Operating and Monitoring the Network

On the Operate tab, Cisco Prime Infrastructure provides tools to help you monitor your network on a daily basis, as well as perform other day-to-day or ad hoc operations relating to network device inventory and configuration management. The Operate tab contains dashboards, the Device Work Center, and tools that you need for day-to-day monitoring, troubleshooting, maintenance, and operations.

Monitoring Dashboards

Prime Infrastructure automatically displays monitoring data on dashboards and dashlets. Table 10-1 describes the dashboards that are available in **Operate > Monitoring Dashboards** for checking summary information.

Note

- The label "*Edited*" next to a dashlet heading indicates that the dashlet has been customized.
- The dashlet arrangement is maintained after upgrading. To display new dashlets or features in a new release, click **Manage Dashboards**.

You can choose one of the following dashboards in **Operate > Monitoring Dashboards** to view summary information:

Table 10-1 Operate > Monitoring Dashboards

Dashboard	Description
Overview	Network overview information, including device counts, top N devices by CPU and memory utilization, and the device credential summary. To troubleshoot and isolate issues, click a device or interface alarm count to view detailed dashboards, alarms, and events. You can also view information about your software such as version, type, and device count. The Overview-General dashboard also displays user-defined jobs under Job Information Status dashlet. The following dashboards appear on the Overview tab: • **General**—Displays general inventory, memory utilization, device summary information, and so on. • **Client**—Displays client-related information to allow you to monitor clients on the network. • **Security**—Displays rogue access points, top security issues, information on attacks, and so on. • **Mesh**—Displays mesh alarms, mesh packet error rate, worst node hop count, and so on. • **CleanAir**—Displays average air quality, interferers, and so on. • **Context Aware**—Displays historical element counts, allows you to troubleshoot clients, and so on.
Incidents	Alarm and event information, including the sites with the most alarms, the most frequently occurring types of alarms, the distribution of alarms and summary of syslog events by severity, syslog events that match user-configured message type criteria. This dashboard also includes a summary of SNMP reachability for all devices in the network.
Performance	Information about CPU and memory utilization, environmental temperatures, and device and interface availability. The following dashboards appear on the Performance tab: • **Network Device**—Displays top CPU utilization, environmental temperature, memory utilization, and so on. • **Network Interface**—Displays interface availability, utilization information, and so on. • **Service Assurance**—Displays top applications, clients, servers, and so on. • **Service Health**—Displays site-application health information.
Detail Dashboards	Network health summaries for sites, devices, or interfaces. The detail dashboards allow you to see congestion in your network and gather detailed site, device, and interface information. For example, you can view detailed dashboards for a particular site to determine which devices have the most alarms, check device reachability status for the site, and so on.

To change the information displayed in the dashboards, see Search Methods.

Table 10-2 describes where to find monitoring information in the Prime Infrastructure dashboards.

Table 10-2 Finding Monitoring Data

To View This Monitoring Data...	Choose this Dashboard...
Alarm information	Operate > Monitoring Dashboards > Incidents
Application information	Operate > Monitoring Dashboards > Detail Dashboards > Application
Client information	Operate > Monitoring Dashboards > Overview > Client
CPU utilization	Operate > Monitoring Dashboards > Overview > General

Table 10-2 Finding Monitoring Data (continued)

To View This Monitoring Data...	Choose this Dashboard...
Device (specific) information	Operate > Monitoring Dashboards > Detail Dashboards > Device
Device (Top N) CPU utilization, memory utilization, and environmental temperature information	Operate > Monitoring Dashboards > Performance > Network Device
Device credential status	Operate > Monitoring Dashboards > Overview > General
Device reachability summary	Operate > Monitoring Dashboards > Detail Dashboards > Site
End user information	Operate > Monitoring Dashboards > Detail Dashboards > End User Experience
Event information	Operate > Monitoring Dashboards > Incidents
Interface information	Operate > Monitoring Dashboards > Detail Dashboards > Interface
Interface status, availability, and utilization information	Operate > Monitoring Dashboards > Performance > Network Interface
Licensing information	Operate > Monitoring Dashboards > Overview > General
Memory utilization	Operate > Monitoring Dashboards > Overview > General
Mesh network information	Operate > Monitoring Dashboards > Overview > Mesh
Security information	Operate > Monitoring Dashboards > Overview > Security
Service assurance information	Operate > Monitoring Dashboards > Performance > Service Assurance
Site information	Operate > Monitoring Dashboards > Detail Dashboards > Site
Syslog Watch and Syslog Summary	Operate > Monitoring Dashboards > Incidents or Operate > Alarms & Events > Syslogs
Utilization statistics	Operate > Monitoring Dashboards > Overview > General
Voice/video information	Operate > Monitoring Dashboards > Detail Dashboards > Voice/Video
WAN information	Operate > Monitoring Dashboards > Detail Dashboards > WAN Optimization

Monitoring Background Tasks

A background task is a scheduled program running in the background with no visible pages or other user interfaces. In Prime Infrastructure, background tasks can be anything from data collection to backing up configurations. You can monitor background tasks to see which background tasks are running, check their schedules, and find out whether the task was successfully completed.

Step 1 Choose **Administration > System Settings > Background Tasks** to view scheduled tasks. The Background Tasks page appears.

Step 2 Choose a command from the drop-down list:

- **Execute Now**—Runs all of the data sets with a checked check box.
- **Enable Tasks**—Enables the data set to run on its scheduled interval.
- **Disable Tasks**—Prevents the data set from running on its scheduled interval.

Device Work Center

From **Operate > Device Work Center**, you can view the device inventory and device configuration information. The Device Work Center contains general administrative functions at the top and configuration functions at the bottom as described in Table 10-3.

Table 10-3 Device Work Center Tasks

Task	Description	Location in Operate > Device Work Center
Manage devices	Add, edit, delete, sync, and export devices, add and delete devices from groups and sites, and perform a bulk import.	Buttons located at the top of the Device Work Center. Refer Adding Devices Manually, Exporting Devices, and Importing Devices from Another Source for more details.
View basic device information and collection status	View basic device information such as reachability status, IP address, device type, and collection status.	Hover your mouse cursor on the IP Address/DNS cell and click the icon to access the 360° view for that device (see Getting Device Details from the Device 360° View). Hover your mouse cursor on the Collection Status cell and click the icon to view errors related to the inventory collection.
Manage device groups	By default, Prime Infrastructure creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that appear under the User Defined folder.	Displayed in the left pane of the Device Work Center Page. See Managing Device Groups for more information about creating and using device groups.
Add devices to site groups	After you set up a site group profile, you can add devices to it. To add devices to site groups in Device Work Center, add them to Group and then select site group. To add devices to site maps, go to the Design > Site Map Design page. **Note** A device can belong to one site group hierarchy only. **Note** The devices added to a site group in Device Work Center do not add devices in the Design > Site Map Design page. Similarly, the devices added in the Site Map Design page are not added to site groups in Device Work Center.	**Add to Group** button located at the top of the Device Work Center page under “Groups & Sites”.

Table 10-3 Device Work Center Tasks (continued)

Task	Description	Location in Operate > Device Work Center
View device details	View device details such as memory, port, environment, and interface information.	Choose a device in the Device Work Center, then click the **Device Details** tab at the bottom of the Page.
	View device information and status, and associated modules, alarms, neighbors, and interfaces. See Getting Device Details from the Device 360° View for more information.	Hover your mouse cursor on a device IP address and click the icon that appears.
Create and deploy configuration templates	You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device. **Note** Using the Device Work Center, it may not be possible to add configuration for a few controller features. In this case, use the Design page and create a new Template and deploy to the device.	Click the **Configuration** tab at the bottom of the Device Work Center Page. See Configuring Device Features for more information about configuring features on a device.
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click **Configuration Archives** at the top of the Device Work Center.
View software images	You can view the recommended software image for a single device, and then import or distribute that image. If you want to distribute a software image to multiple devices, see Deploying Software Images to Devices.	Click **Software Image Management** at the top of the Device Work Center. Select a device for which you want to view the recommended software image. Click the **Image** tab. Scroll down to Recommended Images to view the recommended image for the device you selected. Prime Infrastructure gathers the recommended images from both Cisco.com and the local repository. You can import the recommended image (see Importing Software Images) or distribute (see Deploying Software Images to Devices) the recommended image.
View interface details	You can view the description, admin status, and operational status of the interface.	Choose a device in the Device Work Center, then click the **Configuration** tab at the bottom of the screen. Click **Interfaces** to view the interface details.
View and modify TrustSec configuration	You can view and modify the TrustSec configuration of a TrustSec-based device.	Choose a device in the Device Work Center, then click the **Configuration** tab at the bottom of the screen. Click **Security >TrustSec > Wired 802_1x**.

Import Policy Updates

Import Policy Updates allows you to manually download the policy updates patch file from Cisco.com and import it into the Compliance and Audit Manager Engine.

To import policy updates:

Step 1 From the Cisco.com home page, navigate to **Products & Services > Cloud and Systems Management**. Click **View All Products**, then click **Routing and Switching Management > Cisco Prime Infrastructure**, select the latest version and then click **Compliance Policy Updates**.

Step 2 Download the CompliancePolicyUpdates.vX-y.jar patch file, where *X* is the major version and *y* is the minor version.

Step 3 Enter your Cisco.com credentials.

Step 4 Save the CompliancePolicyUpdates.vX-y.jar patch file to your local system.

Step 5 To select the downloaded CompliancePolicyUpdates.vX-y.jar file from your local system, select **Administration > Import Policy Updates**, then click **Browse**.

Note The Import Policy Updates menu appears only if you have enabled the Compliance Service (**Administration > System Settings**) as described in Configuring Server Settings.

Step 6 To import the CompliancePolicyUpdates.vX-y.jar patch file into the Compliance Engine, click **Upload**.

A message appears indicating the successful importing of policy into the Compliance Engine.

Step 7 After you see the message indicating a successful import, restart the Prime Infrastructure server process to effect the changes. See Restarting the Prime Infrastructure Server, page 10-6.

Note Verify that the Prime Infrastructure server process is restarted to effect the changes.

Restarting the Prime Infrastructure Server

Step 1 To restart the Prime Infrastructure server, log in as the admin user:

```
ssh admin@<server>
```

Step 2 Run the following commands (in the order specified) from the admin prompt:

```
admin# ncs stop
admin# ncs start
```

Monitoring Jobs

Use the Jobs dashboard to:

- View all running and completed jobs and corresponding job details
- Filter jobs to view the specific jobs in which you are interested
- View details of the most recently submitted job
- View job execution results
- Modify jobs, including deleting, editing, running, canceling, pausing, and resuming jobs

Step 1 Choose **Administration > Jobs Dashboard**.

Step 2 Click a job, then perform any of the following actions:

- Click **Run** to start the currently scheduled job immediately. If a job has the status "failed," click **Run** to resubmit the same job, which creates a new scheduled job with the same parameters as the previous job.
- Click **Abort** to stop a discovery job currently in progress and return it to its scheduled state. You cannot abort all jobs. For example, you receive an error message if you try to abort a running configuration job.
- Click **Cancel** to delete any future scheduled jobs for the job you specified. If a job is currently running, it will complete.
- Click the **History** tab to view the history of a job. Hover your mouse over the results in the Status column to display troubleshooting information that can help you determine why a job failed.
- Click the **Details** tab to view job information such as when the job was created, started, or scheduled.

Note When a minute job is scheduled to run recursively, the first trigger of the job falls on n^{th} minute of the hour, as divided by the quartz scheduler, and successive runs will be placed as per the schedule. For example, if you have given the start time as 12:02:00 and you want the job to run every 3 minutes, then the job will be executed at 12:03 (in a minute), with the next recurrence at 12:06, 12:09, and so on. Another example, if you have given the start time as 12:00:00 and you want the job to run every 3 minutes, then the job will be executed at 12:00 (without any delay), with the next recurrence at 12:03, 12:06, and so on.

Monitoring the System Using Reports

Prime Infrastructure reporting helps you monitor the system and network health and troubleshoot problems. You can run a report immediately or schedule it to run at a time that you specify. After you define a report, you can save it for future diagnostic use or schedule it to run on a regular basis. You can save a report in either CSV or PDF format. You can save it to a file on Prime Infrastructure for later download, or email it to a specific email address.

To view a report:

Step 1 Choose **Report > Report Launch Pad**.

Step 2 Click a report name to view the data for that report.

To create a report:

Step 1 Choose **Report > Report Launch Pad**, then click **New** next to the report type that you want to create.

Step 2 Enter the report details, then click one of the save options.

Monitoring and Troubleshooting Network Traffic

In addition to aggregating data from multiple NAMs, Prime Infrastructure with licensed Assurance features makes it easy to actively manage and troubleshoot network problems using multiple NAMs and ASRs.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

Note This feature is supported for NAMs and ASRs. For more information on minimum IOS XE version supported on ASRs, see the *Cisco ASR 1000 Series Aggregation Services Routers Release Notes*.

In the following workflow, a network operator needs to troubleshoot a set of similar authentication violations taking place at multiple branches. Because the operator suspects that the authentication problems are due to a network attack in progress, the operator runs the Packet Capture feature against the NAMs or ASRs for each branch, then runs the Packet Decoder to inspect the suspicious traffic.

Step 1 Create a capture session definition:

a. Choose **Operate > Operational Tools > Packet Capture > Capture Sessions**, then click **Create** to create a new capture session definition.

b. Complete the **General** section as needed. Give the session definition a unique name and specify how you want to file the captured data. To capture the full packet, enter 0 in the Packet Slice Size.

c. If you want to restrict the captured traffic to particular source or destination IPs, VLANs, applications, or ports, click **Add** in the Software Filters section and create filters as needed. If you do not create a software filter, it captures everything.

d. In the **Devices** area, you can select:

   – A NAM and its data ports. You can create one capture session per NAM only, whether the capture session is running or not.

   – An ASR and its interfaces.

e. Click **Create and Start All Sessions**.

Prime Infrastructure (with licensed Assurance features) saves the new session definition, then runs separate capture sessions on each of the devices you specified. It stores the sessions as files on the device and displays the list of packet capture files in the **Capture Files** area.

Step 2 To decode a packet capture file:

a. Choose **Operate > Operational Tools > Packet Capture**.

b. Select a PCAP file in a NAM or ASR device.

c. Select **Copy To** to copy the PCAP file to the PI server (the decode operation only runs on files in the PI server).

d. Click **View Jobs t**o confirm that the copy job completed successfully.

e. Open the localhost folder, click the check box for the new capture file, then click **Decode**. The decoded data appears in the bottom pane.

f. A TCP Stream displays the data as the application layer sees it. To view the TCP Stream for a decoded file, select a TCP packet from the Packet List, then click **TCP Stream**. You can view the data as ASCII text or in a HEX dump.

Step 3 To run a packet capture session again, select the session definition in the **Capture Sessions** area and click **Start**.

Diagnosing Site Connectivity Issues and Comparing Configurations

You can use the Prime Infrastructure dashboards to monitor your network and locate problematic devices, and then use the Device Work Center to change the device configuration.

Step 1 Choose **Operate > Detailed Dashboards**, choose the site for which you are experiencing connectivity issues, then click **Go**.

Step 2 Check the data reported under Device Reachability Status and Top N Devices with Most Alarms to determine the source of the issue.

Step 3 Click the name of the device for which you see the most alarms.

Step 4 From the 360° view of the device, click the Alarm Browser icon to see the alarms for that device. Expand an alarm to view details about the alarm.

Step 5 To compare the current device configuration with a previous, known good configuration, choose **Operate > Device Work Center**, then select the device whose configuration that you want to change.

Step 6 Click the **Configuration Archive** tab, expand the arrow to view additional options, and select the configuration type and a configuration against which to compare.

Step 7 Change or roll back the configuration. See Rolling Back Device Configuration Versions, page 14-4 for more information.

Monitoring a Controller or a Specific AP

Use these dashlets to filter on a controller or a specific AP:

- Top N Applications
- Top N Clients

- Top N Application Groups (not a default dashlet; you must add it to the Detail Dashboard)
- Client Conversations (not a default dashlet)

Before You Begin

If you have not set up a building, floor, and AP, choose **Operate > Maps**, create a building and a floor under a site, then associate that floor with an AP. For example, site=System Campus, building=bldgN, floor=Floor1.

- To filter site data, use this AP in the Detail Dashboards. Choose **Operate > Monitoring Dashboards > Detail Dashboards > Site**.
- To collect only traffic that is associated with the APs on that floor, choose (for example) **Filters > Site > System Campus > bldgN > Floor1** and click **Go**.

To filter on a controller or a specific AP:

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards**, then click the **Site** tab.

Step 2 To enable filtering on a controller or a specific AP:

a. Click the **Dashlet Options** icon (for one of the dashlets that support filtering), then click the **Enable Controller Filter** check box.

b. Select a controller.

c. Optionally, select an AP.

Step 3 Use the Device dashboard to choose:

- A device assigned to a site
- A device from the list of all devices
- A device that is sending NetFlow information to the Prime Infrastructure server

Step 4 Add the **Top N Applications** and **Top N Hosts** dashlets to **Detail Dashboards > Device**. These dashlets will display, using the NetFlow data being sent, what the top applications are. You can then select a device and see the type of traffic that is going through that device.

Step 5 You can create a similar filter using the **End User Experience** dashboard to select a user name, an IP address, or a MAC address. If you click **Select from Client List** and choose an IP address, the user data will be filled in automatically.

Post-Deployment Application Monitoring

Prime Infrastructure with licensed Assurance features lets network operators investigate performance issues starting from any of the many parameters that contribute to them: raw server performance, competition for bandwidth from other applications and users, connectivity issues, device alarms, peak traffic times, and so on. This flexibility makes shorter troubleshooting time and quicker solutions.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

In the following workflow, a network administrator is responding to scattered complaints from multiple branches about poor performance for a newly deployed application. The network administrator suspects a malfunctioning edge router at the application server site to be the problem, but needs to see if other factors are contributing to the issue.

Step 1 Choose **Operate > Monitoring Dashboards > Detail Dashboards > Application**.

Step 2 To limit all of the dashlets on this page to the newly deployed application, select the application from the **Filters** line and click **Go**.

Step 3 Add the following dashlets to this dashboard:

- Application Traffic Analysis
- Top N Devices with Most Alarms
- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics

Step 4 Find the **Application Server Performance** dashlet, which gives statistics on response times for the servers hosting the application. Look for sudden increases in server response time.

Step 5 Compare the data in the **Application Server Performance** dashlet with the data in **Worst N Clients by ART Metrics** and **Worst N Sites by ART Metrics**. See if peaks in server response time match one or more users' experience of poor transaction times, or are more generalized across sites.

Step 6 Check the **Application Traffic Analysis** dashlet for peaks in usage. Use the lower graph Pan and Zoom handles to investigate the time frames of observed traffic peaks. Compare the peaks in application response time with these periods of peak usage.

Step 7 Check the **Top N Clients** dashlet to identify the largest bandwidth consumers for the application. Then find the **Worst N Sites by ART Metrics**, and compare the information in these two dashlets to see if the biggest bandwidth consumers are also part of the worst-performing sites.

Step 8 Examine the worst site in **Worst N Sites by ART Metrics**. Click the site name in the **Site** column. If needed, filter the data on the Site Detail Dashboard by the newly deployed application, as you did in Step 2.

Step 9 On the Site Detail Dashboard, check the **Top N Applications** and **Top N Clients** dashlets to confirm your picture of the top application users on this site and the time periods when performance was a problem for this application.

Step 10 On the Site Detail Dashboard, check the **Top N Devices with Most Alarms** to see if any of the site's servers or edge routers currently have alarms that might indicate why the application performance at this site is so poor.

Step 11 On the Incidents Dashboard, check for the **Device Reachability Status** to confirm if the suspect device is still reachable. If it is, to launch its 360 View, hover your mouse cursor on the device IP address, then click the icon that appears.

Step 12 In the Device 360 View:

a. Click the **Interfaces** tab and confirm that sessions for the affected application flow over this device.

b. Click the **Alarms** tab to see a summary of current alarms for the device.

Step 13 If this device seems to be the source of the application performance problem at this site:

a. Click the Alarm Browser icon at the top of the 360 View to see all alarms for this device.

b. Use the **Show** field to limit the alarms shown to those in the time frame of the problems.

Securing Network Services

Cisco TrustSec Identity-Based Networking Services (IBNS) is an integrated solution consisting of Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco TrustSec IBNS help enterprises to increase productivity and visibility, reduce operating costs, and enforce policy compliance.

Note To use this feature, your Prime Infrastructure implementation must include Assurance licenses.

In Prime Infrastructure, the TrustSec network service design enables you to choose preferred options for provisioning configurations to TrustSec-capable devices to enable 802.1X and other TrustSec functionality. You can configure wired 802_1x devices by creating TrustSec model-based configuration templates and choosing any one of the following navigation paths:

- Design > Network Services > Features-TrustSec > Wired 802_1x.
- Design > Configuration > Feature Design > Features and Technologies > Security > TrustSec > Wired 802_1x

Note that for Catalyst 6000 devices:

- **Security violation as protect** is not available for Catalyst 6000 supervisor devices.
- **Security violation as replace** is available in Cisco IOS Release 15.1(01)SY and later.
- The command **macsec** is not available for Catalyst 6500 supervisor 2T devices.

For more details about configuring TrustSec model-based configuration templates, see Creating Feature-Level Configuration Templates, page 8-2.

Generating a TrustSec Readiness Assessment Report

TrustSec Readiness Assessment displays TrustSec-based device details such as TrustSec version, readiness category, readiness device count, and device percentage displayed in the pie chart.

To generate a TrustSec Readiness Assessment report:

Step 1 Choose **Design > Network Services > Features-TrustSec > Readiness Assessment**.

A pie chart appears with the following types of devices:

- TrustSec Limited Compatibility Devices
- TrustSec Capable Devices
- TrustSec Hardware Incapable Devices
- TrustSec Software Incapable Devices

Step 2 Click **Section view** and click any of the pie chart slices to view the details of the selected TrustSec-based device type.

Step 3 Click **Complete view** to view the details of all TrustSec-based devices.

Step 4 Select the TrustSec version and click **Export** to export the readiness assessment details to a CSV file.