C H A P T E R **5**

Setting Up Native Reports

Prime Network provides two reporting functions. The native reports feature is launched from the Reports menu in the Vision client, Events client, or Administration client; this reporting tool is described in the following topics. The Operations Reports feature is an optional application and is described in *Cisco Prime Network 5.0 Operations Reports User Guide*.

These topics describe how to set up the native reports feature:

- Workflow for Setting Up Regular Reports, page 5-1
- Checking Global Settings for Report Operations, page 5-2
- Setting Up Your Report Folders, page 5-2
- Inventory Hardware and Software Reports, page 5-7
- Network Service Reports, page 5-9
- Creating Your Customized Report, page 5-10
- Entering Report Criteria and Testing Your Report, page 5-12
- Scheduling a Recurring Report, page 5-14
- Sending a Report Through E-mail Notification, page 5-14

Whether you can perform these setup tasks depends on your account privileges. See Permissions Required to Perform Tasks Using the Prime Network Clients for more information.

Workflow for Setting Up Regular Reports

This workflow shows the steps required to set up regular, scheduled reports. If you simply want to run an existing predefined report, see:

- Inventory Hardware and Software Reports, page 5-7
- Network Service Reports, page 5-9

The following table provides the basic workflow for setting up scheduled reports.

	Description	See:
Step 1	If necessary, adjust the global settings that affect reports (for example, whether users can create shared reports which others can view).	Checking Global Settings for Report Operations, page 5-2
Step 2	Set up your report folder structure in Report Manager.	Setting Up Your Report Folders, page 5-2

	Description	See:
Step 3	Choose the report you want to customize:	
	• Event reports—Tickets, Service events, Syslogs, and Traps; Audit, Provisioning, System and Security events; database-related information	• Event Reports, page 5-3
	• Hardware and software reports	• Inventory Hardware and Software Reports, page 5-7
	• Ethernet service, network pseudowire, VPLS/H-VPLS reports	• Network Service Reports, page 5-9
Step 4	Create a customized report based on any of the predefined reports that are packaged with Prime Network.	Creating Your Customized Report, page 5-10
Step 5	Test your customized report.	Entering Report Criteria and Testing Your Report, page 5-12
Step 6	Schedule your recurring report.	Entering Report Criteria and Testing Your Report, page 5-12

Checking Global Settings for Report Operations

The following default report behavior is controlled from the Administration client and will affect report users:

- The report actions users can perform, and the devices users can view and manage. When a user account is created the administrator assigns a user access level to the user account (Viewer, Operator, Operator Plus, Configurator, or Administrator).
  - The user access level controls which reports a user can generate.
  - The device scope determines which devices a user has permission to access, and which devices they can run reports against.

  For a matrix of actions users can perform depending on their user access level and device scope assignments, see Permissions Required to Perform Tasks Using the Prime Network Clients.
- Whether users can create public (shared) reports. By default, users cannot create shared reports.

Users with Administrator privileges can change these settings. They can also configure Prime Network to generate a warning message whenever a user executes a command script. For more information, see the *Cisco Prime Network 5.0 Administrator Guide*.

Setting Up Your Report Folders

Create nested folders to organize your reports under the existing Report Manager categories: Events Reports, Inventory Reports, and Network Service Reports. You can then place your customized reports under these folders (by specifying the Location field when you create the report).

Step 1 Choose **Reports > Report Manager** from the Prime Network client main menu.

Step 2 In Report Manager, choose **Events Reports > New Folder**.

Step 3   In the New Folder dialog, enter a folder name. The new folder appears under the Events Reports.

You can also move folders and reports to new locations from the Report Manager.

Event Reports

These event reports can be run from the Vision client, Events client, or Administration client:

- Generalized Network Event Reports (Tickets, Service Events, Traps, Syslogs), page 5-3
- Ticket Event Reports, page 5-4
- Service Event Reports, page 5-4
- Syslog-Specific Event Reports, page 5-5
- Trap-Specific Event Reports, page 5-5
- Database-Related Event Reports, page 5-6
- Audit, Provisioning, System, Security Event Reports (Non-Network Reports), page 5-7

Generalized Network Event Reports (Tickets, Service Events, Traps, Syslogs)

To get this network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Devices with most severe events (Pie chart shows device percentages)	Events Reports > Devices with the Most Events (By Severity)	Yes	Yes
Devices with most frequent events Pie chart shows device percentages	Events Reports > Devices with the Most Events (By Type)	Yes	Yes
Devices with most syslogs Devices with most traps Devices with most Service events (up to 1,000 devices):	Detailed Event Count (By Device)	Yes	Yes

Ticket Event Reports

To get this ticket information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common tickets for all managed devices Pie chart shows type percentages	Events Reports > Most Common Daily Events	No; all devices chosen by default	Yes
Details about tickets by their severity: • Alarm cause and the root event time • Affected devices • Whether ticket was acknowledged • Other event details: Duplication count, reduction count, alarm count, last modification, etc.	Detailed Tickets	Yes	Yes
Ticket details for specific devices (up to 1,000 devices): • Number of tickets per severity • Number of tickets per ticket type	Detailed Event Count (By Device)	Yes	TBD
Tickets with highest number of associated events with details such as: • Root cause • Ticket creation time	Events Reports > Event Reduction Statistics	Yes	Yes
Ticket MTTR[1] (mean time to repair information): • Number of tickets cleared manually • Number of tickets cleared automatically (by system) • MTTR • Ticket root cause and creation time	Events Reports > Mean Time to Repair	No; all devices chosen by default	Yes

1. MTTR is based on time of ticket creations, and time the ticket was last modified. (Acknowledging a cleared ticket can therefore affect the MTTR for the ticket.)

Service Event Reports

To get this network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common Service events, tickets, syslogs, traps Pie chart shows type percentages	Events Reports > Most Common Daily Events	All chosen by default	Yes
Most severe Service events with details	Detailed Service Events	Yes	Yes

Syslog-Specific Event Reports

To get this Syslog information:	Use this report:	Can you choose devices?	Can you specify time period?
Most common syslogs, and how many of each type? Pie chart shows type percentages	Events Reports > Most Common Syslogs	No; all devices chosen by default	Yes
Devices with most syslogs **Note** This report can also be generated from generic (non-actionable) events. Pie chart shows device percentages	Events Reports > Devices with the Most Syslogs	No; all devices chosen by default	Yes
Time frame when most syslogs occurred	Events Reports > Daily Average and Peak	No; all devices chosen by default	Yes
Syslog details (up to 250,000): • IP address time, description • Syslog raw data (generic events) or description (actionable events) **Note** This report can also be generated from generic (non-actionable) events.	Detailed Syslogs	Yes	No
For specific syslogs, their count and first and last time they occurred Pie chart show s syslog percentages	Events Reports > Syslog Count	No; all devices chosen by default	Yes
For specific syslogs, the devices they occurred on Pie chart show s syslog percentages	Events Reports > Syslog Count (By Device)	Yes	Yes
For specific syslogs and specific devices, a graph of syslogs with their priority	Events Reports > Syslog Trend (By Severity)	Yes	Yes

Trap-Specific Event Reports

To get this trap information:	Use this report:	Can you choose devices?	Can you specify a time period?
Most common traps for all managed devices Pie chart shows type percentages	Events Reports > Most Common Daily Events	Yes	No; all devices chosen by default
Time frame when most traps occurred	Events Reports > Daily Average and Peak	Yes	No; all devices chosen by default

To get this trap information:	Use this report:	Can you choose devices?	Can you specify a time period?
Traps generated by specific devices: • Number of traps per severity • Number of traps per ticket type Note This report can also be generated from generic (non-actionable) events. Pie chart shows device percentages	Events Reports > Devices with the Most Traps	Yes	Yes
Trap details for specific devices: • IP address, time, description (long description if report is generated from actionable events) • SNMP and trap version • Generic or device-specific trap OID, if the event is generic The maximum number of traps retrieved for this report depends on whether the Long Description check box is selected. When checked, a maximum of 30,000 traps are retrieved. When this check box is not checked, a maximum of 100,000 traps are retrieved for this report. Note This report can also be generated from generic (non-actionable) events.	Detailed Traps	No	Yes

Database-Related Event Reports

For this database-related information:	Use this report:	Can you choose devices?	Can you specify time period?
For specific period, the number of active tickets, alarms, and events stored in DB Tickets with most number of events Events-per-second rate	Events Reports > Database Monitoring	N/A	Yes
For specific period, the number of generated tickets with these details: • Ticket type and count • Root cause and ticket creation time • Number of correlated events per ticket (largest, smallest, average)	Events Reports > Event Reduction Statistics	Yes	Yes
For a specific period, total number of actionable and generic events added to the Oracle database by type (Syslogs, Traps, Tickets, correlated/uncorrelated events, network/non-network events)	Events Reports > Fault DB vs. Event Archive Statistics	N/A	Yes

Audit, Provisioning, System, Security Event Reports (Non-Network Reports)

For this non-network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Audit event details: • Severity, timestamp, description • Username, originating IP address • Command details: name, parameters, signature	Detailed Audit Events	No	Yes
Provisioning event details • Severity, timestamp, description, username • Status	Detailed Provisioning Events	No	Yes
Security event details: • Severity, timestamp, description, location • Username, originating IP address	Detailed Security Events	No	Yes
System event details: • Severity, timestamp, description, location	Detailed System Events	No	Yes

Inventory Hardware and Software Reports

For all inventory reports, Prime Network retrieves the inventory information from the network element. These inventory reports can be run from the Vision client, Events client, or Administration client:

- Hardware Reports, page 5-8
- Software Reports, page 5-8

Hardware Reports

Hardware inventory information:	Type of report:	Can you choose devices?
Hardware details (you can filter this report using a string from the device, chassis, module, or port name): • Chassis—Description and serial number; shelf description, serial number, and status ✎ Note When the last Virtualized Services Module (VSM) blade is removed from the chassis, a notification stating that the data center has been removed is sent by the Prime Network. When this notification is received and transformed by Prime Network Integration Layer to the Operations Support Systems (OSS) client, the client is expected to delete all objects (Hosts, VM) under this specific virtual device context (VDC). • Module—Module and sub module name; module status, hardware type, and version • Port—Port location, type, and status; port alias, if port is sending alarms, if port is managed, PID, pluggable type serial number	Hardware Detailed	Yes
Hardware details you can optionally group (the report also provides the device IP address and serial number): • Device name or system name • Vendor, product, device series, element type, or chassis	Hardware Summary	Yes
Module details (you can filter this report using a string from the module name): • Hardware version and serial number • Software version • IP address	Modules Summary (By Type)	Yes

Software Reports

Software information:	Type of report:	Can you choose devices?
Software sorted by devices: • Software version and image file name • Device name, type, IP address, and serial number	Software Summary (By Device)	Yes

Software information:	Type of report:	Can you choose devices?
Software sorted by version: • Number of software versions being run • Image file name and number of devices running that image	Software Summary (By Version)	Yes

Cisco IOS-XR software sorted by devices:
 	
• Cisco IOS XR software version
 	
• For each package installed on device:
 	
  – Package name and state (active or inactive)
 	
  – Storage location
 	
  – Module name
 	
• Device name, type, IP address, and serial number
	IOS-XR Software Package Summary	Yes

Network Service Reports

The following network service reports can be run from the Vision client, Events client, or Administration client.

Table 5-1   Standard Network Service Report Types

For this service information:	Use this report:
Ethernet service information which you can filter using a service, EVC, or map name: • Ethernet service or Layer 2 VPN name, including the customer label (business tag) • EVC name and customer label • Maps containing the Ethernet service or Layer 2 VPN instance	Ethernet Service Summary
Ethernet service summary with the following additional details: • Edge EFPs associated with the EVC or Layer 2 VPN • EFT fragment name and type	Ethernet Service Detailed
Network pseudowire information which you can filter using a pseudowire name, type, or map name: • Pseudowire name and type, including any customer labels (business tags) • Maps containing the pseudowire instance	Network Pseudowire Summary
Network pseudowire summary with the following additional details: • Pseudowire details and type, such as pseudowire edge, Ethernet flow point, or switching entity	Network Pseudowire Detailed
VPLS/H-VPLS information which you can filter using a VPLS/H-VPLS name or map name: • VPLS or H-VPLS name, including any customer labels (business tags) • Maps containing the VPLS/H-VPLS instance	VPLS Summary
VPLS/H-VPLS summary with the following additional details: • Type of VPLS service, such as VPLS forward, access EFP, or core pseudowire	VPLS Detailed

Creating Your Customized Report

Customized reports can be added to Report Manager so that other users can run them using their own criteria (depending on their user access level and device scopes). If you created new report folders as described in Setting Up Your Report Folders, page 5-2, customized reports can be organized under that folder (using the Location field).

This example shows how to create a report called 24-Hour Critical Tickets. The customized report will be stored under a user-created folder called Critical Tickets - Daily Report - August 2014.

Step 1　Right-click **Events Reports > Detailed Network Events > Detailed Tickets > Define Report of This Type**.

Step 2　In the Create Report dialog, enter the required information, such as:

- Report Settings
  - Name—**24-Hour Critical Tickets**
  - Location—Click **Browse** and navigate to **Events Reports > Critical Tickets - Daily Report - August 2014** in the Move To dialog box.
- Date Selection—**Last 1 days**
- Device Selection—**All Devices**
- Filter Events/Tickets By Severity—**Critical**

Step 3　Click **OK**.

Creating Detailed Standard Events Report

This example shows how to create a Detailed Standard Events report for devices from Prime Network Vision client, using the Report manager. When you create a Detailed Standard Events you can schedule, according to the severity and events you can filter the reports. After creating the report you can view the job and export Job details in a report format that are managed by Prime Network. You can save the reports in any one of the following formats PDF, XM,.CSV, HTML, and XLS.

You can export these Standard events report through Prime Network Vision client, schedule and send email notification automatically. Also, you can use the Prime Network Administrator and Events clients to generate the Detailed Standard Events report.

To create a detailed standard events report in Prime Network Vision client:

Step 1　Log in to the Prime Network Vision.client.

Step 2　Select **Reports > Reports Manager > Detailed Network Events > Detailed Standard Events.**

Step 3　Right-click the **Detailed Standard Events > Run**. The Create Report window appears.

> **Note** You can also choose **Reports > Run Report > Events Reports > Detailed Network Reports > Detailed Standard Events.**

Step 4 In the **Create Report** window, on the **General** tab, enter the required information:

- Report Settings
  - Name—Specify the name of the report.
  - Description—Enter the description of the report.
  - Report Security—Click the **Private** or **Public** radio button to set the security.
- Date Selection—**Last 1 days**
- Device Selection—**Select Devices** or **All Devices**

> **Note** You can also click **Add** to add a network element to create a report.

- Filter Events/Tickets By Severity—**Critical**
- Filter Events—Click the **Syslogs** or **Traps** or **All** radio button
- Additional Report Specifications—Enter the additional description, if required.
- On the **Scheduling** tab, enter the required information:
  - Run Now—Click the radio button to run the report
  - Schedule Job—Click the radio to specify all job criteria.

- On the **E-mail Notifications** tab, enter the required information.

Step 5   Click **OK, t**o generate the detailed standard events report in PDF, XM,.CSV, HTML, and XLS formats.

Step 6   In the **Reports Manager** window, the created report details will be displayed and you can click **View As** to select the format, save and download the report in the specified format.
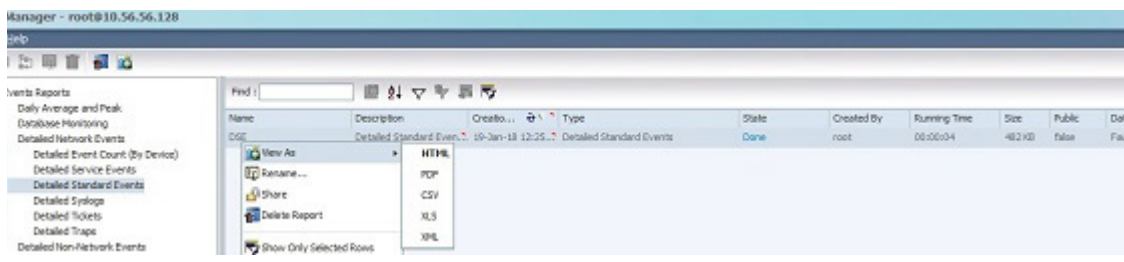
Entering Report Criteria and Testing Your Report

To enter criteria and test a customized report:

Step 1   Select **Reports > Report Manager > Run Report** and navigate to your customized report.

Step 2   Right-click the report and choose **Run Now**.

Step 3   Supply your report criteria. What you must supply depends on the report type. Most criteria is self-explanatory, but the following provides some additional details on the choices.

✎

Note   The settings that are displayed depend on the report type.

• General Criteria:

Report Settings	
Report Security	**Note** This field is displayed only if report sharing is enabled. See Checking Global Settings for Report Operations, page 5-2. • Private—Can only be viewed by creator. • Public—Can be viewed by all users, even if the devices are outside their scope. If sharing is enabled, this setting can be changed after the report is created (by right-clicking the report and selecting **Share** or **Unshare**).
Display *n*	Number of items to be displayed in report.
Data Source	Run report based on actionable or generic events
Include pie charts in report output	Also generate pie chart.
Device Selection	

Select Devices	To select specific devices:
	1. Click **Select Devices**.
	2. Click **Add**.
	3. In the Add Network Element dialog box:
	    – Click **Search** to find NEs based on your criteria.
	    – Click **Show All** to choose from a list of all NEs.
	4. Select the NEs and click **OK**.

• Special Criteria for Traps:

Traps Detailed Description	Include traps with descriptions that match *string*.	
Long Description	(Actionable events) Include traps that have *string* in their long description. 1. Check Show Long Description check box. 2. Enter the string that the trap long description must contain.	
SNMP Version	(Generic events) SNMP versions to include in the report: All, 1, 2, or 3.	
Generic	Include generic (non-actionable) traps:	
	All	All generic traps
	0	coldStart
	1	warmStart
	2	linkDown
	3	linkUp
	4	authenticationFailure
	5	egpNeighborLoss
	6	enterpriseSpecific (enter comma-separated OIDs, up to 125 digits, in Vendor Specific field)

Step 4   Click the Scheduling tab and choose **Run Now**.

Step 5   Verify the results in Report Manager or when the report is displayed in the web browser.

Scheduling a Recurring Report

To schedule a recurring customized report, use the Report Manager. If you want to schedule a predefined report, you can run it from Report Manager or directly from the Prime Network client Reports menu. To run a report immediately, click the Schedule tab and choose **Run Now**.

To schedule a report:

Step 1   Select the report you want to schedule.

Report Type	Run From Main Menu:
Predefined reports that come with Prime Network	**Reports > Run Report**
Customized reports (reports you modified and saved)	**Reports > Report Manager > Run Report**

Step 2   Supply your report criteria.

Step 3   Click the Scheduling tab and give the job a meaningful title (for example, 24-Hour Ticket Report Job).

Step 4   Enter the schedule criteria—for example: Recurring, Daily, Run Indefinitely, and from the current time for 30 days.

Once you schedule a job, the job information can only be edited from the Job Manager by choosing **Tools > Schedule Job** from the Vision client main menu. You can also rerun the job and clone the job using the Job Manager.

Sending a Report Through E-mail Notification

To send a report, you can enter the e-mail notification criteria in the Create Report window. If e-mail notification details are provided, you can run the report and automatically the report is mailed as an attachment in a desired format. You can attach reports in the XML, PDF, CSV, XLS, or HTML format.

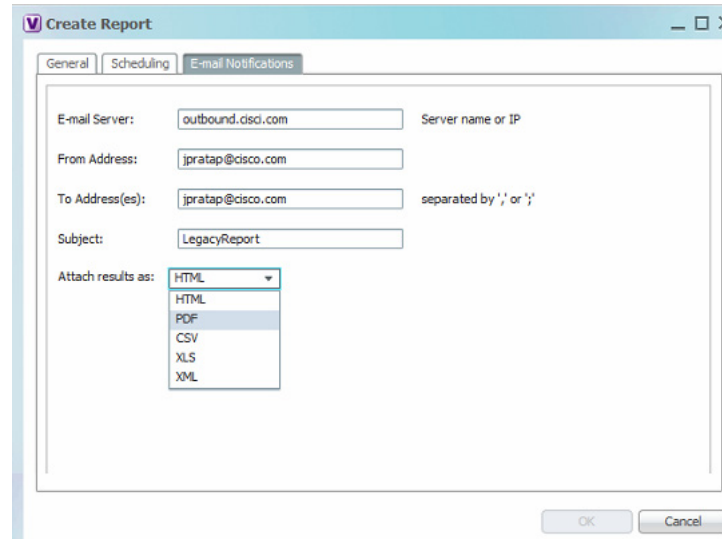To enter criteria and send a report through e-mail notification:

Step 1   Select **Reports > Report Manager. I**n the Reports Manager window, expand either one of the Events Reports, Inventory Reports, or Network Service Reports node.

Note   You can also create and send a report by using the following navigation path:
Select **Reports >Run Report >Events Reports >** click a report
Select **Reports >Run Report >Inventory Reports >** click a report.
Select **Reports >Run Report >Network Service Reports >** click a report.

Step 2   Choose a report **>** right-click a selected report **>** click **Run**. The Create Report page appears.

Figure 5-1   *E-mail Notification Tab*

Step 3   Click the **E-Mail Notifications** tab, enter a valid Email Servers, To-Address, From-Address (es), and Subject details.

> **Note**   If you have configured the **Email Server** and **From Address** in the **Global Report Settings** then those details will be displayed by default.

Step 4   From the **Attach results as** drop-down list, choose a report format to attach in an email.

Step 5   Click **OK** to create a report and to send the report as an attachment.

Sending a Report Through E-mail Notification