CHAPTER 2

Setting up Prime Infrastructure

After you install Prime Infrastructure and launch the browser, read the following sections to learn how to get started using Prime Infrastructure:

Discovering the Network

To view and manage the devices in your network, Prime Infrastructure must first discover the devices and, after obtaining access, collect information about them. Prime Infrastructure uses both SNMP and SSH/Telnet to connect to supported devices and collect inventory data.

The following sections describe how to discover your network:

Planning Discovery Runs

Prime Infrastructure uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime Infrastructure uses the seed device you specify to discover the devices in your network.

Before you run discovery, you must do the following:

1. Configure SNMP Credentials on Devices—Prime Infrastructure uses SNMP polling to gather information about your network devices. You must configure SNMP credentials on all devices you want to manage using Prime Infrastructure.
2. Set Syslog and Trap Destinations on Devices—Specify the Prime Infrastructure server (using the Prime Infrastructure server IP address and port) as the syslog and trap destination on all devices you want to manage using Prime Infrastructure.
3. Configure discovery email notifications—You will then receive email notification when Prime Infrastructure has completed discovering the devices in your network. See Configuring Discovery Email Notifications.

Configuring Discovery Email Notifications

By configuring mail server settings, you will receive e-mail notification when Prime Infrastructure has completed discovering the devices in your network.

Step 1 Choose **Administration > System Settings > Mail Server Configuration**.

Step 2 Enter the required information, then click **Save**.

Note The e-mail addresses you provide for the recipient serve as the default value for other functional areas, such as alarms or reports. Any global changes you make to the recipient e-mail addresses are disregarded if you set up e-mail notifications.

Running Discovery

When you run discovery, Prime Infrastructure discovers the devices and, after access is obtained, collects device inventory data.

It is recommended that you run discovery when first getting started with Prime Infrastructure, as shown in the following steps:

Step 1 Choose **Operate > Discovery**, then click **Discovery Settings**.

Step 2 Click **New**.

Step 3 Enter the Protocol Settings as described in Table 2-1.

Step 4 Do one of the following:

- Click **Save** to save your discovery settings and schedule your discovery to run at a specified time.
- Click **Run Now** to run the discovery now.

Table 2-1 Discovery Protocol Settings

Field	Description
Protocol Settings	
Ping Sweep Module	Gets a list of IP address ranges from a specified combination of IP address and subnet mask. This module pings each IP address in the range to check the reachability of devices.
CDP Module	The discovery engine reads the cdpCacheAddress and cdpCacheAddressType MIB objects in cdpCacheTable from CISCO-CDP-MIB on every newly encountered device as follows: 1. The cdpCacheAddress MIB object is gathered from the current device. This provides a list of neighbor device addresses. 2. If the neighbor device addresses do not already exist in the global device list, they are added to the local cache.
Advanced Protocols	
Routing Table	Queries and analyzes routing tables on seed routers to discover subnets and next-hop routers.
Address Resolution Protocol	The ARP Discovery Module depends on the Routing Table Discovery Module (RTDM), and is executed only when RTDM is processed. This precondition is identified based on the Discovery-module-processed flags, which are part of the DeviceObject. The entries coming out of the ARP Discovery Module need not necessarily pass through RTDM because (per the router Discovery algorithm) active routers are those that RTDM must process and identify. When the ARP table is fetched and the entries are not already discovered by RTDM, then these entries (though they may represent routers) are not active routers and need not be passed on to RTDM. This is ensured by setting the ARP Discovery Module flag to Processed and leaving the RTDM flag set to Unprocessed. When the RTDM comes across an entry with the RTDM flag unset and the ARP flag set, RTDM identifies the entry as a inactive router or other device and it leaves the entry as Unprocessed. The ARP Discovery Module also ignores the entry according to the algorithm, based on the Processed flag set against the ARP Discovery Module. When the ARP Discovery module is checked, the device MAC address needs to be updated in the device information. Applications can retrieve this information in the adapter through the DeviceInfo object. By scanning the device MAC address, the applications can distinguish between Cisco and non-Cisco devices. ARP cache from the device is collected using CidsARPInfoCollector. The MAC ID of the device is retrieved from this data and set in the DeviceInfo object.
Border Gateway Protocol	The BGP Discovery Module uses bgpPeerTable in the BGP4-MIB to find its BGP peer. The table contains its peers' IP addresses, which are added as clues to the local cache.
OSPF	Open Shortest Path First (OSPF) protocol is an interior gateway routing protocol. OSPF discovery uses the ospfNbrTable and ospfVirtNbrTable MIB to find neighbor IP addresses.
Filters	
System Location Filter	Filters the device based on the Sys Location string set on the device during the discovery process.
Advanced Filters	
IP Filter	Filters the device based on the IP address string set on the device during the discovery process.

Field	Description
System Object ID Filter	Filters the device based on the System Object ID string set on the device during the discovery process.
DNS Filter	Filters the device based on the DNS string set on the device during the discovery process.
Credential Settings	
SNMP V2 Credential	SNMP community string is a required parameter for discovering devices in the network. You can enter multiple rows of credentials mapped to a specific IP address, or the IP address can be a wild card; for example, *.*.*.*, 1.2.3.*.
Telnet Credential	You can specify the Telnet credentials during discovery, setting creation to collect the device data.
SSH Credential	Prime Infrastructure support SSH V1 and V2. You can configure SSH before running discovery.
SNMP V3 Credential	Prime Infrastructure supports SNMP V3 discovery for devices.

Verifying Discovery

When discovery has completed, you can verify that the process was successful by following these steps:

Step 1 Choose **Operate > Discovery**.

Step 2 Choose the discovery job for which you want to view details.

Step 3 Under Discovery Job Instances, expand the arrow to view details about the devices that were discovered.

If devices are missing:

- Change your discovery settings, then rerun the discovery. See Table 2-1for information about discovery settings.
- Add devices manually. See Adding Devices Manually for more information.

Adding Devices Manually

You can add devices manually, as shown in the following steps. This is helpful if you want to add a single device. If you want to add all of the devices in your network, it is recommended that you run discovery. (See Running Discovery for more information.)

Step 1 Choose **Operate > Device Work Center**, then click **Add**.

Step 2 Enter the parameters.

Step 3 Click **Add** to add the device with the settings you specified.

Importing Devices in Bulk

If you have another management system into which your devices are imported or if you want to import a spreadsheet that contains all of your devices and their attributes, you can import device information in bulk into Prime Infrastructure.

Step 1 Choose **Operate > Device Work Center**, then click **Bulk**.

Step 2 Click the link to download a sample file that contains all the fields and descriptions for the information that must be contained in your imported file.

Step 3 Click **Browse** to navigate to your file, then click **Import**.

Step 4 To view the status of the import, choose **Administration > Jobs Dashboard**.

Step 5 Click the arrow to expand the job details and view the details and history for the import job.

Adding NAM HTTP Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you will need to add HTTP credentials so that Prime Infrastructure can retrieve data from them. This is especially important for users who have licensed Assurance features, as most Assurance features depend on NAM data to work.

Prime Infrastructure polls NAMs directly, via HTTP (or HTTPS) to collect their data. This type of polling requires Prime Infrastructure to store each NAMs' HTTP credentials. Unlike with SNMP community strings and Telnet/SSH credentials, you cannot enter NAM HTTP credentials during the discovery process. You can only specify NAM HTTP credentials after the modules are discovered or added to inventory.

Follow the steps below to add HTTP credentials for a single NAM. You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

Step 1 Choose **Operate > Device Work Center > Device Type > Cisco Interfaces and Modules > Network Analysis Modules**.

Step 2 Select one of the NAMs and click **Edit.**

Step 3 In the **Edit Device** window, under **Http Parameters**:

- Protocol—Select the HTTP protocol, HTTP or HTTPS. The TCP Port will change automatically to the default port for the protocol you selected.
- TCP Port—Enter a different TCP Port if you want to override the default.
- Username—Enter the name of a user who can access the NAM via HTTP or HTTPS.
- Password—Enter the password for the user name you entered.
- Confirm Password—Re-enter the password to confirm.

Step 4 Choose **Update**.

Related Topics

- Setting Up Assurance

Setting Up Site Profiles

Site profiles help you manage large campuses by associating network elements to physical locations. Site profiles have a hierarchy that includes campuses and buildings, and allows you to segment the physical structure of your network and monitor your network based on location.

There are two areas in which you can set up and change sites:

- **Design > Site Map Design**—Create a new site and change an existing site.
- **Operate > Device Work Center**—If a site has previously been created, you can add devices to a site by clicking **Add to Site** from the Device Work Center.

When you create site profiles, you need to decide how many campuses and buildings to include in your site. Table 2-2 explains how to determine which elements to include in your site profiles.

Table 2-2 Creating Elements in Site Profiles

Create a ...	When you have ...
Campus	More than one business location
Building	More than one location within your campus

To control which users have access to the devices in the sites, you need to create virtual domains. See Setting Up Virtual Domains for more information.

For additional information about sites, see Designing Sites.

Creating Site Profiles

To create a campus location, add a building to the campus:

Step 1 Choose **Design > Site Map Design**.

Step 2 From the command menu, choose **New Campus**, then click **Go**.

Step 3 Enter the necessary parameters, then click **Next**.

Step 4 Change any settings, then click **OK**.

Step 5 Click the campus you just created; then, from the command menu, choose **New Building**, and then click **Go**.

Step 6 Enter the necessary parameters, then click **Save**.

You can now add devices to the site profile as described in Adding Devices to Site Profiles.

Adding Devices to Site Profiles

After you have created site profiles, you can assign devices to those sites. By associating devices with a campus and building, you can simplify maintenance tasks. When you need to perform maintenance tasks on devices, you can choose the site that contains the devices and apply the changes to all devices in the site.

To control which users have access to the devices in the sites, you need to create virtual domains. See Setting Up Virtual Domains for more information.

Step 1 Choose **Operate > Device Work Center**.

Step 2 Choose the devices you want to add to a site, then click the **>>** icon and click **Add to Site**.

Step 3 Choose the campus and building to which to assign the device, then click **Add**.

Note The Campus and Building fields are populated with the settings you previously entered in **Design > Site Map Design**. See Creating Site Profiles for more information.

Setting Up Port Monitoring

To monitor your device ports, you can create a port group and then display monitoring information on the Prime Infrastructure dashboard.

Port Groups

Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

After you create port groups, you can more efficiently configure all the devices belonging to a port group.

You need to determine which types of ports you want to monitor as a group. The following port groups are typical of most networks:

- Port Type
- User Defined
- WAN Interfaces

Monitoring Templates

Monitoring templates monitor device features, usage, health, and other factors. After you create and deploy monitoring templates, Prime Infrastructure collects and processes data from specified devices and displays the information in dashboards, dashlets, and reports. See Setting Up WAN Interface Monitoring.

Setting Up WAN Interface Monitoring

You create a WAN interface port group in order to efficiently configure settings on all the WAN interfaces in a specific port group.

The following steps show you how to create a port group for the WAN interfaces for an edge router, create and deploy a WAN interface health monitoring template on those ports, and then view the results.

Step 1 Choose **Design > Port Grouping**.

Step 2 Choose device IP addresses to add to the WAN interfaces port group, then click **Add to Group**.

Step 3 From the Select Group drop-down menu, choose **WAN Interfaces**, then click **Save**.

Step 4 Create a WAN interface health monitoring template:

a. Choose **Design > Monitoring**.

b. Choose **Features > Metrics > Interface Health**.

c. Enter the parameters for the interface health template. It is recommended that you check all parameters to be monitored for WAN interfaces.

d. Click **Save as New Template**.

Step 5 Deploy the template:

a. Choose **Deploy > Monitoring Tasks**.

b. Choose the template you created, then click **Activate**. Click **OK** to confirm.

c. Choose the template you created, then click **Deploy**.

d. Choose Port Groups, then click WAN Interfaces.

e. Click **Submit**.

Step 6 Verify the monitoring results:

a. Choose **Operate > Overview > General**.

b. Check the Top N Interfaces by WAN Utilization dashboard for the parameters you specified.

Related Topic

- Changing Port Groups

Setting Up Virtual Domains

Virtual domains allow you to control who has access to specific sites and devices. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domains are logical groupings of devices and are used to control who can administer the group. By creating virtual domains, an administrator allows users to view information relevant to them specifically and restricts their access to other areas. Virtual domain filters allow users to configure devices, view alarms, and generate reports for their assigned part of the network *only*.

Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose.

Before you set up virtual domains, you should determine which users should have access to which sites and devices in your network.

Creating a Site-Oriented Virtual Domain

By default, there is only one virtual domain defined (*root*) in Prime Infrastructure.

When you create a site-oriented virtual domain, you allows users to view information in a specific site and restrict their access to other areas.

The following steps explain how to choose a segment of all the devices at a particular location and make them part of the "Site 1 Routers" virtual domain.

Step 1 Choose **Administration > Virtual Domains**.

Step 2 From the left Virtual Domain Hierarchy sidebar menu, click **New**.

Note By default, only one virtual domain (*root*) is defined in Prime Infrastructure. The selected virtual domain becomes the parent virtual domain of the newly created, subvirtual domain.

Step 3 Enter **Site 1 Routers** for the virtual domain name, then click **Submit**.

Step 4 On the Sites tab, move the sites that you want to associate with the virtual domain to the Selected Sites column, then click **Submit**.

Step 5 Click **OK** on the confirmation screens.

Assigning Users to a Virtual Domain

After you create a virtual domain, you can associate the virtual domain with specific users. This allows users to view information relevant to them specifically and restricts their access to other areas. Users assigned to a virtual domain can configure devices, view alarms, and generate reports for their assigned virtual domain *only*.

The following steps walk you through creating a user who is in charge of the Site 1 Routers virtual domain you previously created.

Step 1 Choose **Administration > Users, Roles, & AAA**.

Step 2 Click the username that you want to assign to a virtual domain.

Step 3 Click the Virtual Domains tab, then move the specific virtual domain from the Available list to the Selected list.

Step 4 Click **Submit**.

Note When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server.

Related Topic

- Controlling User Access

Setting Up Assurance

If your Prime Infrastructure implementation includes Assurance licenses, you will need to enable data collection via NAMs and NetFlow configurations. This is necessary to populate the additional dashlets, reports and other features supplied with Assurance.

Setting up Assurance-oriented data collection is covered in the following topics:

Enabling NAM Data Collection

To ensure that you can data from your Network Analysis Modules (NAMs), you must enable NAM data collection. You can do this for each discovered or added NAM, or for all NAMs at once.

Note NAM data collection will not work unless you have first specified HTTP/HTTPs credentials for each NAM (see Adding NAM HTTP Credentials).

Step 1 Choose **Administration > Data Sources > NAM Data Collector**.

Step 2 Select all of the NAMs for which you want to enable data collection.

Step 3 Click **Enable**.

Related Topics

- Discovering the Network
- Adding Devices Manually
- Adding NAM HTTP Credentials

Enabling NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you need to configure your NetFlow-enabled switches, routers, and other devices to export this data to Prime Infrastructure. Prime Infrastructure provides an “out of the box” configuration template that allows you to set this up quickly. You can apply it to all or just a subset of your NetFlow enabled devices.

The following procedure is basic, and assumes that you want to configure all types of NetFlow-enabled devices in the same way. You may want to repeat this procedure with variations if, for example, you want create a separate configuration for each type of device, vary exporter or monitor names, set up multiple flow exporters or monitors on the same device type, or set up data export for multiple interfaces on a particular type of device.

Step 1 Choose **Design > Configuration Templates > My Templates > OOTB > Collecting Traffic Statistics**.

Step 2 In the Template Basic section, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria section, select the Device Type dropdown, then select all of the Device Types that you want to export their NetFlow data to Prime Infrastructure.

Step 4 In the Validation Criteria section, enter the OS Version.

Step 5 In the Template Detail section, complete the fields as follows:

- Flow Exporter Name—Enter a name for the NetFlow exporter on the device types you selected. This can be any collection of characters (for example: `EXPORTER-1`).
- IP Address—Enter the IP address of the Prime Infrastructure server.
- Flow Exporter Port—Enter the port on which the NetFlow monitor will receive the exported data. Use the default 9991 port unless you have a special need to override it.
- Flow Monitor Name—Enter an arbitrary name for the NetFlow monitor caching the data from the flow exporter (for example: `FLOW-MONITOR-1`).
- Int—The name of the interface on the device whose NetFlow data you want to monitor (for example: `ethernet 0/0`).

Step 6 Click **Save as New Template**. After you save the template, deploy it to your NetFlow-enabled devices using the procedures in Deploying Templates.

Setting Up External Management Servers

This section contains the following topics:

Configuring ACS View Servers

To facilitate communication between Prime Infrastructure and the ACS View Server and to access the ACS View Server tab, you must add a view server with credentials.

Note Prime Infrastructure only supports ACS View Server 5.1 or later.

To configure the ACS View Server Credentials, follow these steps:

Step 1 Choose **Design > External Management > ACS View Servers**.

Step 2 Enter the port number of the ACS View Server you are adding. (Some ACS View Servers do not allow you to change the port on which HTTPS runs.)

Step 3 Enter the password that was established on the ACS View Server. Confirm the password.

Step 4 Specify the time in seconds after which the authentication request times out and a retransmission is attempted by the controller.

Step 5 Specify the number of retries to be attempted.

Step 6 Click **Save**.

Configuring TFTP or FTP Servers

Step 1 Choose **Design > External Management > TFTP/FTP Servers**.

Step 2 From the Select a command drop-down list, choose **Add TFTP/FTP Server**.

Step 3 From the Server Type drop-down list, choose **TFTP**, **FTP**, or **Both**.

Step 4 Enter a TFTP/FTP server name. This is a user-defined name for the server.

Step 5 Enter the IP address of the TFTP/FTP server.

Step 6 Click **Save**.

Next Steps

Now that you have completed the basic setup steps, you might want to do the following tasks:

Table 2-3 Next Steps after Completing Setup Tasks

Task	GUI Path	Documentation Reference
Set up additional users	**Administration > Users, Roles & AAA**, then click **Users**	Controlling User Access
Add additional virtual domains	**Administration > Virtual Domains**	Setting Up Virtual Domains
Refine your sites	**Design > Site Map Design**	Designing Sites
Create additional port groups and change existing port groups	**Design > Port Grouping**	Changing Port Groups
Start monitoring and responding to alarms	**Operate > Alarms & Events**	Monitoring Alarms