except the parent group.

To modify groups:

---

**Step 1** Select a group, and click **Edit**.

You can modify the Group Name, Description, and Membership Update Type.

**Step 2** Click **Next**.

- To modify group rule, edit the rule either using the **Rule Expression** fields or edit the rule in the Rule Text field and Click **Next**.
- To add or remove devices from the Objects in Group, click **Add** or **Remove**, as appropriate and Click **Next**.
- To modify access permissions, select the access levels in the Permission field and Click **Next**.

**Step 3** Click **Finish** to save the modified groups.

---

## Viewing Group Details

To view the attributes of a group:

---

**Step 1** Select **Campus Manager > Administration > Groups**.

**Step 2** Select a group.

Group information is displayed in the right window.

- To view detailed attributes for the group, click **Details**.
  - To view the rules attributes of the parent group, click **View Parent Rules**.
  - To view the list of devices in the group, click **Membership Details**.
- 

## Deleting a Group

You can delete a group and all child groups under it.

To delete a group:

---

**Step 1** Select **Campus Manager > Administration > Groups**.

The Group Management window appears.

**Step 2** Select a group.

**Step 3** Click **Delete** to remove the group.

**Step 4** Click **Yes** to confirm.

The selected group is deleted.

---

## Recomputing Group Membership

You can re-evaluate and re-apply the rules of a group to recompute the membership of groups.

To recompute group membership:

---

**Step 1** Select **Campus Manager > Administration > Groups**.

**Step 2** Select a group.

**Step 3** Select **Refresh** to recompute the membership of the group.

**Step 4** Click **Yes** to confirm.

The group membership is recomputed.

---

## Configuring Discrepancy Reporting and Syslog Message Generation

You can customize the Discrepancy Report to display only those discrepancies about which you want to be notified.

To customize the reports:

---

**Step 1** Select **Campus Manager > Administration > Network Discrepancies**.

The Configuring Network Discrepancies window appears.

- To include a discrepancy in the Discrepancy Reports, check the box next to it. Checking all the boxes results in a report displaying all discrepancies in the network.

- To exclude a discrepancy from the Discrepancy Reports, uncheck the box.
- Step 2** Select the **Configure Syslog** check box and click **Next**.  
The list of selected discrepancies appears.
- Step 3** Select the **Send Syslogs** check box and enter the name of the server in the Syslog Server field.
- Step 4** Select the discrepancies for which you want to generate syslog messages and click **Next**.  
A summary of the selected discrepancies appears.
- Step 5** Click **Finish**.
- 

You can use the filters to display discrepancy reports for specific devices, link or network types. This makes it easy to find a particular discrepancy for a particular type.

You can use more than one filter at the same time, but results will vary.

- If you select more than one filter in the same top-level category, Boolean OR is used.  
For example, if you select Duplex, Speed under Link, any link or port that fulfils at least one filter criteria will be displayed in the report.
- If you select more than one filter from different top-level categories, Boolean AND is used.  
For example, if you select both a Link type and a Port type filter from the Physical discrepancy filter, any link that fulfils both filter criteria will appear in the report.

## Scheduling Jobs for Path Analysis

You can configure scheduling of Path Analysis traces using the Schedule Path Analysis window. To do this:

- 
- Step 1** Select **Administration > Admin > Schedule Path Analysis**.  
The Schedule Path Analysis window appears.
- Step 2** See [Table 4-17](#) to interpret the fields in the Scheduled Jobs table.

**Table 4-17** *Scheduled Jobs Column Description*

| <b>Column Name</b> | <b>Description</b>                                                     |
|--------------------|------------------------------------------------------------------------|
| JobID              | Unique Job ID of the job                                               |
| JobName            | Name of the job                                                        |
| Source             | Source of the path trace (either IP address or valid domain name)      |
| Destination        | Destination of the path trace (either IP address or valid domain name) |
| UserName           | Owner of the job                                                       |
| Schedule           | Start time and frequency at which the job is to be repeated            |
| TimeOut            | Timeout value for the path trace                                       |
| Traces             | Number of traces                                                       |
| Run Status         | Result of the previous run of the job                                  |
| Last Run Time      | Start and end time for the previous run of the job                     |

**Step 3** Click **Add**.

The Add Schedule dialog box appears.

**Step 4** Select Run Type as **Immediate** if you want the job to start immediately.

After a job is scheduled, it will start immediately, with the default settings.

**Step 5** Select Run Type as **At** if you want to specify the date and periodicity for the job.

**Step 6** Enter the Job Info details as specified below:

| <b>Field Name</b> | <b>Description</b>                                                     |
|-------------------|------------------------------------------------------------------------|
| Job Name          | Job name                                                               |
| Source            | Source of the path trace (either IP address or valid domain name)      |
| Destination       | Destination of the path trace (either IP address or valid domain name) |

| Field Name         | Description                                   |
|--------------------|-----------------------------------------------|
| Timeout (minutes)  | Timeout value for path traces in minutes      |
| Number of Archives | Number of archives should be between 1 and 50 |

**Step 7** Click **Apply** to set the periodic schedule.

- To edit scheduled jobs, select a scheduled job and click **Edit**.
- To delete scheduled jobs, select a scheduled job and click **Delete**.
- To get updates on scheduled jobs, Click **Refresh**.

## Displaying Scheduled Traces

You can view traces, scheduled using Path Analysis. However, you will be able to view only completed traces.

See [Table 4-18](#) to interpret the fields in the View Scheduled Traces dialog box.

**Table 4-18** *Interpreting View Scheduled Traces Fields*

| Field          | Description                                  |
|----------------|----------------------------------------------|
| Job Name       | Name of the job that has been scheduled      |
| Source         | IP address of the source                     |
| Destination    | IP address of the destination                |
| Execution Time | Time at which the job gets executed          |
| Status         | Whether the trace was successfully completed |

To view the scheduled traces, select **Edit > View Scheduled Traces** from the menu bar in the Path Analysis Main Window.

The View Scheduled Traces dialog box appears. You can select a job from the Trace List in the View Scheduled Traces dialog box

- To view a scheduled trace, click **View**.
- To delete the job name entry from the Trace List, click **Delete**.
- To see the updated list of scheduled traces, click **Refresh**.

## Using Administration Reports

You can view an analysis of the ANI Server, details of devices discovered, Data Collection metrics, and list of devices supported using the Reports tab of Campus Manager Administration window.

### Analyzing ANI Server

You can analyze the ANI server for its performance using the Analyze ANI Server option in the Reports tab of Campus Manager Administration window.

To analyze the ANI server:

- 
- Step 1** Click **Campus Manager > Administration**.  
The Campus Manager Administration window appears.
  - Step 2** Click **Reports**.  
The Reports dialog box appears.
  - Step 3** Choose ANI Server and click **Generate Report**.  
The ANI Server details appear.
- 

### Viewing Details of Discovered Devices

You can view details of devices discovered using the Discovery Report option in the Reports tab of Campus Manager Administration window.

To view the details of devices discovered:

- 
- Step 1** Select **Campus Manager > Administration**.  
The Campus Administration window appears.
  - Step 2** Click **Reports**.  
The Reports dialog box appears.
  - Step 3** Select **Discovery Report**.

**Step 4** Select **All Devices**, **Reachable Devices**, or **Unreachable Devices** from the Report Type list.

**Step 5** Click **Generate Report**.

The details of the discovered devices appear.

[Table 4-19](#) describes the columns of the Device Discovery Report.

**Table 4-19** *Device Discovery Report*

| <b>Field</b> | <b>Description</b>                                    |
|--------------|-------------------------------------------------------|
| Type         | Type of the discovered device.                        |
| OID          | sys Object ID of the device.                          |
| IP Address   | IP address of the discovered device.                  |
| Host Name    | Host name of the discovered device.                   |
| Neighbors    | IP address of the neighbors of the discovered device. |
| Status       | Status of the discovered device.                      |

## Viewing Data Collection Metrics

You can view the Data Collection metrics using the Data Collection Metrics option in the Reports tab of Campus Manager Administration window.

To view the Data Collection metrics:

**Step 1** Select **Campus Manager > Administration**.

The Campus Manager Administration window appears.

**Step 2** Click **Reports**.

The Reports dialog box appears.

**Step 3** Select **Data Collection Metrics**.

**Step 4** Enter the number of Data Collection cycles for which data is to be archived and click **Apply**.

**Step 5** Click **Generate Report**.

The Data Collection metrics appear.

[Table 4-20](#) describes the columns of the Data Collection Metrics report.

**Table 4-20 Data Collection Metrics**

| <b>Field</b>     | <b>Description</b>                                                                                                               |
|------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Start Time       | Time at which Data Collection was started.                                                                                       |
| Percent Complete | Percentage of Data Collection that has been completed.                                                                           |
| End Time         | Time at which Data Collection was completed.                                                                                     |
| Total Time       | Total time taken for Data Collection.                                                                                            |
| Total Devices    | Total number of devices from which data was collected. When you click on the hyperlink, the Data Collection Detail page appears. |
| New Devices      | Number of devices from which data was collected. When you click on the hyperlink, the Data Collection Detail page appears.       |
| Devices Deleted  | Number of devices that were deleted.                                                                                             |
| Devices Per Hour | Number of devices in each hour for which data was collected.                                                                     |
| Objects Per Hour | Number of objects in each hour for which data was collected.                                                                     |

## Viewing Data Collection Details

The Data Collection Metrics report displays the number of devices and the new devices for which data was collected during the Data Collection cycle.

You can click on the hyperlink in the Total Devices field and the New Devices field in the report to view the Data Collection Detail page.

[Table 4-21](#) describes the fields in the Data Collection Detail page.

**Table 4-21 Data Collection Detail**

| Field      | Description                                                                       |
|------------|-----------------------------------------------------------------------------------|
| IPAddress  | IP address of the device for which data is collected                              |
| HostName   | Host name of the device for which data is collected                               |
| DeviceType | Type of the device for which data is collected - the device family it belongs to. |
| Neighbors  | Host names of the neighboring devices                                             |

## Viewing List of Devices Supported

You can view the icon, name and object ID of the supported devices using the Device Support option in the Reports tab of Campus Manager Administration window.

To view the supported devices supported:

---

**Step 1** Select **Campus Manager > Administration**.

The Campus Administration window appears.

**Step 2** Click **Reports**.

The Reports dialog box appears.

**Step 3** Select **Device Support** and click **Generate Report**.

The details of supported devices appear.

[Table 4-22](#) describes the columns of the Devices Supported report.

**Table 4-22** *Devices Supported Report*

| Field | Description                 |
|-------|-----------------------------|
| Icon  | Icon of the device.         |
| Name  | Name of the device.         |
| OID   | sysObject ID of the device. |

## Administration Command Line Interface

### Replacing Corrupted Database

If you have a corrupted database, you can use the database administration tools to restore the database from a previous backup. However, if you do not have a previous backup, you must re-initialize the database.

When you run this command, if Data Collection is running, it is automatically stopped and then restarted when the database initialization is complete.



#### Caution

If you re-initialize the database, information from discovered devices will be lost. However, user and host information is retained. Replace the database only if recommended by a Cisco technical representative.



#### Note

Your login determines whether you can use this option.

### Re-initializing the database

From the command prompt or shell window, enter:

- On Solaris: `NMSROOT/campus/bin/reinitdb.pl`
- On Windows: `perl NMSROOT\campus\bin\reinitdb.pl`

This will erase all data from the database. Are you sure [y/n] ?

If you enter **y**, it erases all data (database tables Wbu\*...) from the server.

**Erasing data for user tracking and phone tracking, and restarting the server**

- On Solaris: `NMSROOT/campus/bin/reinitdb.pl -ut`
- On Windows: `perl NMSROOT\campus\bin\reinitdb.pl -ut`

**Restoring the Original data in the server**

- On Solaris: `NMSROOT/campus/bin/reinitdb.pl -restore`
- On Windows: `perl NMSROOT\campus\bin\reinitdb.pl -restore`

where *NMSROOT* is the root directory where you installed CiscoWorks.

**Note**

Before executing the `-restore` command, you should stop the daemon manager and start again manually. For details, see [Using Daemon Manager](#).

## Deleting Devices

The Delete Device command is used to delete a device managed by Campus Manager from its server.

**Usage**

```
DeleteDevice -host hostname -port portnumber -secure -log logfile -device
devices -file filename -u unreachable devices -user username -password
password
```

## Configuration Settings for SNMPv3 Devices

For using various Campus Manager features in devices running SNMPv3, you must make specific configurations on the devices. The commands that you need to configure are:

**Configuring MIB views**

For Catalyst devices, enter the following command:

```
set snmp view campusview 1.3.6.1 included nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server view campusview oid-tree included
```

### Setting access rights

You must set the access rights for a group with a certain security model in different security levels.

For Catalyst devices, enter the following command:

```
set snmp access campusgroup security-model v3 authentication read
campusview write campusview nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server group campusgroup v3 auth read campusview write campusview
access access-list
```

### Configuring a new user

For Catalyst devices, enter the following command:

```
set snmp user campususer authentication md5
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3 auth md5 password1
```

### Configuring password for a user

For Catalyst devices, enter the following command:

```
set snmp user campususer authentication md5 password1
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3 auth md5 password1
```

### Relating a user to a group

Using a specified security model you can relate a user to a group.

For Catalyst devices, enter the following command:

```
set snmpw group campusgroup user campususer security-model v3
nonvolatile
```

For IOS devices, enter the following command:

```
snmp-server user campususer campusgroup v3
```

# Security

After a period of inactivity, the CiscoWorks Homepage times out and is no longer accessible. Close all browser instances and relaunch CiscoWorks.

## Frequently Asked Question

- Q.** I have an office with 300 remote branches each with a Cisco router. The routers are connected to the head office over an SP infrastructure and IPSec is used to encrypt the traffic between the remote branches and the head office. How do I manage the devices in the remote network using Campus Manager?
- A.** If you want to discover and manage the devices in the remote network, add those as seed devices in Campus Manager.