CHAPTER 11

Working with Reports

Cisco Prime Network (Prime Network) provides a Report Manager that enables you to schedule, generate, view, and export reports of the information managed by Prime Network. You can save the generated reports in any of the following formats: PDF, CSV, HTML, XLS, and XML.

In addition to a variety of standard reports for events and inventory, you can define reports as required for your environment. The following topics discuss the Report Manager and reports in more detail:

User Roles Required to Manage Reports

This topic identifies the roles that are required to manage reports. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.
- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the *Cisco Prime Network 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 11-1 identifies whether you can generate a report if a selected element **is not in** one of your assigned scopes.
- Table 11-2 identifies whether you can generate a report if a selected element **is in** one of your assigned scopes.
- Table 11-3 identifies the tasks you can perform on the reports that you generate.
- Table 11-4 identifies the tasks you can perform on the reports that someone else generates.
- Table 11-5 identifies the tasks you can perform on report folders.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.10 Administrator Guide*.

Table 11-1 Default Permission/Security Level Required for Generating Reports - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports	—	—	—	—	X
• Detailed Non-Network Events Reports	—	—	—	Partial[1]	X
• All other events reports	—	—	—	—	X
Generate Inventory Reports	—	—	—	—	X
Generate Network Service Reports	—	—	—	—	X

[1] A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Table 11-2 Default Permission/Security Level Required for Generating Reports - Element in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Generate Events Reports					
• Detailed Network Events Reports[1]	X	X	X	X	X
• Detailed Non-Network Events Reports	—	—	—	Partial[2]	X
• All other events reports	X	X	X	X	X
Generate Inventory Reports	X	X	X	X	X
Generate Network Service Reports	X	X	X	X	X

[1] Detailed Ticket reports include only those tickets that have a root cause alarm associated with an element in the user's scope.

[2] A user with the Configurator role can generate Detailed Provisioning Events reports for elements that are in and outside their scope.

Table 11-3 Default Permission/Security Level Required for Working with Reports You Generate

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Tasks					
Schedule reports	X	X	X	X	X
Cancel reports	X	X	X	X	X
Delete reports	X	X	X	X	X
Export reports	X	X	X	X	X
Rename reports	X	X	X	X	X
Save reports	X	X	X	X	X
Set report preferences for purging and sharing	—	—	—	—	X
Share/unshare reports	X[1]	X[1]	X[1]	X[1]	X
View report properties	X	X	X	X	X
View reports	X	X	X	X	X

[1] You can share or unshare reports only if sharing is enabled in Prime Network Administration.

Table 11-4 Default Permission/Security Level Required for Working with Reports Another User Generates

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Tasks					
Schedule reports	—	—	—	—	X
Cancel reports	—	—	—	—	X
Delete reports	—	—	—	—	X
Export reports	—	—	—	—	X
Rename reports	—	—	—	—	X
Save reports	—	—	—	—	X
Set report preferences for purging and sharing	—	—	—	—	X
Share/unshare reports	—	—	—	—	X
View report properties	—	—	—	—	X
View reports	—	—	—	—	X

Table 11-5 Default Permission/Security Level Required for Working with Report Folders

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Report Folder Tasks					
Create folders	X	X	X	X	X
Delete folders[1]	X	X	X	X	X
Move folders[1]	X	X	X	X	X
Rename folders[1]	X	X	X	X	X

Table 11-5 Default Permission/Security Level Required for Working with Report Folders (continued)

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
View report folder properties	X	X	X	X	X
View report type properties	X	X	X	X	X

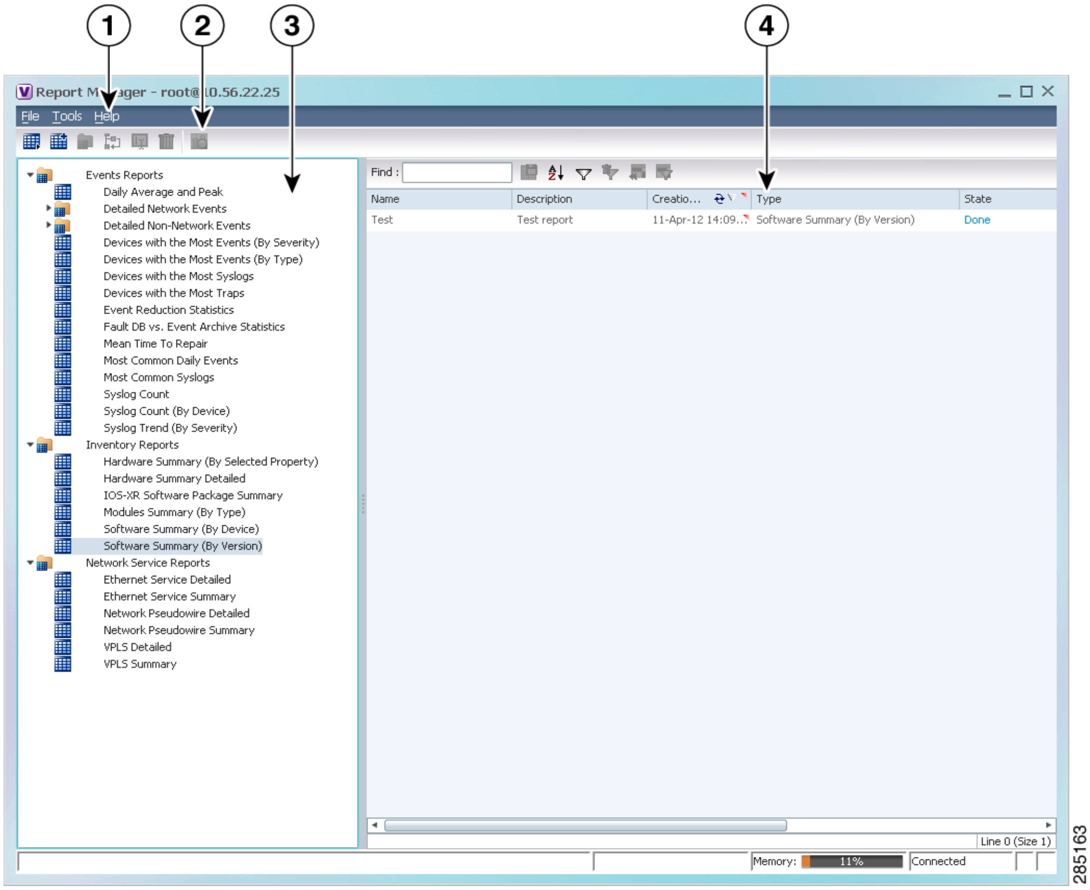
1. You cannot perform this action on system-generated folders, such as the Events Reports folder.

Using the Report Manager

The Report Manager is available from Prime Network Vision, Prime Network Events, and Prime Network Administration by choosing **Reports > Report Manager**. The Report Manager (shown in Figure 11-1) enables you to run standard reports, such as the number of syslogs by device.

The Report Manager also enables you to create reports and folders, view previously generated reports, define report types for your use, and organize reports in a manner suited to your environment and needs.

Figure 11-1 Report Manager Window



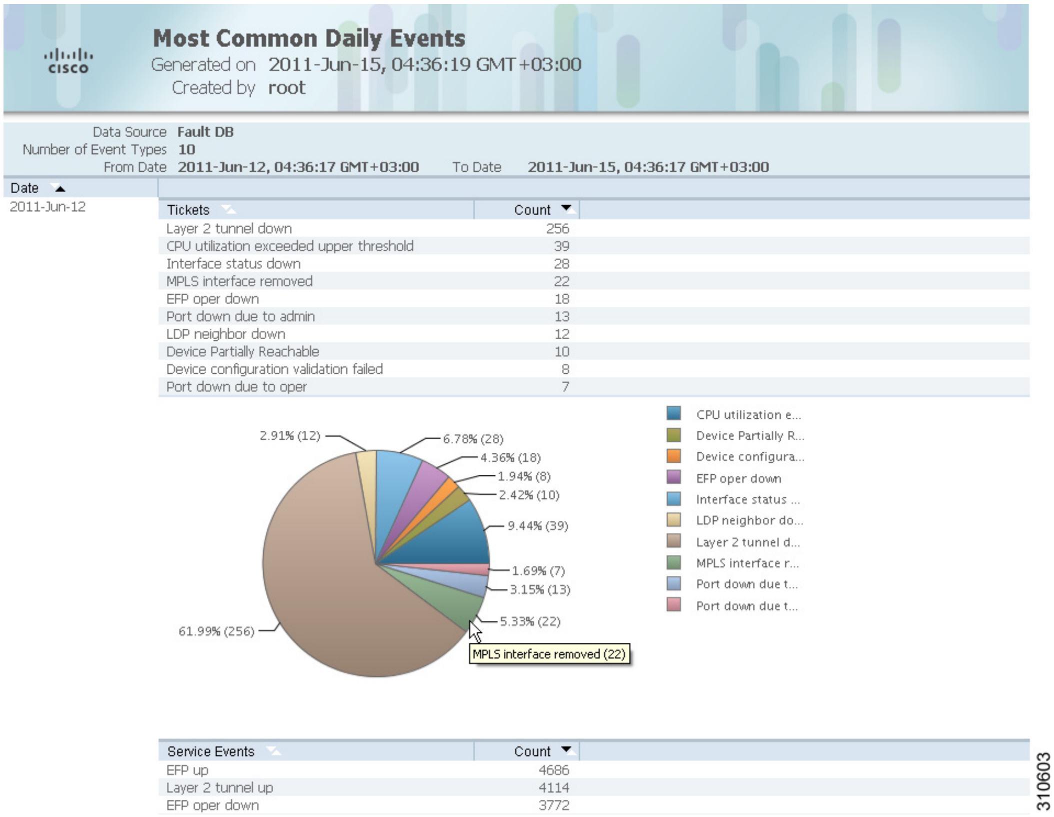
- Events Reports
  - Daily Average and Peak
  - Detailed Network Events
  - Detailed Non-Network Events
  - Devices with the Most Events (By Severity)
  - Devices with the Most Events (By Type)
  - Devices with the Most Syslogs
  - Devices with the Most Traps
  - Event Reduction Statistics
  - Fault DB vs. Event Archive Statistics
  - Mean Time To Repair
  - Most Common Daily Events
  - Most Common Syslogs
  - Syslog Count
  - Syslog Count (By Device)
  - Syslog Trend (By Severity)
- Inventory Reports
  - Hardware Summary (By Selected Property)
  - Hardware Summary Detailed
  - IOS-XR Software Package Summary
  - Modules Summary (By Type)
  - Software Summary (By Device)
  - Software Summary (By Version)
- Network Service Reports
  - Ethernet Service Detailed
  - Ethernet Service Summary
  - Network Pseudowire Detailed
  - Network Pseudowire Summary
  - VPLS Detailed
  - VPLS Summary

Name	Description	Creatio...	Type	State
Test	Test report	11-Apr-12 14:09...	Software Summary (By Version)	Done

1	Menu bar	**3**	Navigation tree with report types and folders
2	Toolbar	**4**	Content pane

Figure 11-2 shows an example of a generated report with a pie chart.

Figure 11-2 Sample Report



Most Common Daily Events
Generated on 2011-Jun-15, 04:36:19 GMT+03:00
Created by root

Data Source **Fault DB**
Number of Event Types **10**
From Date **2011-Jun-12, 04:36:17 GMT+03:00** To Date **2011-Jun-15, 04:36:17 GMT+03:00**

Date ▲
2011-Jun-12

Tickets	Count ▼
Layer 2 tunnel down	256
CPU utilization exceeded upper threshold	39
Interface status down	28
MPLS interface removed	22
EFP oper down	18
Port down due to admin	13
LDP neighbor down	12
Device Partially Reachable	10
Device configuration validation failed	8
Port down due to oper	7

Service Events	Count ▼
EFP up	4686
Layer 2 tunnel up	4114
EFP oper down	3772

Generated reports contain the following information in the report heading:

- Report name
- Date, time, and time zone in which the report was generated
- Name of user who generated the report

Depending on the type of report, the following additional information can appear in the report heading:

- Source of the data, such as the fault or alarm database
- Time period covered by the report
- Number of items included in the report
- Any filters or maps applied to the report

A report might also include a pie chart. If you hover your mouse cursor over a section in the pie chart, a tooltip displays the information associated with that section, such as IP address, number of events, type of event, or percentage of total events.

Note Not all reports include pie charts. In addition, reports that normally include a pie chart do not display a pie chart if the chart exceeds 25 slices.

Menu Options

Table 11-6 describes the menu options available in the Report Manager window.

Table 11-6 Report Manager Menu Options

Option	Description
File Menu	
Exit	Exits the Report Manager window.
Tools Menu	
Change User Password	Enables you to change the password used when logging into the Prime Network client application suite. The change takes effect the next time you log into the application. **Note** The administrator can also change a user password in Prime Network Administration.
Help Menu	
Cisco Prime Network Report Manager Help	Opens the online help for Prime Network Vision and Prime Network Events.
Cisco.com	Unavailable.
About Cisco Report Manager	Displays application information about Prime Network Vision and Prime Network Events.

Report Manager Toolbar

Table 11-7 identifies the buttons that appear in the Report Manager toolbar.

Table 11-7 Report Manager Toolbar Buttons

Icon	Name	Description
	Run	Generates the selected report.
	Define Report of This Type	Enables you to define a report of this type that is suited specifically to your environment.
	New Folder	Creates a new folder.
	Move	Moves one or more folders or reports that you created.

Table 11-7 Report Manager Toolbar Buttons (continued)

Icon	Name	Description
	Rename	Renames a folder that you created.
🗑	Delete	Deletes one or more folders that you created.
🗑	Delete Report	Deletes one or more selected reports.
	View	Displays the selected report in HTML format.

Navigation Tree

The navigation pane displays a tree-and-branch representation of report folders and types of reports. The highest level in the tree displays report folders. The following standard report folders are provided in Report Manager:

- Events Reports
- Inventory Reports
- Network Service Reports

Each folder contains the types of reports that are provided with Prime Network and any user-defined reports. For more information on the standard report types, see Table 11-12.

When you select an item in the tree, the content pane displays the generated reports as follows:

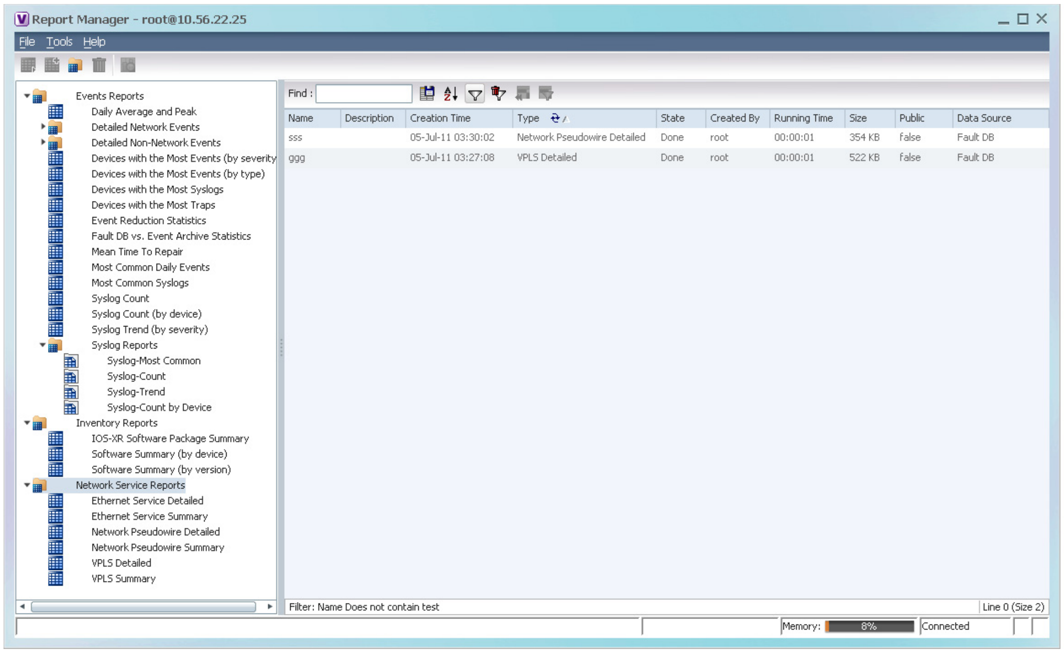
- If you select a folder, the content pane lists all reports that have been generated using any of the report types in that folder.
- If you select a report type, the content pane lists all reports that have been generated of that report type.

Content Pane

The content pane lists all reports generated for the folder or report type selected in the navigation tree. You can double-click a report to view the report in HTML format.

Figure 11-3 shows an example of the content pane.

Figure 11-3 Reports Manager Content Pane



- Events Reports
  - Daily Average and Peak
  - Detailed Network Events
  - Detailed Non-Network Events
  - Devices with the Most Events (by severity
  - Devices with the Most Events (by type)
  - Devices with the Most Syslogs
  - Devices with the Most Traps
  - Event Reduction Statistics
  - Fault DB vs. Event Archive Statistics
  - Mean Time To Repair
  - Most Common Daily Events
  - Most Common Syslogs
  - Syslog Count
  - Syslog Count (by device)
  - Syslog Trend (by severity)
  - Syslog Reports
    - Syslog-Most Common
    - Syslog-Count
    - Syslog-Trend
    - Syslog-Count by Device
- Inventory Reports
  - IOS-XR Software Package Summary
  - Software Summary (by device)
  - Software Summary (by version)
- Network Service Reports
  - Ethernet Service Detailed
  - Ethernet Service Summary
  - Network Pseudowire Detailed
  - Network Pseudowire Summary
  - VPLS Detailed
  - VPLS Summary

Name	Description	Creation Time	Type	State	Created By	Running Time	Size	Public	Data Source
sss		05-Jul-11 03:30:02	Network Pseudowire Detailed	Done	root	00:00:01	354 KB	false	Fault DB
ggg		05-Jul-11 03:27:08	VPLS Detailed	Done	root	00:00:01	522 KB	false	Fault DB

Filter: Name Does not contain test

Line 0 (Size 2)

Memory: 8%

Connected

Table 11-8 describes the information displayed in the content pane for each report.

Table 11-8 Reports Manager Content Pane Information

Attribute	Description
Name	Name of the report. Double-click the report to view the report in HTML format.
Description	Brief description of the report.
Creation Time	Date and time when the report was generated.
Type	Report type.
State	State of the report: Running, Done, Canceled, or Failed. For more information about the Failed state, see Generating Reports, page 11-23.
Created By	User who created the report.
Running Time	Amount of time it takes for the report to be complete.
Size	Report size.

Table 11-8 Reports Manager Content Pane Information (continued)

Attribute	Description
Public	Availability of the report to other users: • True—The report is available to all users. • False—The report is available to only the user who generated the report and the administrator.
Data Source	Source of the information for the report: Fault Database, Event Archive, or Network Elements.

Note Reports are purged from Prime Network after 90 days by default. This setting can be modified by changing the setting in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide.*

Right-Click Options

Right-click options are available for:

- Navigation Pane Folders, page 11-9
- Navigation Pane Reports, page 11-10
- Content Pane Reports, page 11-10

Navigation Pane Folders

Table 11-9 describes the options available when you right-click a folder in the navigation pane.

Table 11-9 Report Manager Navigation Pane Folder Right-Click Options

Option	Description
New Folder	Creates a new folder.
Delete	Deletes a user-defined folder.
Rename	Renames a user-defined folder.
Move	Moves a user-defined folder.
Properties	Displays the Folder Properties window which lists the folder contents. For more information on the Reports Category Properties window, see Viewing Folder and Report Type Properties, page 11-48.

Navigation Pane Reports

Table 11-10 describes the options available when you right-click a report in the navigation pane.

Table 11-10 Report Manager Navigation Pane Report Right-Click Options

Option	Description
Run	Displays the Run Report dialog box so you can run a report of this type specifically for your environment and adds the generated report to the table in the content pane.
Define Report of This Type	This option is available only for Cisco-supplied report types. Displays the Define Report dialog box so you can create a report of this type specifically for your environment, and adds the newly defined report to the navigation tree.
Delete	Deletes a user-defined report.
Move	Moves a user-defined report.
Properties	For a standard report type, displays the Reports Type Properties window which includes a brief description of the report and enables you to generate the report. For more information on the Reports Type Properties window, see Viewing Report Properties, page 11-45. For a user-defined report, displays the Edit report dialog box so that you can modify the currently defined settings and generate the report.

Content Pane Reports

Table 11-11 describes the options available when you right-click a report in the content pane.

Table 11-11 Report Manager Content Pane Report Right-Click Options

Option	Description
View As	Displays the report in the selected format: • HTML • PDF • CSV • XLS • XML The default option, HTML, is displayed in bold font. For more information on viewing reports, see Viewing and Saving Reports, page 11-41.
Rename	Renames the selected report.

Table 11-11 Report Manager Content Pane Report Right-Click Options (continued)

Option	Description
Share or Unshare	Shares the selected reports or limits them to your viewing only. The option toggles between Share and Unshare, as appropriate for the selected reports. By default, the Share and Unshare options are available only to users with administrator access. These options are available to other users only if an administrator has enabled sharing in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Delete Report	Deletes the selected reports.
Cancel	This option is displayed only while the selected report is being generated or queued. Cancels the report that is being generated or is queued.
Show Only Selected Rows	Displays only the rows that you select.
Show All Rows	Displays all table rows that meet the current filtering criteria.
Properties	Displays the Reports Type Properties window, which includes a brief description of the report and enables you to edit its name and description.

Report Categories

Prime Network Vision provides reports related to:

- Events—See Events Reports, page 11-11.
- Inventory—See Inventory Reports, page 11-19.
- Network services—See Network Service Reports, page 11-21.

Events Reports

Prime Network Vision provides the following standard event report types:

- General report types, as described in Table 11-12.
- Detailed network event reports, as described in Table 11-13.
- Detailed non-network event reports, as described in Table 11-14.

Table 11-12 Standard Events Report Types

Report Name	Description	Data Source
Daily Average and Peak	For each day of the specified time period, the peak number and average rate of syslogs and traps for each of the following time periods: • Second • Ten seconds • Minute • Hour • Day	Fault database
Database Monitoring	For regular time intervals: • Number of active tickets • Number of active alarms • Number of active events • Number of unconnected events • Number of auto-archive candidates • Number of notifications • Biggest Ticket ID • Number of event count in the biggest ticket • Actionable Event rate per second • Number of dangling events handled by the integrity process • Number of tickets created by the integrity process	Fault Database
Devices with the Most Events (By Severity)	For the specified number of devices with the most events, the following information for each device for the specified time period: • Severity of the events associated with the device, sorted by severity • Number of events for each severity A pie chart presents the information by device and percentage in a graphical format.	Fault database
Devices with the Most Events (By Type)	For the specified number of devices with the most events, the following information for each device for the specified time period: • Type of events associated with the device • Number of events received for each event type A pie chart presents the information by device and percentage in a graphical format.	Fault database

Table 11-12 Standard Events Report Types (continued)

Report Name	Description	Data Source
Devices with the Most Syslogs	For the specified number of devices with the most syslogs, the number of syslog messages for each device for the specified time period. You can run this report on the Prime Network fault database or the event archive. A pie chart presents the information by device and percentage in a graphical format.	User choice: • Fault database • Event archive
Devices with the Most Traps	For the specified number of devices with the most traps, the number of traps associated with each device for the specified time period. You can run this report on the fault database or the event archive. A pie chart presents the information by device and percentage in a graphical format.	User choice: • Fault database • Event archive
Event Reduction Statistics	For the specified devices and time period: • Names of those tickets with: – The root cause in the device list – The ticket creation time within the specified period • For each ticket type identified: – Number of tickets of that type – Fewest number of correlated events – Highest number of correlated events – Average number of correlated events	Fault database
Events Troubleshooting Info	Provides the following information: • State—The event condition. • Troubleshooting—The probable cause, action to be taken, and the clearing condition.	Fault database
Fault DB vs. Event Archive Statistics	For each day in the specified time period, the number of each of the following items in the fault database and the event archive: • Syslogs • Traps • Tickets • Correlated events • Uncorrelated events • Nonnetwork events • Network-originated events • Network-originated and service events	Fault database and event archive

Table 11-12 Standard Events Report Types (continued)

Report Name	Description	Data Source
Mean Time to Repair	For the specified devices and time period: • Names of those tickets with: – The root cause in the device list – The ticket creation time within the specified period • For each ticket type identified: – Whether the tickets were cleared by the user or network – Number of tickets – Minimum time (in seconds) to repair – Maximum time (in seconds) to repair – Average time (in seconds) to repair **Note** The time to repair is based on the ticket creation time and the time the ticket was last modified. For example, if you acknowledge a ticket after it has been cleared. the acknowledgement time affects the time to repair for that ticket.	Fault database
Most Common Daily Events	For each day in the specified time period: • Specified number of most common tickets, service events, syslogs, and traps • Number of each type of ticket, service event, syslog, and trap • If selected, a pie chart presenting the events by percentage in a graphical format	Fault database
Most Common Syslogs	Most common syslog messages and the number of each for the specified time period and devices. A pie chart presents the information by syslog message and percentage in a graphical format.	Fault database
Syslog Count	Number of syslog messages by type for the specified time period with the times of the first and last occurrences. A pie chart presents the information by syslog message and percentage in a graphical format.	Fault database
Syslog Count (By Device)	For each device, the type and number of each syslog message and the times of the first and last occurrences for each type. A pie chart presents the information by device and percentage in a graphical format.	Fault database
Syslog Trend (By Severity)	For the specified devices, the trend of specified syslog messages in graph format: • By priority • For the specified time period • At the specified intervals	Fault database

Table 11-13 Detailed Network Events Report Types

Report Name	Description	Data Source
Detailed Event Count (By Device)	For each device, the following information for the specified time period: • For syslogs: – Syslog severities – Number of syslogs per severity – Syslog type – Number of each syslog type • For traps: – Trap severities – Number of traps per severity – Trap type – Number of each trap type • For tickets: – Ticket severities – Number of tickets per severity – Ticket type – Number of each ticket type You can select a maximum of 1000 devices for this report.	Fault database
Detailed Service Events	For each service event of the specified severities, time period, and devices: • Event severity • Event identifier • Timestamp • Brief and detailed descriptions • Device on which the event occurred • Alarm identifier • Ticket identifier • Causing event identifier • Duplication count • Reduction count	Fault database

Table 11-13 Detailed Network Events Report Types (continued)

Report Name	Description	Data Source
Detailed Syslogs	For each device that is selected, the following information from the event archive for the specified time period: • IP address • Date and time of each syslog, in ascending order • Syslog raw data or description, depending on the data source The maximum number of syslogs retrieved for this report is 250,000.	User selection: Event archive or fault database
Detailed Tickets	For each ticket of the specified severities, time period, and device: • Ticket severity • Ticket identifier • Last modification time • Root event time • Description • Entity that caused the alarm • Whether or not the ticket is acknowledged • Ticket creation time • Event count • Affected devices count • Duplication count • Reduction count • Alarm count	Fault database
Detailed Traps	For each managed device that is selected, the following information for the specified time period: • IP address • Time of trap • SNMP version • Trap description • Generic or device-specific trap OID, if the source is the event archive • Long description, if the data source is the fault database 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.	User Selection: Event archive or fault database

Table 11-14 Detailed Non-Network Events Report Types

Report Name	Description	Data Source
Detailed Audit Events	For each audit event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Command name • Command signature • Command parameters • Originating IP address • Username	Fault database
Detailed Provisioning Events	For each provisioning event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location • Username • Device username • Status	Fault database

Table 11-14 Detailed Non-Network Events Report Types (continued)

Report Name	Description	Data Source
Detailed Security Events	For each security event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location • Username • Originating IP address	Fault database
Detailed System Events	For each system event included in the report for the specified time period, severities, and search criteria: • Event severity • Event identifier • Timestamp • Description • Location	Fault database

Inventory Reports

Table 11-15 describes the standard inventory report types provided by Prime Network Vision and the data source.

Table 11-15 Standard Inventory Report Types

Report Name	Description	Data Source
Hardware Detailed	For each device included in the report: • IP address • Device series • Element type You can view other hardware information for each device by selecting the required items from the available list as given below: • Chassis—chassis description, chassis serial number, shelf description, shelf serial number, and shelf status • Module—module name, sub module name, module status, hardware type, and hardware version • Port—port location, port type, porting sending alarm, port alias, port status, port managed, PID, and pluggable type serial number.	Network elements
Hardware Summary	For each device included in the report: • IP address • System name • Serial number • Element type • Device series • Vendor • Product • Chassis You can group the report contents by vendor, product, device series, element type, system name, or chassis and specify part or whole of the selected entity, if required.	Network elements

Table 11-15 Standard Inventory Report Types (continued)

Report Name	Description	Data Source
IOS-XR Software Package Summary	For each device included in the report: • Device name • Element type • IP address • Serial number • Cisco IOS XR software version • For each software package installed on the device: – Storage location – Software package name – Module name – Software package state: Active or Inactive	Network elements
Modules Summary (By Type)	For each device filtered by module type: • IP address • Module serial number • Module hardware version • Module software version You can filter the report contents by specifying part or whole of the module type.	Network elements
Software Summary (By Device)	For each device included in the report: • Device name • Element type • IP address • Serial number • Software version on the device • Name of image file	Network elements
Software Summary (By Version)	For each software version included in the report: • Number of devices running the version • Device names • Element types • Device IP address • Device serial number • Name of image file	Network elements

Network Service Reports

Table 11-16 describes the standard network service report types provided by Prime Network Vision and the data source.

Table 11-16 Standard Network Service Report Types

Report Name	Description	Data Source
Ethernet Service Detailed	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Ethernet service or Layer 2 VPN • Edge EFPs associated with the EVC or Layer 2 VPN • EFD fragment names • EFD fragment type You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name	Fault database
Ethernet Service Summary	For each Ethernet service in the report: • Ethernet service or Layer 2 VPN name • Business tag assigned to the Ethernet service or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Ethernet service or Layer 2 VPN You can filter report content by specifying part or all of the: • Ethernet service name • EVC name • Ethernet service business tag • EVC business tag • Map name	Fault database

Table 11-16 Standard Network Service Report Types (continued)

Report Name	Description	Data Source
Network Pseudowire Detailed	For each network pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps containing the pseudowire • Pseudowire details • Type of pseudowire, such as pseudowire edge, Ethernet flow point, or switching entity You can filter report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name	Fault database
Network Pseudowire Summary	For each network pseudowire in the report: • Pseudowire name • Pseudowire type • Business tag assigned to the pseudowire • Maps containing the pseudowire You can filter the report content by specifying part or all of the: • Pseudowire name • Pseudowire type • Business tag • Map name	Fault database

Table 11-16 Standard Network Service Report Types (continued)

Report Name	Description	Data Source
VPLS Detailed	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag associated with the VPLS or H-VPLS instance • Maps containing the VPLS or H-VPLS instance • VPLS details • Type of VPLS service, such as VPLS forward, access EFP, or core pseudowire You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name	Fault database
VPLS Summary	For each VPLS or H-VPLS instance in the report: • VPLS or H-VPLS name • Business tag assigned to the VPLS or H-VPLS instance • Maps containing the VPLS or H-VPLS instance You can filter report content by specifying part or all of the: • VPLS or H-VPLS name • Business tag • Map name	Fault database

Generating Reports

You can generate reports in any of the following ways:

- Generating Reports from Report Manager, page 11-24
- Generating Reports from the Reports Menu, page 11-38
- Generating Reports from Prime Network Vision, page 11-39

You can generate reports only for devices that are within your scope.

Note Report Manager generates reports up to 150 MB in size. If you generate a report that exceeds this limit:

- Report Manager window displays Failed in the State column.
- An error message is entered in the log stating that the report failed because the resulting output is too large.

To run the report successfully, enter more specific report criteria or limit the time period covered by the report.

Database Load and Report Generation

If you generate reports while Prime Network Vision is working under a database load, the reports move to a *Load* mode which is indicated by a system event. While Prime Network Vision is in Load mode, the reports currently running are cancelled and new reports are queued.

After Prime Network Vision returns to normal operation and is no longer operating under a load, a new system event is generated and the queued reports start running.

Report Generation Failure

If a report fails to generate successfully, the State column contains the word *Failed*. Click **Failed** to view the reason for the failure. A window is displayed with the cause of the failure, such as *The disk space allocated for report storage is full* or *AVM 84 was restarted while the report was running*.

Report Generation Canceled

If a report is canceled before it completes, the State column contains the word *Canceled*. Click **Canceled** to view the reason for the cancellation. A window is displayed with the cause of the cancellation, such as *The report was canceled by user <user-name>* or *The report was canceled by the system to prevent system overload*.

Generating Reports from Report Manager

Prime Network Vision provides three report categories as described in Report Categories, page 11-11. The information that you need to provide when generating a report depends on the report type. The following topics describe the information required to generate each report type:

- Generating Events Reports, page 11-24
- Generating Inventory Reports, page 11-32
- Generating Network Service Reports, page 11-35

Note You can generate reports only for devices that are within your scope.

Generating Events Reports

To generate an events report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

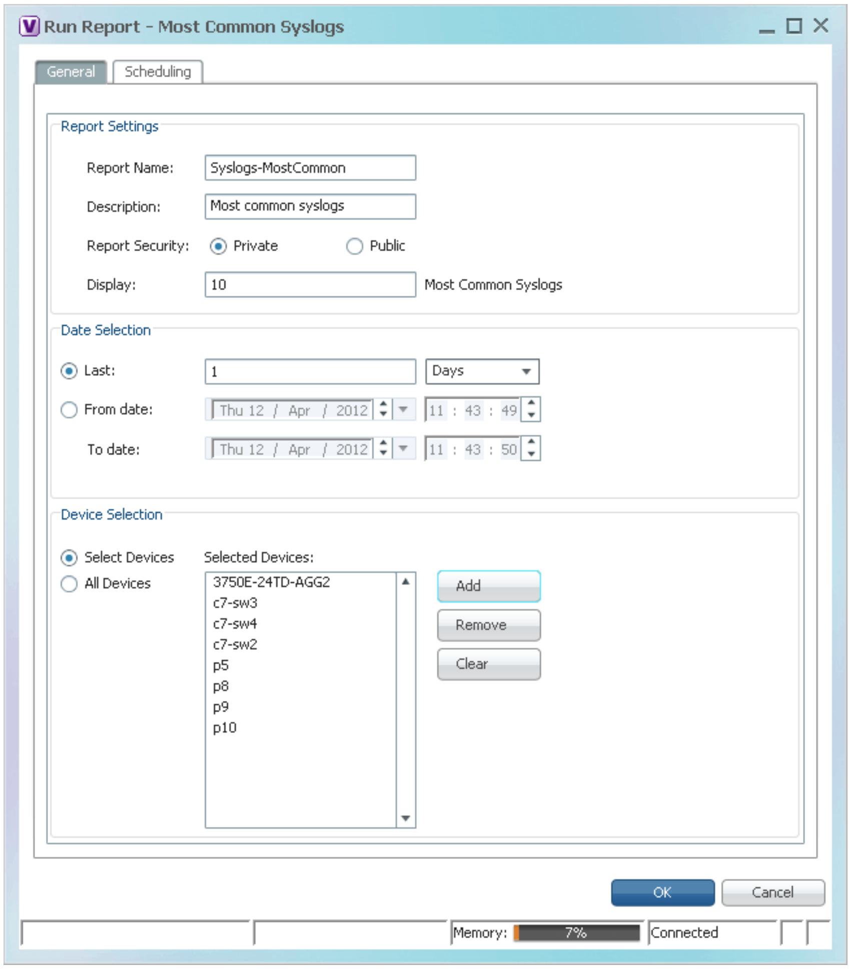
Step 2 In the Report Manager window, choose **Events Reports >** *report-type*.

For information on the reports available for events, see Table 11-12.

Step 3 Generate the report by right-clicking the report type, then choosing **Run**.

The Run Report dialog box is displayed. An example is shown in Figure 11-4. The fields displayed in the Run Report dialog box vary depending on the type of report.

Figure 11-4 Events Report - Run Report Dialog Box



Run Report - Most Common Syslogs

General | Scheduling

Report Settings

Report Name: Syslogs-MostCommon

Description: Most common syslogs

Report Security: ● Private ○ Public

Display: 10 Most Common Syslogs

Date Selection

● Last: 1 Days

○ From date: Thu 12 / Apr / 2012 11 : 43 : 49

To date: Thu 12 / Apr / 2012 11 : 43 : 50

Device Selection

● Select Devices
○ All Devices

Selected Devices:
3750E-24TD-AGG2
c7-sw3
c7-sw4
c7-sw2
p5
p8
p9
p10

Step 4 In the Run Report dialog box, specify the report settings as follows:

- For standard events reports, use the information in Table 11-17.
- For detailed network reports, use the information in Table 11-18.
- For detailed non-network reports, use the information in Table 11-19.

Table 11-17 Events Report - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Display *n*	This field does not appear for all reports. Enter the number of items to be displayed in the generated report.
Data Source	This field does not appear for all reports. Select the source of information to use for the report: Fault Database or Event Archive.
Include pie charts in report output	This field does not appear for all reports. Check the check box to view pie charts in the report with the standard numerical output.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click **From Date**. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.

Table 11-17 Events Report - Run Report Dialog Box Fields (continued)

Option	Description
Device Selection	
Select Devices	**Note** • You can add only those devices that are within your scope. • A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All Devices	This field does not appear for all reports. Click **All Devices** to include all devices in your scope in the report.
Syslog Trend (by Severity) Report—Additional Report Specifications	
Intervals	In the Grouped by drop-down list, choose the unit of time to use for tracking the trend: Seconds, Minutes, Hours, or Days.
Severity	Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Syslog Messages	Specify the syslog messages to be included in the report: • To include selected syslog messages in the report, in the list of syslog messages on the left, select the required syslog messages, and then click **Add Selected** to move them to the list of syslog messages on the right. • To include all syslog messages in the report, click **Add All**. To find syslog messages that match a string, enter the string in the Find field. The list of syslog messages is automatically updated to include only those messages that contain the string you enter. Click the **Sort Order** button to sort the syslog messages in alphabetic or reverse alphabetic order.

Table 11-18 Detailed Network Events Reports - Run Report Dialog Box Fields

Option	**Description**
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Data Source	This field does not appear for all reports. Select the source of information to use for the report: Fault Database or Event Archive.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: **1.** Click **From Date**. **2.** In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. **3.** Enter a time for the start date, using the format HH MM SS. **4.** In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. **5.** Enter a time for the end date, using the format HH MM SS.

Table 11-18 Detailed Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Device Selection	
Select Devices	**Note** • You can add only those devices that are within your scope. • A user with the Administrator role can select unmanaged devices (by IP address) for reports that run on the Event Archive. • The Detailed Event Count (by device) report accepts a maximum of 1000 devices. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All Devices	This field does not appear for all reports. Click **All Devices** to include all devices in your scope in the report.
Severity	
Severity	This field does not appear for all reports. Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Detailed Service Events Report—Additional Report Specifications	
Description Contains	Enter the string that the service event must contain to be included in the report.
Detailed Syslogs Report—Additional Report Specifications	
Syslogs Description	This field is displayed if you choose Fault DB for the data source. In the Description Contains field, enter the string that the syslog must contain to be included in the report.
Syslogs Raw Data	This field is displayed if you choose Event Archive for the data source. In the Raw Data Contains field, enter the string that the syslog raw data must contain to be included in the report.

Table 11-18 Detailed Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Detailed Traps Report—Additional Report Specifications	
Traps Detailed Description	In the Description Contains field, enter the string that the trap must contain to be included in the report.
Long Description	This option is enabled if you choose Fault DB for the data source. 1. Check the Show Long Description check box to include the long description in the report. 2. In the Long Description Contains field, enter the string that the long description must contain to be included in the report.
SNMP Version	Specify the SNMP versions to include in the report: All, 1, 2, or 3.
Generic	This option is enabled if you choose Event Archive for the data source. Specify the generic traps to include in the report: 1. Select the generic traps to include in the report: – All—Include all generic traps – 0—coldStart – 1—warmStart – 2—linkDown – 3—linkUp – 4—authenticationFailure – 5—egpNeighborLoss – 6—enterpriseSpecific 2. If you select generic type 6, enter the OIDs (comma separated) in the Vendor Specific field. The Vendor Specific field accepts a maximum of 125 digits.

Table 11-19 Detailed Non-Network Events Reports - Run Report Dialog Box Fields

Option	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Date Selection	
Last	Specify the length of time before the current date and time, and the unit of measure: seconds, minutes, hours, days, weeks, or months.
From Date To Date	Specify the date range for the report: 1. Click **From Date**. 2. In the From date field, enter the start date for the time period, or click the drop-down arrow to select the start date from a calendar. 3. Enter a time for the start date, using the format HH MM SS. 4. In the To Date field, enter the end date for the time period, or click the drop-down arrow to select the end date from a calendar. 5. Enter a time for the end date, using the format HH MM SS.
Severity	
Severity	Check the check boxes of the syslog message severities to be included in the report: All, Critical, Major, Minor, Warning, Cleared, Information, and Indeterminate.
Detailed Audit Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.
Command Name Contains	Enter the string that the command name must contain to be included in the report.
Originator IP Contains	Enter the string that the originating IP address must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.

Table 11-19 Detailed Non-Network Events Reports - Run Report Dialog Box Fields (continued)

Option	Description
Detailed Provisioning Events Report—Additional Report Specifications	
Description Contains	Enter the string that the trap must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.
Status	Choose the statuses to be included in the report: All, Unknown, Configuring, Success, and Fail.
Detailed Security Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.
Originator IP Contains	Enter the string that the originating IP address must contain to be included in the report.
User Name Contains	Enter the string that the username must contain to be included in the report.
Detailed System Events Report—Additional Report Specifications	
Description Contains	Enter the string that the event must contain to be included in the report.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 11-39.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Inventory Reports

To generate an inventory report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

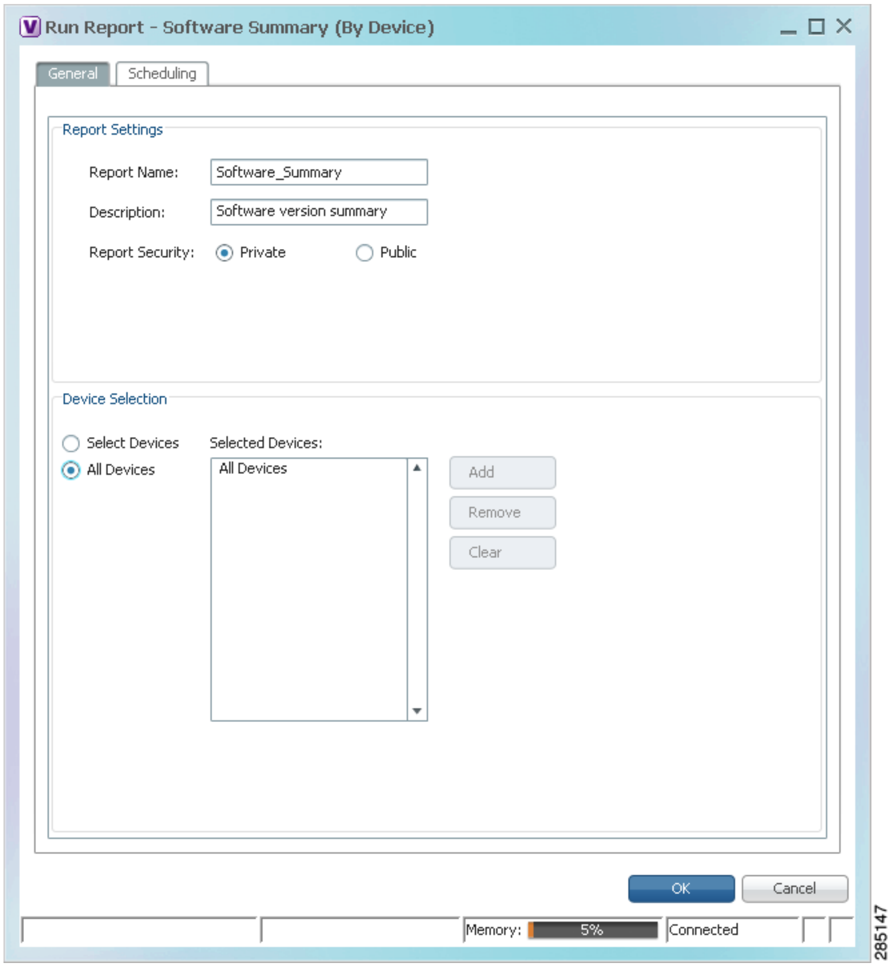
Step 2 In the Report Manager window, choose **Inventory Reports >** *report-type*.

For information on the standard reports available for inventory, see Table 11-15.

Step 3 Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 11-5.

Figure 11-5 Inventory Report - Run Report Dialog Box



Run Report - Software Summary (By Device)

Report Settings

Report Name: Software_Summary

Description: Software version summary

Report Security: ● Private ○ Public

Device Selection

○ Select Devices

● All Devices

Selected Devices: All Devices

Memory: 5%

Connected

Step 4 Enter the required information in the Run Report dialog box as described in Table 11-20.

Table 11-20 Inventory Report - Run Report Dialog Box Fields

Field	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.

Table 11-20 Inventory Report - Run Report Dialog Box Fields (continued)

Field	Description
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Device Selection	
Select Devices	**Note** You can add only those devices that are within your scope. Select devices to include in the report: 1. Click **Select Devices**. 2. Click **Add**. 3. In the Add Network Element dialog box, select devices using either of the following methods: – To select devices that meet specific criteria, click **Search** and enter the required criteria. – To select from all network elements, click **Show All**. 4. In the list of displayed elements, select the network elements that you want to include in the report. You can select multiple network elements at a time. 5. Click **OK**.
All devices	Click **All Devices** to include all devices in your scope in the report.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 11-39.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Network Service Reports

If you generate a detailed network service report on a large-scale setup, a message is displayed in the Run Report dialog box recommending that you apply a filter to limit the size of the report.

To generate a network service report using Report Manager:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports > Report Manager**.

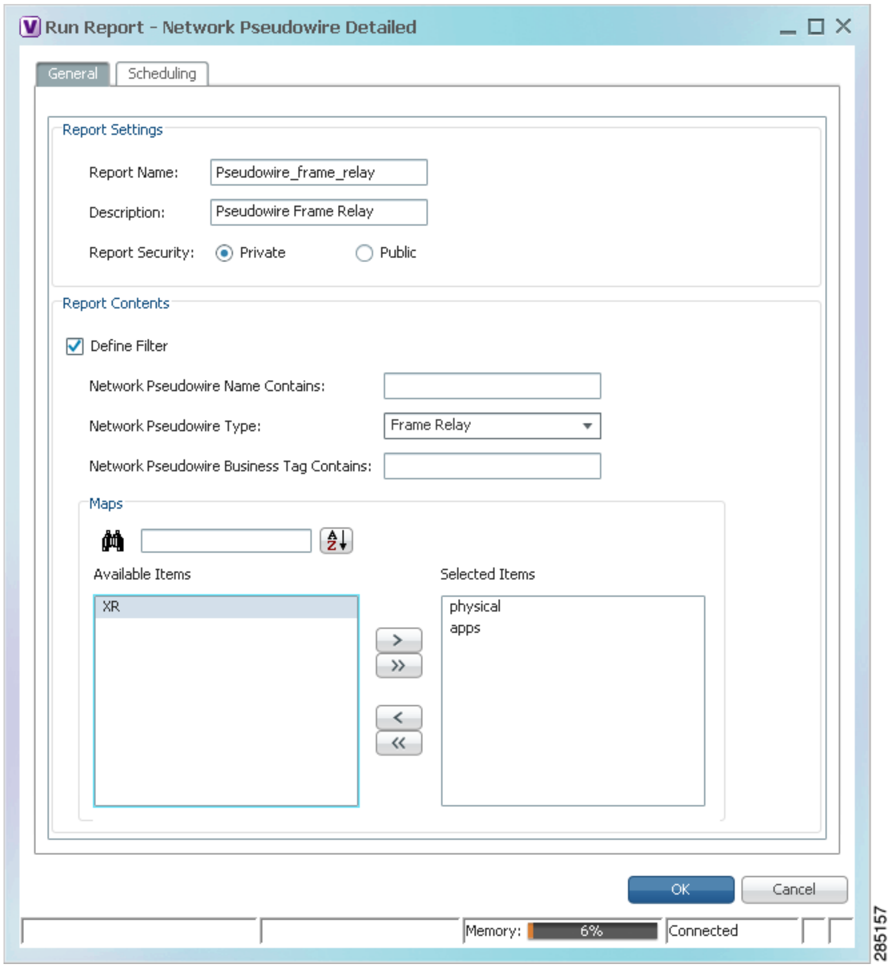
Step 2 In the Report Manager window, choose **Network Service Reports >** *report-type*.

For information on the standard reports available for network services, see Table 11-16.

Step 3 Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed as shown in Figure 11-6.

Figure 11-6 Network Service Report - Run Report Dialog Box



Run Report - Network Pseudowire Detailed

Report Settings

Report Name: Pseudowire_frame_relay

Description: Pseudowire Frame Relay

Report Security: ● Private ○ Public

Report Contents

☑ Define Filter

Network Pseudowire Name Contains:

Network Pseudowire Type: Frame Relay

Network Pseudowire Business Tag Contains:

Maps

Available Items	Selected Items
XR	physical apps

Memory: 6% Connected

Step 4 Enter the required information the Run Report dialog box as described in Table 11-21.

Table 11-21 Network Service Report - Run Report Dialog Box Fields

Field	Description
Report Settings	
Report Name	Enter a unique name for the report, from 1 to 150 characters in length. Report names cannot include the following characters: ;?<>/:\"#*|.
Description	Enter a brief description of the report.
Report Security	This field is displayed only if report sharing is enabled in Prime Network Administration. Indicate the level of security for the report by clicking the appropriate option: • Private—The report can be viewed and used only by the report creator and the administrator. • Public—The report can be viewed and used by all other users, regardless of whether the devices are listed in the report are in the user's scope. **Note** You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.
Ethernet Service Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
Ethernet Service Name Contains	Enter a string that must appear in the Ethernet service name for the Ethernet service to be included in the report.
EVC Name Contains	Enter a string that must appear in the EVC name for the EVC to be included in the report.
Ethernet Service Business Tag Contains	Enter a string that must appear in the Ethernet service business tag for the Ethernet service to be included in the report.
EVC Business Tag Contains	Enter a string that must appear in the EVC business tag for the EVC to be included in the report.
Maps	Specify the maps to include in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.

Table 11-21 Network Service Report - Run Report Dialog Box Fields (continued)

Field	Description
Network Pseudowire Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
Network Pseudowire Name Contains	Enter a string that must appear in the network pseudowire name for the pseudowire to be included in the report.
Network Pseudowire Type	In the drop-down list, choose the type of network pseudowire to be included in the report.
Network Pseudowire Business Tag Contains	Enter a string that must appear in the network pseudowire business tag for the pseudowire to be included in the report.
Maps	Specify the maps to include in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.
VPLS Reports—Report Contents	
Define Filter	Check the **Define Filter** check box to enter criteria that must be matched for inclusion in the report. You can specify match criteria in any or all of the following fields.
VPLS Name Contains	Enter a string that must appear in the VPLS name for the VPLS or H-VPLS to be included in the report.
VPLS Business Tag Contains	Enter a string that must appear in the VPLS business tag for the VPLS or H-VPLS to be included in the report.
Maps	Specify the maps to be included in the report: • To include specific maps in the report, in the list of maps on the left, select the required maps, and then click **Add Selected** to move them to the list of maps on the right. • To include all maps in the report, click **Add All**. To find maps that match a string, enter the string in the Find field. The list of maps is automatically updated to include only those maps that contain the string you enter. Click the **Sort Order** button to sort the maps alphabetically or in reverse alphabetic order.

Step 5 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 11-39.

Step 6 Click **OK**.

The report appears in the table in the content pane with a state of Running, if the report is scheduled to run immediately, or Scheduled, if the report is scheduled to run at a later point in time. When the report is complete, the state changes to Done.

You can view the reports when the state is Done. Occasionally, some report formats require additional time for generation. If so, a progress bar is displayed, indicating that the report is being created and will be available soon.

If the report exceeds 150 MB, the state changes to Failed and an error message is written to the log. We recommend running the report with more specific criteria or a shorter time period to avoid this situation.

If no data is found for the report, the report states that no results were found.

Generating Reports from the Reports Menu

To generate reports quickly and without opening the Reports Manager window, choose **Reports > Run Report >** *folder* **>** *report-type*. The menus include all standard folders and reports, and any folders or reports that you have created. After entering the required information, you can view the report as soon as it is generated or at a later time.

Note You can generate reports only for devices that are within your scope.

To generate a report from the Reports menu:

Step 1 Choose **Reports > Run Report >** *folder* **>** *report-type* where:

- *folder* is the required folder.
- *report-type* is the required type of report.

Step 2 In the Run Report dialog box, enter the required information. For more information on the options in the Run Report dialog box, see Generating Reports, page 11-23.

Step 3 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 11-39.

Step 4 Click **OK**.

Step 5 In the Running Report dialog box, select the required viewing options:

a. Check the **Open Report Manager to monitor status** check box to open the Report Manager window so that you can view the report generation process. Uncheck the check box to proceed without opening the Report Manager window.

b. Check the **View report immediately upon completion** check box to view the report as soon as it is generated. If you enable this option, the report is displayed in HTML format as soon as it is complete. Uncheck the check box to view the report at a later time by using Report Manager.

Step 6 Click **OK**.

Depending on your selections in Step 5, the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.

Generating Reports from Prime Network Vision

Prime Network Vision enables you to run reports on selected devices from the map and list views.

Note You can generate reports only for devices that are within your scope.

To generate a report from Prime Network Vision:

Step 1 In Prime Network Vision, select the required devices in the map or list view.

Step 2 In the navigation tree or content pane, right-click the selected devices, then choose **Run Report** > *folder* > *report-type*.

Step 3 In the Run Report dialog box, enter the required information as described in Generating Reports, page 11-23.

The devices that you select in the navigation pane or content pane are automatically included in the report.

Step 4 To schedule a report to run immediately or at a later point in time, click the **Scheduling** tab. For more information, see Scheduling Reports, page 11-39.

Step 5 Click **OK**.

Step 6 In the Running Report dialog box, specify the desired viewing options:

a. Check the **Open Report Manager to monitor status** check box to open the Report Manager window so that you can view the report generation process. Uncheck the check box to proceed without opening the Report Manager window.

b. Check the **View report immediately upon completion** check box to view the report as soon as it is generated. If you enable this option, the report is displayed in HTML format as soon as it is complete. Uncheck the check box to view the report at a later time by using Report Manager.

Depending on your selections in Step 6, the Report Manager window is displayed, the report is displayed, or the report is available for viewing at a later time.

Scheduling Reports

Prime Network allows you to schedule a report to run immediately or at a later point in time.

To schedule a report:

Step 1 In Prime Network Vision, Prime Network Events, or Prime Network Administration, choose **Reports** > **Report Manager**.

Step 2 In the Report Manager window, choose *report-category* > *report-type*.

For information on the various report categories and report types, see Report Categories, page 11-11.

Step 3 Right-click the report type, then choose **Run**.

The Run Report dialog box is displayed.

Step 4 In the Settings tab, specify the required report criteria. For more information on the options in the Run Report dialog box, see Generating Reports, page 11-23.

Step 5 Click the **Scheduling** tab. By default, the Run Now option is selected and the report is scheduled to run immediately.

Step 6 To schedule the report for a later date/time:

a. Select the **Schedule Job** radio button. The scheduling options Once and Recurring are enabled.

b. To generate the report once, select the **Once** radio button and specify the date and time when you want the report to be generated.

c. To generate the report on a recurring basis, select the **Recurring** radio button and specify the following:

  – The date and time range for the recurrence.

  – How often you want to generate the report within that time range - every X minutes, daily, weekly, or monthly.

Step 7 Specify comments, if required and click **Schedule**. Prime Network creates a report job and executes it according to your scheduling specifications. Go to the **Scheduled Jobs** page (**Tools** > **Scheduled Jobs**), to check that your report job has been created. You can use the Scheduled Jobs page to monitor the job status and to reschedule a job if necessary. You can also clone a scheduled job and edit the report criteria, if required.

Managing Reports

Prime Network provides the following options for working with reports:

- Managing the Maximum Number of Concurrent Reports, page 11-40
- Viewing and Saving Reports, page 11-41
- Renaming Reports, page 11-42
- Sharing Reports, page 11-43
- Moving Reports Between Folders, page 11-44
- Deleting Reports, page 11-44
- Viewing Report Properties, page 11-45

Managing the Maximum Number of Concurrent Reports

Prime Network enables you to run multiple reports at the same time. When the maximum number of concurrent reports is running, new report requests are queued for generation and have the status Queued (*n*) where *n* is the number in the report queue. When a running report moves to a Completed, Failed, or Cancelled state, the first report in the queue starts running.

The maximum number of concurrent reports is set at 5 by default. As the event rate approaches the maximum committed event rate, we recommend that you decrease the maximum number of concurrent reports. The maximum number of concurrent reports is defined in the registry, in reports.xml, under site/reports/reports-setting/reports-running-settings/maxRunningReports.

Note Changes to the registry should only be carried out with the support of Cisco. For details, contact your Cisco account representative.

To change the maximum number of concurrent reports, use the **runRegTool** command (located in *ANAHOME*/Main) as follows:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
site/reports/reports-setting/reports-running-settings/maxRunningReports value
```

where `value` is the new maximum number of concurrent reports.

You do not need to restart any AVMs after entering this command.

For more information on the **runRegTool** command, see the *Cisco Prime Network 3.10 Administrator Guide*.

Viewing and Saving Reports

You can view any reports that appear in the Report Manager content pane with the state Done. After viewing a report, you can save it in any of the available formats.

Note Reports are purged from Prime Network after 90 days by default. This setting can be modified by changing the setting in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.

To view and save a report:

Step 1 Choose **Reports > Report Manager**.

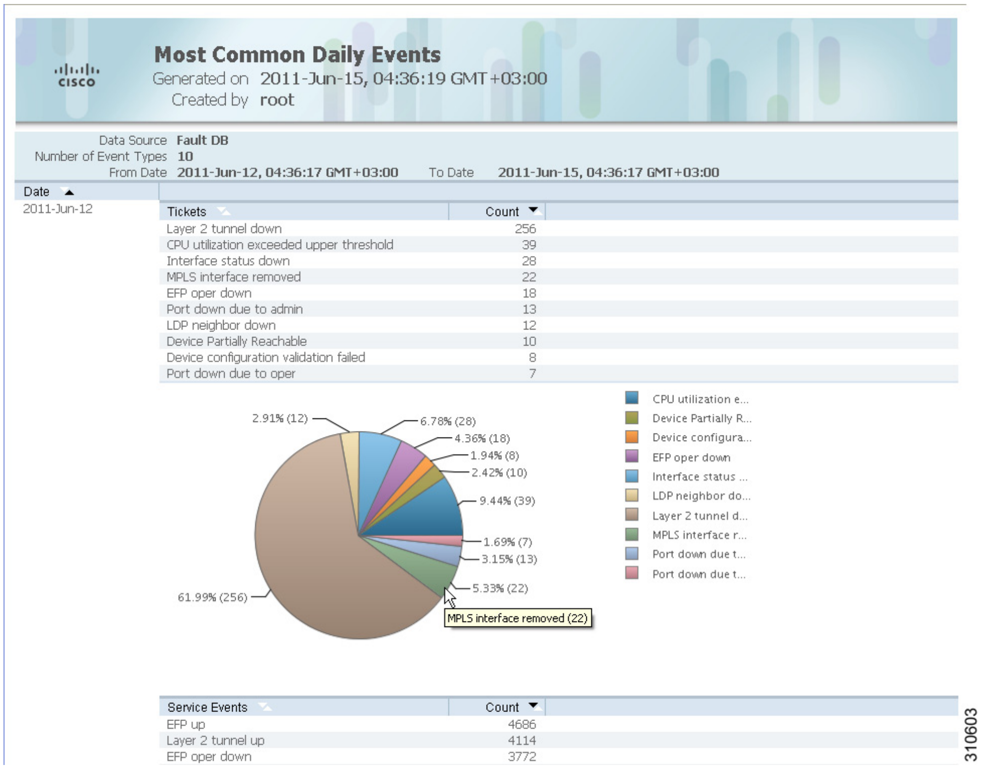
Step 2 In the navigation pane, locate the required report.

Step 3 In the content pane, right-click the report, then choose **View As >** *format* where *format* is one of the following:

- HTML—Displays the report in a browser window. Clicking a column heading in the report sorts the report by that value; clicking the column heading again sorts the data in the reverse order. HTML is the default format.
- PDF—Displays a PDF version of the report.
- CSV—Creates a CSV version of the report that you can either save to a specific location or view using another application. The CSV version contains only the report data; it does not contain the header information, layout, or formatting information that is available in other formats.
- XLS—Creates an XLS version of the report that you can either save to a specific location or view using another application, such as Microsoft Excel.
- XML—Creates an XML version of the report that you can either save to a specific location or view using an XML editor or viewer.

Figure 11-7 is an example of the Most Common Daily Events report in HTML format. The data is sorted by the Count column, in descending order.

Figure 11-7 Most Common Daily Events Report Example



Most Common Daily Events
Generated on 2011-Jun-15, 04:36:19 GMT+03:00
Created by root

Data Source **Fault DB**
Number of Event Types **10**
From Date **2011-Jun-12, 04:36:17 GMT+03:00** To Date **2011-Jun-15, 04:36:17 GMT+03:00**

Date ▲
2011-Jun-12

Tickets	Count ▼
Layer 2 tunnel down	256
CPU utilization exceeded upper threshold	39
Interface status down	28
MPLS interface removed	22
EFP oper down	18
Port down due to admin	13
LDP neighbor down	12
Device Partially Reachable	10
Device configuration validation failed	8
Port down due to oper	7

Service Events	Count ▼
EFP up	4686
Layer 2 tunnel up	4114
EFP oper down	3772

Step 4 Save the report as required.

Renaming Reports

You can rename:

- Any report type that you defined.
- Any generated report that you have access to.

You cannot rename any of the Prime Network standard report types.

Renaming a User-Defined Report Type

Note When you rename a report type, the new name applies to only those reports that you run after changing the name; it does not change the names of reports that were run prior to changing the name.

To rename a user-defined report type:

Step 1 In the navigation tree, select the user-defined report type.

Step 2 Right-click the report type, then choose **Properties**.

Step 3 In the Edit dialog box, enter a new name for the report type in the Report Name field, using the following conventions:

- The name can contain 1 to 150 characters.
- The name cannot include the following characters: ;?<>/:\"#*|.

Step 4 Click **OK**.

The navigation pane is refreshed and the report type is displayed with the new name.

Renaming a Generated Report

To rename a report:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the content pane, right-click the report that you want to rename, then choose **Rename** or **Properties**.

Step 3 In the Name field, enter the new name for the report, using the following conventions:

- The name can contain 1 to 150 characters.
- The name cannot include the following characters: ;?<>/:\"#*|.

Step 4 Click **OK**.

The content pane is refreshed and the report is displayed with the new name.

Sharing Reports

Prime Network enables you to share reports that you generate with other users, or limit access to a report to only you and the administrator.

Note You can share reports with others only if sharing is enabled in Prime Network Administration. For more information, see the *Cisco Prime Network 3.10 Administrator Guide*.

Sharing a Report

To share access to a report that you generated:

Step 1 Choose **Reports > Report Manager**.

Step 2 Locate the required report.

Step 3 In the content pane, right-click the report that you want to share, then choose **Share**.

The report is available to all system users for viewing and using.

Limiting Access to a Report

To limit access to a report that you generated and subsequently shared:

Step 1 Choose **Reports > Report Manager**.

Step 2 Locate the required report.

Step 3 In the content pane, right-click the report that you want to limit access to, then choose **Unshare**.

The report can be viewed and used by only you and the administrator.

Moving Reports Between Folders

You can move a report type that you have defined from the current folder to another folder in the navigation tree.

Note You cannot move a standard report type from one folder to another.

To move a report type to a new folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation tree, select the required report that you have defined.

Step 3 Right-click the report, then choose **Move**.

Step 4 In the Move To dialog box, select the folder to which you want to move the report.

Step 5 Click **OK**.

The Report Manager window is refreshed and the report appears in the specified folder.

Deleting Reports

You can delete reports to which you have access.

To delete a report:

Step 1 Choose **Reports > Report Manager**.

Step 2 Locate the required report.

Step 3 In the content pane, select the required report.

Step 4 Right-click the report, then choose **Delete Report**.

Step 5 In the Delete Report confirmation window, click **Yes** to confirm deletion.

The Report Manager window is refreshed and the deleted report no longer appears.

Viewing Report Properties

The Report Properties dialog box enables you to view the report settings and to modify some of them.

To view report properties, and optionally change the name, description, or access:

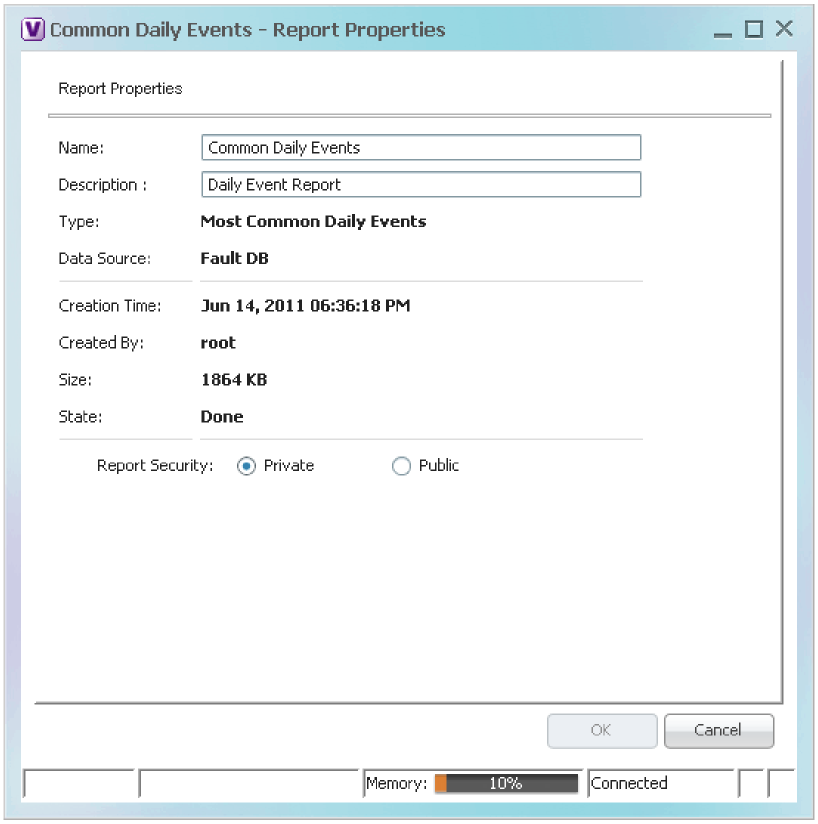
Step 1 Choose **Reports > Report Manager**.

Step 2 Locate the required report.

Step 3 In the content pane, right-click the selected report, then choose **Properties**.

The Report Properties dialog box is displayed, as shown in Figure 11-8.

Figure 11-8 Report Properties Dialog Box



Common Daily Events - Report Properties

Report Properties

Name: Common Daily Events

Description : Daily Event Report

Type: **Most Common Daily Events**

Data Source: **Fault DB**

Creation Time: **Jun 14, 2011 06:36:18 PM**

Created By: **root**

Size: **1864 KB**

State: **Done**

Report Security: ● Private ○ Public

Step 4 Change the information in the following fields as required:

- Name
- Description
- Report Security

Step 5 Click **OK**.

Defining Report Types

You can modify any of the report types provided by Prime Network so that it better suits your needs and environment. This is extremely beneficial if you generate a particular type of report for specific devices or events on a regular basis.

To define a report type:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, right-click the existing report type, then choose **Define Report of This Type**.

Step 3 In the Define report of type dialog box, specify the options using the information in Generating Reports, page 11-23.

Step 4 In the Location field, use the specified reports folder or click **Browse** to select a different folder.

Step 5 Click **OK**.

The newly defined report type appears in the navigation tree in the specified folder.

Managing Report Folders

Prime Network provides the following options for working with report folders:

- Creating Folders, page 11-46
- Moving Folders, page 11-47
- Renaming Folders, page 11-47
- Deleting Folders, page 11-48
- Viewing Folder and Report Type Properties, page 11-48

Creating Folders

Prime Network enables you to create additional report folders in Report Manager.

To create a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 Select a folder in which to place the new folder.

Step 3 Right-click the folder, then choose **New Folder**.

Step 4 In the New Folder dialog box, enter a name for the folder.

Step 5 Click **OK**.

The navigation pane is refreshed and the new folder is displayed.

Step 6 To move the new folder to another folder, or to the top level in the folder hierarchy:

a. Right-click the folder, then choose **Move**.

b. In the Move To dialog box, select the location where you want the folder to reside.

c. Click **OK**.

The folder is displayed in the new location.

Moving Folders

Prime Network enables you to move folders that you have created in Report Manager. You cannot move the Events Reports, Inventory Reports, or Network Service Reports folder.

To move a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 Right-click the folder, then choose **Move**.

Step 3 In the Move To dialog box, select the location where you want the folder to reside.

Step 4 Click **OK**.

The navigation pane is refreshed and the folder is displayed in the new location.

Renaming Folders

Prime Network enables you to rename folders that you have created in Report Manager. You cannot:

- Rename a folder that resides at the highest level in the hierarchy, such as the Events Reports, Inventory Reports, or Network Service Reports folder.
- Use the same name for different folders that reside at the same level in the hierarchy.

To rename a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 Right-click the folder, then choose **Rename**.

Step 3 In the Rename Folder dialog box, enter the new name for the folder.

Step 4 Click **OK**.

The navigation pane is refreshed and the folder is displayed with the new name.

Deleting Folders

You can delete folders that you have created in Report Manager if they are empty. You cannot delete the following folders:

- Events Reports
- Detailed Network Events
- Detailed Non-Network Events
- Inventory Reports
- Network Service Reports
- User-created folders that contain other folders or report types

To delete a report folder:

Step 1 Choose **Reports > Report Manager**.

Step 2 Right-click the folder, then choose **Delete**.

Step 3 In the Confirm Folder Delete dialog box, click **Yes** to confirm the deletion.

The navigation pane is refreshed and the folder no longer appears.

Viewing Folder and Report Type Properties

Viewing Report Folder Properties

The Report Properties window enables you to view report properties and to add folders.

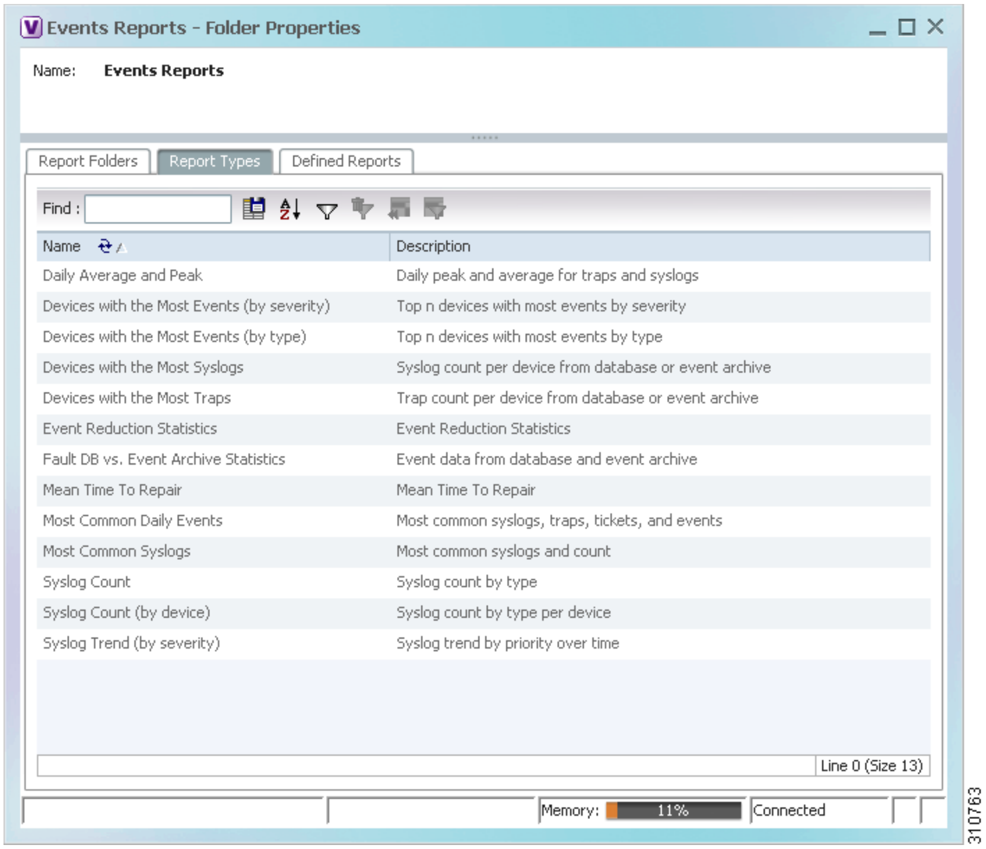
To view report properties:

Step 1 Choose **Reports > Report Manager**.

Step 2 In the navigation pane, right-click the required folder, then choose **Properties**.

The Folder Properties window is displayed, as shown in Figure 11-9.

Figure 11-9 Folder Properties



Events Reports - Folder Properties

Name: **Events Reports**

Name	Description
Daily Average and Peak	Daily peak and average for traps and syslogs
Devices with the Most Events (by severity)	Top n devices with most events by severity
Devices with the Most Events (by type)	Top n devices with most events by type
Devices with the Most Syslogs	Syslog count per device from database or event archive
Devices with the Most Traps	Trap count per device from database or event archive
Event Reduction Statistics	Event Reduction Statistics
Fault DB vs. Event Archive Statistics	Event data from database and event archive
Mean Time To Repair	Mean Time To Repair
Most Common Daily Events	Most common syslogs, traps, tickets, and events
Most Common Syslogs	Most common syslogs and count
Syslog Count	Syslog count by type
Syslog Count (by device)	Syslog count by type per device
Syslog Trend (by severity)	Syslog trend by priority over time

Line 0 (Size 13)

Memory: 11% Connected

Table 11-22 describes the information that is displayed in each tab, depending on the folder's contents.

Table 11-22 Folder Properties Window

Field	Description
Report Folders Tab	
Name	Name of the folder included in the selected folder.
Report Types Tab	
Name	Name of the report type included in the selected folder.
Description	Description of the report type included in the selected folder.
Defined Reports Tab	
Name	Name of the user-defined report in the selected folder.
Description	Description of the user-defined report in the selected folder.
Type	Report type on which the user-defined report is based.
Public	Status of public access to the report: True or False.

Viewing Report Type Properties

To view report type properties:

Step 1 In the navigation pane, right-click the required report type, then choose **Properties**.

The information that is displayed depends on whether the report type is one that you defined or one provided by Prime Network:

- Prime Network-provided report type—The Report Type Properties window is displayed with the report name and description. Click **Run** to generate the report.
- User-defined report type—The Edit dialog box is displayed with all settings specified for the report type. You can modify the settings or leave them as they are.

Step 2 Click **Close** or the upper right corner to close the window.