JUNIPER NETWORKS

# Junos® Space

## Network Director Report Mode User Guide

Release
1.5

Published: 2013-10-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net



*Junos® Space Network Director Report Mode User Guide*
1.5


The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

# List of Figures

# List of Tables

# About the Documentation



## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

## Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

## Table 1: Notice Icons

| Icon | Meaning | Description |
|---|---|---|
|  | Informational note | Indicates important features or instructions. |
|  | Caution | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning | Alerts you to the risk of personal injury or death. |
|  | Laser warning | Alerts you to the risk of personal injury from a laser. |

Table 2 on page x defines the text and syntax conventions used in this guide.

## Table 2: Text and Syntax Conventions

| Convention | Description | Examples |
|---|---|---|
| **Bold text like this** | Represents text that you type. | To enter configuration mode, type the **configure** command:<br><br>user@host> **configure** |
| `Fixed-width text like this` | Represents output that appears on the terminal screen. | `user@host>` **show chassis alarms**<br><br>`No alarms currently active` |
| *Italic text like this* | • Introduces or emphasizes important new terms.<br>• Identifies guide names.<br>• Identifies RFC and Internet draft titles. | • A policy *term* is a named structure that defines match conditions and actions.<br>• *Junos OS CLI User Guide*<br>• RFC 1997, *BGP Communities Attribute* |
| *Italic text like this* | Represents variables (options for which you substitute a value) in commands or configuration statements. | Configure the machine's domain name:<br><br>[edit]<br>root@# **set system domain-name** *domain-name* |
| **Text like this** | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components. | • To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level.<br>• The console port is labeled **CONSOLE**. |
| < > (angle brackets) | Enclose optional keywords or variables. | **stub <default-metric** *metric***>;** |

Table 2: Text and Syntax Conventions *(continued)*

| Convention | Description | Examples |
|---|---|---|
| \| (pipe symbol) | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | **broadcast \| multicast**<br><br>**(*string1* \| *string2* \| *string3*)** |
| # (pound sign) | Indicates a comment specified on the same line as the configuration statement to which it applies. | **rsvp { # Required for dynamic MPLS only** |
| [ ] (square brackets) | Enclose a variable for which you can substitute one or more values. | **community name members [ *community-ids* ]** |
| Indention and braces ( { } ) | Identify a level in the configuration hierarchy. | [edit]<br>routing-options {<br>  static {<br>  route default {<br>  nexthop *address*;<br>  retain;<br>  }<br>  }<br>} |
| ; (semicolon) | Identifies a leaf statement at a configuration hierarchy level. | |
| GUI Conventions | | |
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select **All Interfaces**.<br>• To cancel the configuration, click **Cancel**. |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select **Protocols>Ospf**. |

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

# Overview

CHAPTER 1

# Report Mode Overview

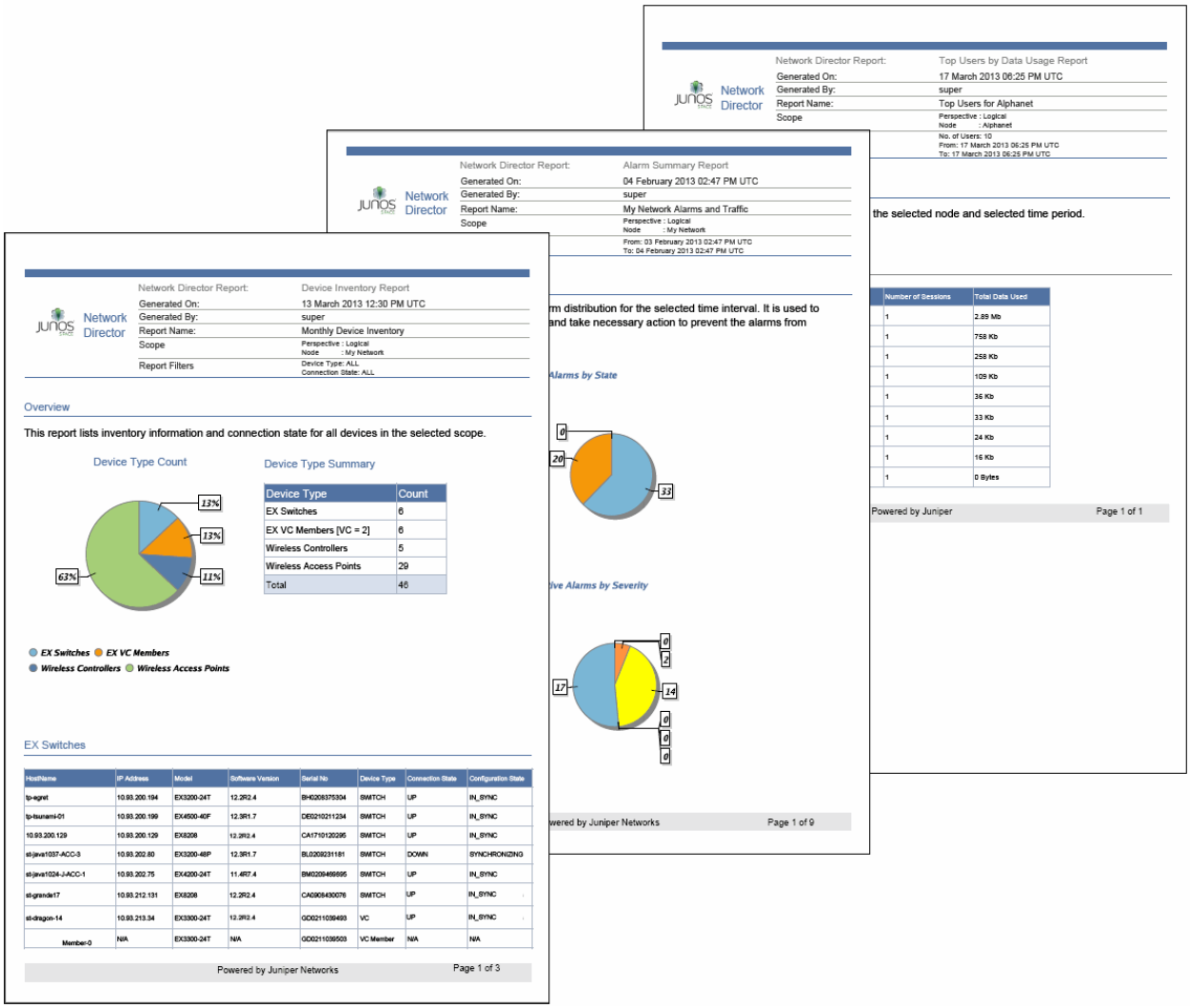


## Understanding Report Mode in Network Director

In Report mode in Junos Space Network Director, you can create standardized reports from the monitoring and fault data collected by Network Director. An essential part of the network management lifecycle, reporting provides administrators and management insight into the network for maintenance, troubleshooting, trend and capacity analysis, and provides records that can be archived for compliance requirements.

Network Director provides reports in PDF and HTML formats that use graphs and tables to clearly convey data. Reports are also available in CSV format for importation into spreadsheets. Figure 1 on page 4 shows some example PDF reports.

## Figure 1: Examples of Network Director Reports

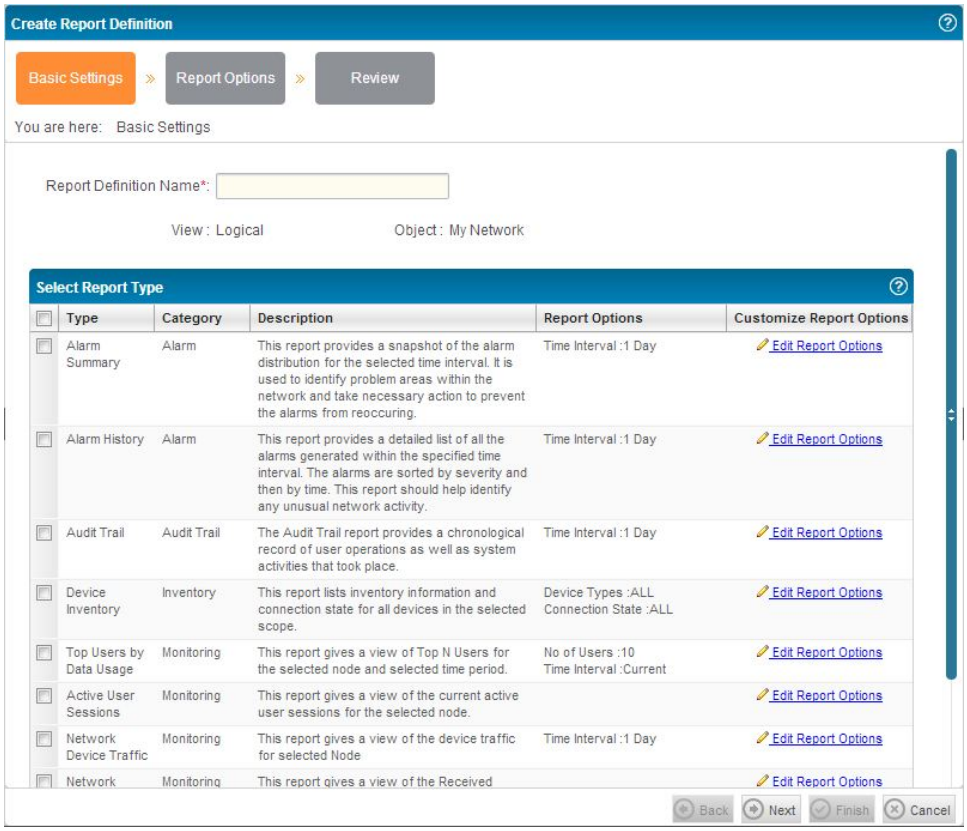



In addition to choosing the formats you want your reports to be in, you can:

- Run reports on-demand or schedule them to run at a specific time or on a recurring schedule.
- Select the portion of your network you want the report to cover by selecting a scope in the View pane when you create a report definition. For example, you can run a Device Inventory report on your entire network, on all devices in a wiring closet, or on all EX4200 switches.
- Select the report options—for example, the historical time frame you want an Audit Trail report to cover or the type of devices you want to be included in a Device Inventory report.
- Have reports sent to an e-mail address or automatically archived on a file server.

The process for generating reports is simple. Select a scope in the View pane and then create a report definition by using the Create Report Definition wizard shown in Figure 2 on page 5. When you complete the report definition, the reports are immediately scheduled to run according to the scheduling choices you have made.

## Figure 2: Creating a Report with the Create Report Definition Wizard




**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Understanding the Report Mode Tasks Pane on page 6

## Understanding the Report Mode Tasks Pane

Network Director has built-in reporting features to create standardized reports from your network data. You can schedule these reports to run either in real time or in batch to gain insight into the network for ensuring compliance, performing maintenance, or troubleshooting.

The Report mode analyzes data from different perspectives and filters the data based on the node selected in the network tree.

For example, if you want to view inventory reports on only your wireless controllers, you can select the Device view and the Wireless LAN Controllers node in the network tree to provide granular information on just those devices. After selecting the view and node in the network tree, create a report definition. In this definition file you select from a number of preconfigured reports and set the time frame, schedule, and output options.

From the Reports Tasks pane, you can:

- Set up a new report or change how an existing report is run by clicking Report Definition. From this page, you can launch a wizard that guide you through the process of defining a report or changing a report definition file. The report definition file is based on the report content on the view and the node you select in the network tree. The Filter option in the View pane does not affect the report content.
- View the summary details of the last run of a report, export a report, or to delete a report output by clicking Manage Generated Reports. This page is also the default Reports page. After a report definition is created and a report is generated from that definition, it is shown in the Generated Reports page.

  Reports are stored on the application server on which Network Director is running. However, because reports can be large, the report is delivered in a compressed or *zipped* format. and can be stored offline or on a Secure Copy Protocol (SCP) server.
- Set or change the path to an SCP server for report storage. You can also test the connectivity to the server by clicking Test Connection on the Manage SCP Servers page.
- Set or change the path to an SMTP server for e-mail notifications of alerts or for mailing reports to administrators. You can test the connectivity to the server by clicking Test Connection on the Manage SMTP Servers page.
- Create or change a schedule that is used by one or more reports by clicking Manage Schedules. Unless you want to run the report immediately, you need to create a schedule and associate it with the report definition file. Create the schedule before you create the report definition file.

  For example, you might want to run several reports that run on the weekend and are available first thing on Monday morning. You could create a single schedule that runs at midnight on Saturday and is delivered to you through e-mail.
- Add frequently performed tasks to Key tasks list. You can add any task from the Tasks pane to the Key Tasks list by selecting a task and clicking the plus (+) sign that appears adjacent to the task. For some modes, you can see that Network Director has predefined

some key tasks for you. You can modify this set of tasks to suit your requirements. This feature is available in Task pane irrespective of your current mode, scope, or view.

**Related Documentation**

- Managing Reports in Network Director on page 20
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22
- Mailing Reports on page 11
- Scheduling Reports on page 24
- Understanding the Types of Reports You Can Create on page 7

## Understanding the Types of Reports You Can Create

The Report mode enables you to create standard reports from your network information. Reports are based on a report definition that can either be global or granular. You control this global or granular scope of the report definition by your selections in the View pane (Logical, Location, or Device) and the network tree node.

For example, if you want to run your reports against all switches, you could select the Logical view and the Switching Network node in the network tree. Or if you wanted to run reports on all the devices on a floor of a building, you would select the Location view and navigate to the floor node of a building in the network tree. To pinpoint the performance on a particular switch, you would select the Device view and the individual switch node in the network tree.

TIP: **When naming your report definition, include the scope in the name. You cannot tell the scope from the report definition after you have created the definition; you can, however, determine the scope from the generated report.**

The reports generated from the report definition file are either formatted and sent to you through e-mail or sent using Secure Copy Protocol (SCP) to a designated repository.

You can create these reports in the Report mode:

- Alarm Summary
- Alarm History
- Audit Trail
- Device Inventory
- Top User by Data Usage
- Active User Sessions
- Network Device Traffic
- Network Neighborhood
- Port Bandwidth Utilization

- Virtual Machine vMotion History
- Virtual Machines Inventory

**Related Documentation**

- Creating Reports on page 13
- Alarm History Report on page 30
- Alarm Summary Report on page 33
- Audit Trail Report on page 34
- Device Inventory Report on page 36
- Active User Sessions Report on page 29
- Top Users by Data Usage Report on page 42
- Network Device Traffic Report on page 38

PART 2

# Administration

CHAPTER 2

# Report Creation and Management



## Mailing Reports

You can set up one or more electronic mail servers to send reports to e-mail addresses. These servers use the Simple Mail Transfer Protocol (SMTP) to forward the reports. While you can configure many servers as SMTP servers, you can only designate one as the primary mail server.

This topic describes:



### How to Configure SMTP Servers

An SMTP server is responsible for sending e-mails. Network Director uses the SMTP server to send reports to users. Under most circumstances, you need only one SMTP server. However, you might want to configure more than one SMTP server if you need a server with a distinct SMTP server configuration. In this case, you would configure multiple SMTP servers and mark the server you want to use as Active.

You can set up or manage SMTP servers from the Manage SMTP Servers page in the Report mode. To access this page:

1. Select **Report** in the Network Director banner. The Report Tasks pane opens, displaying the tasks available in the Report mode. The Generated Reports page loads in the main window.

2. Select **Manage SMTP Servers** in the Report Tasks pane. The Manage SMTP Servers page opens in the main window, displaying all existing SMTP servers configured for Network Director.

Use the Manage SMTP Servers page to:

- View existing SMTP server settings
- Set up new SMTP servers
- Edit existing SMTP server settings
- Test the connection to a SMTP server
- Set an SMTP server as the active server
- Delete an SMTP configuration
- See details of the SMTP configuration

## Managing SMTP Servers

Use the Manage SMTP Servers page to view and manage SMTP server settings. The Manage SMTP Servers page lists any existing SMTP server settings. The fields in the Manage SMTP Server page are described in Table 3 on page 12.

### Table 3: Managing SMTP Server Fields

| Field | Description | Hidden or Displayed by Default |
|---|---|---|
| Name | The name you are using to identify the SMTP server. | Displayed |
| Host Address | The IP address or hostname of the SMTP server. | Displayed |
| Port | The forwarding port number. Default port number for SMTP is 587. | Displayed |
| Active | Either yes or no to indicate whether it is the active server. Only one server can be active at a time. | Displayed |
| User Auth | Indicates whether SMTP authentication is required for the server. This field is either yes or no. | Displayed |
| Use TLS | Indicates whether Transport Layer Security (TLS) protocol is used to provide shared-secret encryption. | Displayed |
| User Name | Indicates the username when user credentials are required for SMTP authentication. | Hidden |
| From E-mail Address | The e-mail account that sends the report. | Hidden |

1. Establish a new server definition by clicking **Add** or edit an existing definition by selecting the server and clicking **Edit**. Either an Add SMTP Settings or Edit SMTP Settings page opens. See "Adding or Editing SMTP Server Settings" on page 13 for details on setting up or changing server settings.
2. Click **Done** to complete the process.
3. Click **Test Connection** to ensure your server is set up correctly. Network Director tells you whether the attempted connection to the SMTP server could be established.
4. Select a server and click **Set Active** to make that server responsible for sending e-mail.

   You can also delete any SMTP server definition from use by Network Director reports by clicking **Delete**.

### Adding or Editing SMTP Server Settings

The process of establishing a new SMTP server or to changing the values on an existing server is straightforward. Simply enter or change the values in the fields in the Add SMTP Server or Edit SMTP Server page. These fields are described in Table 4 on page 13.

**Table 4: Defining an SMTP Server**

| Field | Action |
|---|---|
| Server Name | Type a name for this SMTP server. |
| Host Address | Type the IP address of SMTP server. |
| Port Number | Type the forwarding port number. Default port number for SMTP is 587. |
| From Email Address | Type the e-mail address used to send the notification. |
| Set as Active Server | Checking this box sets the server as the Active server. If there is only one server, you cannot clear this box. |
| Use SMTP Authentication | Checking this box requires the server to use SMTP authentication. You must provide user credentials to use SMTP Authentication. |
| User Name | Type the account name accessing the server for SMTP authentication. |
| Password | Type the password twice that is used for authentication. |
| Use TLS | Select if you want this server to use TLS protocol on the SMTP server. |

**Related Documentation**

- Understanding the Report Mode Tasks Pane on page 6

## Creating Reports

Network Director has built-in reporting features to create standardized reports from your network data. You can schedule these reports either to run in real time or in batch to

provide insight into the network for compliance, maintenance, or troubleshooting. To define a new report, you select from a number of preconfigured report types and set the timing and output options.

This topic describes:



## How to Create a Report Definition

You create new reports from the Report Definition page while in the Report mode. To locate this page:

1. Select **Report** in the Network Director banner. The Report Tasks pane opens, displaying the tasks available in the Report mode.
2. Select your view of the network. You can generate reports from any view (Logical, Location, or Device).
3. Select the node. Some reports are designed to be run at the device level or for a specific type of device. For example, if you select an EX Series switch node and attempt to run Network Neighborhood report, which reports on RF strength, the report runs but is empty.
4. Select **Report Definition** in the Tasks pane. The Manage Report Definition page opens, displaying all existing report setup files.

## Creating a Report Definition

Your report is based on a report definition file that declares the:

- Name of the report definition
- Report type
- Reporting filters
- Scheduling options
- Output format

To create a report definition file:

1. Click **Add** on the Manage Report Definition main page to open the Create Report Definition wizard.
2. Type a name for the report in the Report Definition Name field. After the report runs, you can find a report by this name in the Generated Reports list. Names can contain letters, numbers, spaces, dashes (-), and underscores (_).

3. Select the type of report from the list. You can either select multiple report types or select the box next to the Report Type in the table heading to select all of the reports.

   When selecting multiple reports, be sure all of the reports you select are supported at this node in the view. Details for the report types are described in *Selecting Report Types and Filter Options*

4. Click **Next** or **Report Options** to set up the report options. You can also click **Cancel** to exit the wizard. For details on report options, see "Setting Report Options" on page 16.

## Selecting Report Types and Report Options

You must select at least one Report Type from the list of reports to create a report definition.

1. Select the type of report from the Select Report Type table. You can either select individual reports or select the box next to the Report Type in the table heading to select all of the available reports. The columns of the table are defined in Table 5 on page 15.

### Table 5: Select Report Type Table Columns

| Column Heading | Description |
|---|---|
| Type | The Report name. |
| Category | The general classification of the report. |
| Description | A description of the use or purpose of the report. |
| Report Option | The type of filtering that can be performed on the report data. |
| Edit Report Options | Clicking the edit link enables you to change the filter options for the report. |

2. (Optional) Click the Edit link in the table row to change the report options for filtering data for the report. See Table 6 on page 15 for details on the different report filters.

### Table 6: Report Options for Data Filtration

| Filter Option | Values | Description | Reports That Use this Option |
|---|---|---|---|
| Time Interval | 1 Day (default)<br>1 Hour<br>7 Days<br>30 Days<br>Custom | Limits the report to the indicated time period.<br><br>When Custom is selected, an additional dialog opens, enabling you to set a specific reporting period. | Alarm Summary<br>Alarm History<br>Audit Trail<br>Network Device Traffic |

Table 6: Report Options for Data Filtration *(continued)*

| Filter Option | Values | Description | Reports That Use this Option |
|---|---|---|---|
| Time Interval | Current (default)<br>1 Hour<br>8 Hours<br>1 Day<br>7 Days<br>30 Days<br>3 Months<br>6 Months<br>1 Year<br>Custom | Limits the report to the indicated time period.<br><br>When Custom is selected, an additional dialog opens, enabling you to set a specific reporting period. | Top Data by Data Usage |
| Device Types | All (default)<br>EX Switches<br>Wireless Controllers<br>Wireless Access Points<br>QFX Devices<br>QFabric Devices | Limits the report to this type of device. | Device Inventory |
| Connection State | All (default<br>Up<br>Down<br>N/A | Limits the report to devices in this state. | Device Inventory |
| Number of Users | 10 (users default) | Customizes the report to the specified number of users. | Top Users by Data Usage |

3. Click **Next** or **Report Options** to continue with the report definition.

## Setting Report Options

This page establishes the report schedule and the output format of the report.

1. Choose from the following scheduling options:
   - Run the report now
   - Select or create a schedule for the report
   - Select to both run the report now and to run the report by a schedule

   Options for report scheduling are shown in Table 7 on page 16:

Table 7: Schedule Options for Reports

| Field | Action |
|---|---|
| Run Now | Select this option to immediately run the report one time. |

Table 7: Schedule Options for Reports *(continued)*

| Field | Action |
|---|---|
| Select Schedule | Select this option to either create a schedule so that it is run at regular intervals, or to select an already established schedule.<br>• The Add Schedule link enables you to create a new schedule.<br>• The Select button opens Choose Schedule window that displays the currently configured schedules. Select the check box to choose a schedule to use for the report. To associate the schedule to your report, click **OK**. |

2. Establish the report output format and destination.

| Field | Options |
|---|---|
| Select Format | A report is available in these formats:<br>• PDF—Choose this format If you want to print the report. Portable Definition Format (PDF) enables the report to be printed from any operating system with the same formatting results.<br>• CSV—Choose this format if you want to export the report data to a spreadsheet or other business application. The Comma-Separated Values (CSV) format takes the raw data from the report and delineates the fields with commas so that it imports into popular spreadsheet programs.<br>• HTML—Choose this format if you want to view the report in a browser.<br>NOTE: Because reports can be quite large, they are initially delivered as a zipped (compressed) file. |
| Mode | Reports can be sent to your e-mail address, to a secure server, or to both.<br>• Select **EMAIL** and type the e-mail address to have the report sent through e-mail. Network Director uses SMTP server settings for e-mail routing. You can configure an SMTP server from the Tasks pane.<br>• Select **SCP** to send the report to the secure server that is marked as active, using Secure Copy Protocol. The settings for secure servers are available in Tasks > Manage SCP Servers. |

3. Click **Next** or **Summary** to review the report definition.

## Reviewing Report Definition Files

The Report wizard guides you to the Summary Page where you can review your report configuration and make any changes before you run the report.

1. Review your Report Name and Report Type in basic settings. If you want to change either of these settings, click **Edit** to return to the Basic Settings page.
2. Review your Report Options. If you want to change these settings, click **Edit** to return to the Report Options page.
3. Click **Finish** when you are done with the report configuration and to exit the wizard.

## Changing Report Definition Files

You can change an existing report definition file from the Manage Report Definition page.

To change a report definition:

1. Select the check box for the report definition.
2. Click **Edit** to reopen the report definition in the Report wizard. The system returns you to the Summary page, where you can make changes to the report definition.
3. Click **Details** to review the details of the report definition or click **Delete** to remove the report definition. To remove all of the report definitions, select the check box in the header next to Report Definition to select all of the report definitions and click **Delete**.

**Related Documentation**

- Managing Generated Reports on page 18
- Understanding the Types of Reports You Can Create on page 7
- Managing Reports on SCP Servers on page 22
- Mailing Reports on page 11
- Scheduling Reports on page 24
- Understanding Report Mode in Network Director on page 3

## Managing Generated Reports

After a report definition is created and the initial report is run, Network Director populates the Generated Reports page with summary information about the run of the report.

From the Generated Reports page you can view the report details, export the report to view or store in a new location, or delete the report.

This topic describes:

- Reviewing Generated Reports on page 18
- Viewing Report Details on page 19
- Exporting Reports on page 19
- Deleting Generated Reports on page 20

### Reviewing Generated Reports

After a reports runs, information about the report is recorded on the Generated Reports page, as shown in Table 8 on page 18.

#### Table 8: Fields in the Generated Reports Page

| Field | Description |
|---|---|
| Report Definition | The name assigned at report creation time. |
| Executed By | The userid of the report owner who ran the report. |
| Start Time | When the report began to run. |

Table 8: Fields in the Generated Reports Page *(continued)*

| Field | Description |
|---|---|
| End Time | When the report ended. |
| Format | The chosen report format, possible values are PDF, CSV, or HTML. |
| Generated Report | Links to view or download the report. |

From the Generated Reports page, you can either select the check box in the heading to select all of the reports or select the check box for the individual reports and:

- View details about the running of the report by clicking Report Details.
- Export the report by clicking Export.
- Delete the report by clicking Delete.

## Viewing Report Details

Use the Generated Report Details window to see information about the report composition. Viewing the Report Details is helpful when a report comprises many smaller reports. See Table 9 on page 19 for these field descriptions.

Table 9: Generated Report Details

| Field | Description |
|---|---|
| Report Definition Name | The name assigned at report creation time. |
| Executed By | The userid of the report owner who ran the report. |
| Start Time | When the report began to run. |
| End Time | When the report ended. |
| Format | The chosen report format, possible values are PDF, CSV, or HTML. |
| Generated Report | This link opens the Report Details window where you can view or download the report. |

Reports are kept on the application server until either you delete them or they are deleted by the system. The amount of time a report is saved on the system depends on the report retention settings for Network Director. Network Administrators can globally set the report retention period for reports in the system Preferences, located in the Network Director banner.

## Exporting Reports

Use the Export Report window to store multiple reports to a file location. Because reports can be large, they are delivered as compressed *zipped* files for both viewing or storing.

After you choose a report to export, you are prompted to select a program to view the report or to download the file.

You can either unzip the report for viewing or save the report to a file location.

TIP: If you choose to save the file, you might want to give a unique name to the unzipped file. After unzipping the report, the name of the report reverts to the type of report you selected. It does not retain the name of the report.

### Deleting Generated Reports

Use Delete to discard unneeded or outdated reports. When you click **Delete**, you are prompted to confirm the file deletion. Because deleted reports cannot be recovered, save the report offline before deleting them from the system.

**Related Documentation**

- Creating Reports on page 13
- Managing Reports in Network Director on page 20
- *Retaining Reports*

## Managing Reports in Network Director

Reports are generated from a report definition file. These files establish the type of report, when it is run, and how the report output is presented and preserved. You create, modify, or delete these definition files from the Manage Report Definition page.

This topic describes:

- How to Locate and Manage Reports on page 20
- Managing Report Definitions on page 21

### How to Locate and Manage Reports

The Manage Report Definition page is available from the Report Tasks pane while the Report mode is selected. To locate this page:

1. Select **Report** in the Network Director banner. The Report Tasks pane opens displaying the tasks available in the Report mode.
2. Select **Report Definition** in the Tasks pane. The Manage Report Definition page opens displaying all existing report definition files.

3. Use the Manage Report Definition page to review existing report definitions, create new definitions, or change a definition.
   - Create a new report definition by clicking Add. See "Creating Reports" on page 13 for help using the Report wizard.
   - Modify an existing report definition by selecting a report definition in the table and clicking Edit.
   - Delete an existing report definition by selecting a report type in the table and clicking Delete
   - View details of the report composition, the scope, and perspective of the report definition by clicking Details.

## Managing Report Definitions

Use the Manage Report Definition page to review existing report definitions, or follow the Report wizard to create new report definitions, delete definitions, or see report details.

Existing report definitions are listed on the page in the format discussed in Table 10 on page 21; the reports created from these definitions are found under the Manage Generated Reports task.

### Table 10: Manage Report Definition Fields

| Field | Description |
|---|---|
| Report Definition Name | The name of the report definition. Specify a name that indicates the purpose of the report. |
| Updated By | The userid of the last person to modify the report definition. |
| Schedule Name | (Optional) When the report is scheduled to run. |
| Report Format | The format or file extension of the report output; the final rendering of the output. Valid values are:<br>• PDF—(Portable Definition Format) is used for output that is either viewed in a reader or printed.<br>• CSV—(Comma Separated Format) is used for output that is exported into a spreadsheet.<br>• HTML—(Hypertext Markup Language) is used for output that is viewed in a web browser. |
| Reporting Mode | (Optional) Where the generated report is sent. Valid values are:<br>• Email—Sends a zipped file of the report to an e-mail address.<br>• SCP–Sends a zipped file to a secure server. |

**Related Documentation**

- Creating Reports on page 13
- Managing Generated Reports on page 18
- Understanding the Types of Reports You Can Create on page 7

- Understanding the Report Mode Tasks Pane on page 6
- *Retaining Reports*

## Managing Reports on SCP Servers

If your organization requires reports be stored on a secure server using Secure Copy Protocol (SCP), you can set one or more servers as a reports repository. A reports repository enables you to keep reports long-term for compliance requirements or for your organizational needs.

This topic describes:

- How to Configure SCP Servers on page 22
- Managing SCP Servers on page 22

### How to Configure SCP Servers

SCP servers are used as report repositories for Network Director reports. You can set up or manage a secure server for Network Director reports from the Manage SCP Servers page in the Report mode. To access this page:

1. Select **Report** in the Network Director banner. The Report Tasks pane opens, displaying the tasks available in the Report mode.
2. Select **Manage SCP Servers** in the Report Tasks pane. The Manage SCP Servers page opens, displaying all existing report schedules.

   Use the Manage SCP Servers page to:

   - View existing SCP server settings
   - Set up new SCP servers for reports
   - Edit SCP server settings
   - Test the connection to an SCP server
   - Make an SCP server active
   - Delete an SCP server setting

### Managing SCP Servers

Use the Manage SCP Servers page to view and manage SCP server settings.

- The Manage SCP Servers page lists any existing server settings. The fields in the Manage SCP Server page are described in Table 11 on page 22.

#### Table 11: Managing SCP Server Fields

| Field | Description |
|---|---|
| Server Name | The name you are using to identify the SCP server. |

Table 11: Managing SCP Server Fields *(continued)*

| Field | Description |
|---|---|
| IP Address | The IP address or hostname of the SCP server. |
| Port Number | The forwarding port number. Default port number for SCP is 22. |
| Active | Either yes or no to indicate whether it is the active server. Only one server can be active at a time. |
| Base Path | The path on the server where the reports are to be stored. |

- Create new or edit existing server settings:

  1. Establish a new server definition by clicking **Add** or edit an existing definition by clicking **Edit**. Either an Add SCP Settings or Edit SCP Settings page opens.
  2. Fill in the settings described in Table 12 on page 23.

Table 12: Defining an SCP Server

| Field | Action |
|---|---|
| Server Name | Type a name for this SCP server. |
| IP Address/Host Name | Type the IP address of SCP server. |
| Port Number | Type the forwarding port number. Default port number for SCP is 22. |
| User Name | Type the account name accessing the server. |
| Password | Type the password twice for the account on the secure server. |
| Default Path | Type the file path to the server where the reports are to be stored. |
| Set Active | Select if you want this server to the active server. While many servers can be set up as SCP servers for reports, only one server is marked as active. |

  3. Click **Done** to complete the process.
  4. Click **Test Connection** to ensure your server is set up correctly. Network Director attempts to connect to the SCP server and tells you whether the connection could be established.
  5. Select a server and click **Set Active** to make that server available for secure services.

     You can also delete any SCP server definition from use by Network Director reports by clicking Delete.

**Related Documentation**

- Understanding the Report Mode Tasks Pane on page 6

- Managing Generated Reports on page 18


## Scheduling Reports

You can run Network Director reports as needed or you can automate reports to run in batch by creating a schedule. You can associate a single schedule with one or more reports when you create the report definition. Although you can create a schedule during the report definition process, it is helpful to have the schedules configured before defining the report. To create a new schedule you name the schedule and set the time and frequency of the run.

This topic describes:


- How to Create or Manage Schedules on page 24
- Managing Schedules on page 24
- Creating New Schedules on page 25
- Editing Schedules on page 27
- Deleting Schedules on page 27


### How to Create or Manage Schedules

You create a schedule from the Manage Schedules page. You can display this page from the Report mode Tasks pane.

- Select **Report** in the Network Director banner. The Report mode Tasks pane displays the tasks available in the Report mode. Reports run in any network view (Logical, Location, or Device).
- Select **Manage Schedules** in the Tasks pane. The Manage Schedules page opens, displaying all existing report schedules.

From the Manage Schedules page, you can:

- Create a new schedule
- Edit an existing schedule
- See the details of a schedule
- Delete a schedule

### Managing Schedules

Use the Manage Schedules page to administer report schedules. From this page, you can create new schedules and view, modify, and delete existing schedules. On the Manage Schedules page, a table of existing report schedules appears. You can sort and customize this table to exclude fields that might not be relevant to your needs. The fields in the table are defined in Table 13 on page 25.

### Table 13: Manage Report Schedules

| Field | Description |
|---|---|
| Schedule Name | The name of the schedule. Indicate the purpose of the schedule in the name. |
| Schedule Type | Schedules are either One-Time or Recurring.<br>• One-Time—These schedules are helpful for running a non-repeating report in batch-mode, such as running it at 3:30 a.m.<br>• Recurring—These schedules are helpful for routine reports and trend analysis. |
| Recurrence Pattern | How often the pattern repeats. The pattern applies only to recurring schedules. Valid values are:<br>• Hourly<br>• Daily<br>• Weekly<br>• Monthly |
| Description | Details of the reoccurrence pattern. |
| Status | Either Active or blank. Active indicates the schedule is running. |

From this page you can:

- Display a summary of all the parameter settings of a schedule by selecting the schedule and clicking Details. The Report Schedule Summary opens.
- Create a new schedule by clicking Add. The Create Schedule window opens.
- Select a schedule and change the settings by clicking Edit. The Edit Schedule window opens.
- Select a schedule and click **Delete** to remove a schedule.

CAUTION: **Take care when deleting a schedule. Network Director enables you to delete a schedule even if it is active.**

## Creating New Schedules

Use the Create Schedule window to create a one-time or a recurring schedule.

To create a new schedule:

1. Click **Add** on the Manage Schedules page. The Create Schedule window opens.
2. Enter the name for the schedule in **Schedule Name**. Indicate the purpose of the schedule in the name.
3. Choose a one-time run-option or a recurring schedule from the list.
   - One-time schedule options are described in Table 14 on page 26.

- Recurring schedule options are described in Table 15 on page 26.

  Depending on the schedule range selected, these settings change dynamically.

### Table 14: One-Time Schedule Options

| Field | Action |
|---|---|
| Execute Start Date | Select the date when the schedule is run. You can either fill in a date directly or click the calendar icon to pick a date from a traditional calendar. |
| Execute Start Time | Select the time the report is run. Time is shown in 24-hour clock format in increments of 15 minutes. |

### Table 15: Recurring Schedule Options

| Field | Action |
|---|---|
| Hourly | Run the report associated with the schedule, hourly between these hours at intervals of *x* minutes. Start and end times are shown are in 24-hour clock format, in increments of 15 minutes. For example, if you want to schedule a report to run from 1 am to 3 pm at 30 minute intervals, your settings would be:<br><br>between *13:00* and *15:00* at *30* min(s). |
| Daily | Run the report associated with the schedule either every weekday or on the specified number of sequential days. Use the up and down arrows to set the number of sequential days or click **Every weekday**. |
| Weekly | Run the report associated with the schedule on one or more days of the week. Set the schedule to repeat the run in the specified number of weeks. Use the up and down arrows to set the weekly frequency of how often the schedule is repeated. Click one or more of the days when the report is run. |
| Monthly | Run the report associated with the schedule either on a certain day of the month or on a specified day and week for the specified number of months.<br><br>For example, if your organization has a congestion spike at the end of the fiscal quarter, you might want to run reports on the last Friday every 4 months. |

4. Specify when to start and end implementation of this schedule as described in Table 16 on page 26.

### Table 16: Range of Recurrence Fields

| Field | Action |
|---|---|
| Start Time: | Select the time of day. The clock is in 24-hour format, in increments of 15 minutes, when the schedule begins to run. |
| Start Date: | Select the date when the schedule is first implemented. Format is *yyyy-mm-dd*. |
| No end date | Select to indicate to continue to use this schedule until it is modified or deleted. |

Table 16: Range of Recurrence Fields *(continued)*

| Field | Action |
|---|---|
| End After: *x* occurrence | Select to run the schedule for a specified number of times. Use the up and down arrow keys to specify the number of times to run the schedule. |
| End by: | Select a time and date to stop running the schedule. Date format is *yyyy-mm-dd*. Select the time from the list; clock times are in increments of 15 minutes. |

5. Click **Add** to finish and to validate the schedule.

## Editing Schedules

To change an existing schedule:

1. Select a schedule from the list in the Manage Schedules page.
2. Click **Edit** to reopen the schedule settings.
3. Change the settings based on the values described in Table 14 on page 26.
4. Click **Edit** to save the revised settings.

## Deleting Schedules

CAUTION: **Network Director enables you to delete an active schedule. Be aware that deleting a schedule that is active will cause reports not to run.**

You can also permanently remove a schedule by selecting the schedule in the Manage Schedule page and clicking Delete.

**Related Documentation**

- Creating Reports on page 13
- Understanding the Report Mode Tasks Pane on page 6

CHAPTER 3

# Report Reference



## Active User Sessions Report

The Active User Sessions report is a standardized report generated in Network Director to show the activity level of current users on a specified node. There are two portions of the report: a report header and the report body. The contents of the report header are found in Table 17 on page 29.

### Table 17: Active User Session Report Header

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Active User Sessions report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2013 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned when the report was created. |
| Scope | The report is generated from this view and node in the network.<br>• *Perspective*—Can be a Logical view, Location view, or a Device view of the network.<br>• *Node*—Represents the selected object on which the report is based. |

The base report is a table with the fields described in Table 18 on page 30.

### Table 18: Active User Session Report Fields

| Field | Description |
|---|---|
| User Name | The name that identifies the user to the network. |
| Client MAC Address | The MAC address of the user. |
| Controller IP | The IP address of the wireless controller. |
| Total Bytes | The total number of bytes for the session. Bytes are shown in system international (SI) notation. For example, terabytes (TB), gigabytes (GB), megabytes (MB), and Kilobytes (KB). |
| AP Name | The network name for the access point. |
| SSID | The network identifier for the access point that the client is using. |
| Client IP | The IP address of the client. |
| Auth Type | The authentication type. |
| Bandwidth (KBps) | The transfer speed in Kilobytes per second. |
| VLAN | The VLAN name. |
| Session Elapsed Time | The amount of time after the user started the session. |

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22

## Alarm History Report

The Alarm History report is a standardized report generated in Network Director. It shows all active, acknowledged, and cleared alarms that occurred within a specified period of time for the indicated node. The report has two portions: a report header and the report body.

This topic describes:

- Alarm History Header on page 31
- Alarm History Tables on page 31

## Alarm History Header

The Alarm History report header provides file creation information about the report. The contents of the report header are described in Table 19 on page 31.

### Table 19: Alarm History Report Header

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT | The type of report—in this case, the Alarm History report. |
| Generated On | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST. |
| Generated By | The username of the user that generated the report. |
| Report Name | The name of the report assigned when the report was created. |
| Scope | The report is generated from this view and node in the network. Perspective can be Logical view, Location view, or Device view of the network. Node represents the selected object upon which the report is based. |
| Report Filters | The period of time specified for data collection. |

## Alarm History Tables

The body of the Alarm History report is a set of tables: one table for each alarm state (active, acknowledged, and cleared). In each table the alarms are listed by severity level. The fields of the tables have a common format, which is described in Table 20 on page 31.

### Table 20: Active Alarm History Fields

| Field | Description |
|---|---|
| Alarm Name | The SNMP alarm name. |
| Severity | One of six levels that indicate the gravity of the alarm based on the impact on the system:<br>• Critical<br>• Major<br>• Minor<br>• Warning (customer defined)<br>• Alert (customer defined)<br>• Notice<br>• Info |

Table 20: Active Alarm History Fields *(continued)*

| Field | Description |
|---|---|
| Category | One of twenty-four functional areas:<br>• APAndRadio<br>• BFD<br>• BGP<br>• Chassis<br>• ClientAndUserSession<br>• Config<br>• CoreAndControllers<br>• CoS<br>• DHCP<br>• DOM<br>• FlowCollection<br>• General<br>• GenericEvent<br>• L2ALD<br>• L2CP<br>• MACFDB<br>• Misc.<br>• PassiveMonitoring<br>• Ping<br>• RFDetect<br>• RMON<br>• SONET<br>• SonetAPS<br>• VirtualChassis |
| Description | An indication of what caused the alarm. |
| Source | The Entity ID of the network device sending the trap. |
| Acknowledged | Whether or not the alarm has been acknowledged. |
| Updated On | The date when the alarm was last updated (assigned, annotated, or acknowledged) otherwise, the date the alarm was created. |

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22
- *Changing Alarm Settings*

# Alarm Summary Report

The Alarm Summary Report is a standardized report generated in Network Director. It shows a graphical summary of the alarms that occurred within a specified period of time, node, and network view. The report has two portions: a report header and a report body.

This topic describes:


- Alarm Summary Header on page 33
- Alarm Summary Charts on page 33


## Alarm Summary Header

The report header provides file creation information about the report. The contents of the report header are described in Table 21 on page 33.

### Table 21: Alarm Summary Report Header

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT | The type of report—in this case, the Alarm Summary report. |
| Generated On | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST. |
| Generated By | The username of the user that generated the report. |
| Report Name | The name of the report assigned when the report was created. |
| Scope | The report is generated from this view and node in the network. Perspective can be Logical view, Location view, or Device view of the network. Node represents the selected object upon which the report is based. |
| Report Filters | The period of time specified for data collection. |

## Alarm Summary Charts

The body of the Alarm Summary report contains a series of colored charts that provide insight into the trends or distribution of alarms in the network. The first chart summarizes the proportion of active and clear alarms. The rest of the charts are divided into two identical sets: one set for active alarms and one set for clear alarms. If there are no alarms in an active or in a clear state, the set of charts for that state are omitted.

The charts are:

- Alarms by State—Shows the proportion of alarms in active and clear states.
- Active Alarms by Severity (Clear Alarms by Severity)—Shows the proportion of alarms in each severity classification. The default severity levels are:

Critical (Red)— A critical condition exists; immediate action is necessary.

Major (Orange)— A major error has occurred; escalate or notify as necessary.

Minor (Yellow)— A minor error has occurred; notify or monitor the condition.

Info (Light Blue) —An informational message; no action is necessary.

In Preferences, administrators can override the default severity of an alarm and set the severity to match their inhouse guidelines.

- Active Alarm Summary Chart (Clear Alarm Summary Chart)—Shows alarms by category and severity.
- Active Alarms by Category (Clear Alarms by Category)—Shows the number of alarms in each alarm category and, within category, the number of alarms that are acknowledged or unacknowledged.
- Active Alarms by Type (Clear Alarms by Type)—Shows the number of alarms of each specific type. The types are color-coded by severity.
- Top 10 Sources of Active Alarms (Top 10 Sources of Clear Alarms)—Identifies the top 10 devices that are generating the most alarms. Shows the number of alarms each device is generating by severity.
- Active Alarms by Timestamp (Clear Alarms by Timestamp)—This section of the report contains two graphs that plot alarms by their created timestamp:
  - Alarms by timestamp per severity—Plots each alarm of given severity against the time the alarm was created. For example, if during the time period covered by the report there are 10 alarms of major severity, the graph shows 10 orange data points that are plotted against the time the alarms were created.
  - Active alarms by timestamp for top 10 sources (Clear alarms by timestamp for top 10 sources)—For each source, plots the alarms generated by the source against the time they were created.

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22

## Audit Trail Report

The Audit Trail report is a standardized report generated in Network Director. It shows a history of users accessing the system, modifications to applications, and network management activities for a specific period of time. The report is defined and generated from the Report mode in Network Director.

There are two portions of the report: a report header and the report body. The contents of the report header are shown in Table 22 on page 35.

### Table 22: Audit Trail Report Header Information

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Audit Trail report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned when the report was created. |
| Scope | The report is generated from this view and node in the network. Perspective can be Logical view, Location view, or Device view of the network. Node represents the selected object upon which the report is based. |
| Report Filters | The period of time specified for data collection. |

The body of the report comprises the Audit Logs by Task Type chart, the Audit Logs by User chart, and a Audit Detail table.

The Audit Logs by Task Type is a bar chart that lists all of the user and system activities over the specified time period for all users.

The Audit Logs by Users is a pie chart that graphically represents all the active users in a specified time period.

The fields in the report body table are shown in Table 23 on page 35.

### Table 23: Audit Trail Report Fields

| Field | Description |
|---|---|
| User Name | The userid of the individual associated with the activity. |
| User IP | The IP address of the client. |
| Task | A short summary of the activity, such as Backup or Login. |
| Description | The description of the system activity being logged. Examples of common logging activities include logging in and out of the system, modifying application settings, creating SMTP or SCP servers, or database backups. |
| Result | The result of the system activity: whether it is successful or not. Regularly scheduled events, such as backups, show as recurring. |
| Job ID | The system generated identification for applicable tasks. |
| Timestamp | The date and time of the activity. The date is shown in the format: [Day of the Month] [Month] [Year], while the time is shown in standard 12-hour clock format. |

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22
- *Viewing Audit Logs From Network Director*

## Device Inventory Report

The Device Inventory report is a standardized report generated in Network Director to show all devices that are visible to Network Director. There are two portions of the report: a report header and the report body. The contents of the report header are found in Table 24 on page 36.

### Table 24: Device Inventory Report Header

| | |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Device Inventory report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST |
| Generated By: | The username of the user that generated the report. |
| Report Name: | The name of the report assigned by the user when the report was created. |
| Scope | The report is generated from this view and node in the network.<br>• *Perspective*—Can be Logical view, Location view, or Device view of the network.<br>• *Node*—Represents the selected object that the report is based. |
| Report Filters | The report specified these device and connection state filters.<br>Device Type—Supported device types are:<br>• EX Series switches<br>• Wireless LAN controllers<br>• Wireless access points<br>• QFX<br>• QFabric<br>• All (supported device types)<br>Connection State—Device connection states for filtering are:<br>• Up<br>• Down<br>• N/A<br>• All (connection states) |

The body of the report comprises:

- Device Type Count, which is a pie chart that graphically represents the network composition. Each segment represents:
  - EX Series switches
  - Wireless LAN controllers
  - Wireless access points
- Device Type Summary, which gives the total count of each type of device covered in the node.
- Device details by logical groups.

Following the pie chart, details for each device segment are listed by device type. For descriptions of the device fields see Table 25 on page 37.

### Table 25: Inventory Report Fields

| Field | Description |
|---|---|
| HostName | The device label. |
| IP Address | Either the IPv4 or the IPv6 address.<br>NOTE: Not applicable for access points. |
| Model | The full model number of the EX Series switch. |
| Software Version | The Junos software version and release number. |
| Serial No | The hardware serial number of the device. |
| Device Type | The type of hardware, such as switches, controllers, or access points. Switches can also be designated as NORMAL for standalone or VC for Virtual Chassis. |
| Connection State | The connection state of the switch. |
| Configuration State | The administrative or operational state of the device. |

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22
- *Viewing the Device Inventory Page*

## Network Device Traffic Report

The Network Device Traffic report is a standardized report generated in Network Director to show the device traffic for a device. There are two portions of the report: a report header and the report body.

This topic describes:



### Network Device Traffic Report Header

The contents of the report header are found in Table 26 on page 38.

**Table 26: Network Device Traffic Report Header**

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Network Device Traffic report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned by the user when the report was created. |
| Scope | The report is generated from this view and node in the network.<br>• *Perspective*—Can be Logical view, Location view, or a device view of the network.<br>• *Node*—Represents the selected object upon which the report is based.<br>NOTE: If you select a device that is down, the report might not contain any data. |
| Report Filters | The period of time specified for data collection. |

### Network Device Traffic Charts

The body of the Network Device Traffic report is a series of four colored charts that show a comparison of data or trend information about the packets. The charts are:

- Unicast Vs Non-unicast

  This pie-chart shows the percentage totals for packets over the specified period of time at the node:

  - Inbound unicast packets
  - Inbound non-unicast (such as broadcast and multicast) packets

- Outbound unicast packets
- Outbound non-unicast packets

The percentage of non-unicast packets is normally less than that of unicast packets. If the percentage of non-unicast packets is as high or higher than that of the unicast percentage, it means that too many non-unicast packets are being sent in the network.

- Unicast Vs Non-Unicast Trend

  This line chart shows the trend in unicast and non-unicast packets over the specified period of the report. The x axis shows the polling period; the y axis shows the number of packets. Use this chart to see if the plots are symmetric or asymmetric. It can also be useful for identifying unusual patterns.

- Traffic Trend

  This line chart shows the overall trend of all packets over the specified period of time. The x axis shows the polling period; the y axis shows the number of packets. Use this chart to find abnormalities in the traffic trend.

- Error Trend

  This line chart shows the errors over the specified period of time. An error is caused by a missing packet. Missing packets can be a result of: packet loss in the network, uncorrectable packet out of sequence, packet length error, jitter buffer overflow, or jitter buffer underflow. Use this chart to see the overall trend in errors. The x axis shows the polling period; the y axis shows the number of errors.

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18
- Managing Reports on SCP Servers on page 22

## Network Neighborhood Report

The Network Neighborhood report is a standardized report generated in Network Director to show the Received Signal Strength Indication (RSSI) data for a location or for an access point cluster. The report is available in all views (Logical, Location, and Device), however it supports only selecting a Floor or Outdoor area in Location View, or a node that contains an access point or an access point cluster in Logical or Device view. There are two portions of the report: a report header and the report body.

This topic describes:

- Network Neighborhood Report Header on page 39
- Network Neighborhood Report Tables on page 40

### Network Neighborhood Report Header

The contents of the report header are described in Table 27 on page 40.

Table 27: Network Neighborhood Report Header

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Network Neighborhood report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2013 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned by the user when the report was created. |
| Scope | The report is generated from this view and node in the network.<br>• *Perspective*—Can be Logical view, Location view, or a device view of the network.<br>• *Node*—Represents the selected object upon which the report is based.<br>NOTE: Selecting a node that does not contain wireless equipment can cause this report to be blank. |

## Network Neighborhood Report Tables

The body of the Network Neighborhood report is a series of four tables that provide information on radios within a selected view. The first two tables provide the RSSI values of the listeners for the radios. RSSI is the power level being received by the antenna. The last two tables list the radios that are being heard by the selected radio, which are grouped by channels.

The Radio 2.4 GHz RSSI Mapping table shows the Radio1NG values of listeners for the radios in the selected scope. The column headings of the table show the radio identifier, which is the access point name, a colon, and the radio number. The table rows represent the lists the 2.4-GHz radios available in the scope. The signal strength is shown in decibels, with the stronger signals being less negative, or closer to zero.

The Radio 5 GHz RSSI Mapping table shows the Radio2NA values of listeners for the radios in the selected scope. The column headings of the table show the radio identifier, which is the access point name, a colon, and the radio number. The table rows represent the lists the 5-GHz radios available in the scope. The signal strength is shown in decibels, with the stronger signals being less negative, or closer to zero.

The Radio 2.4 GHz Channel Mapping and the Radio 5 GHz Channel Mapping tables shows which access points are being heard on a channel. The Channel column list the channels using the frequency; the APs Heard column list the radio identifiers being heard on the channel.

**Related Documentation**

- *Monitoring the RF Neighborhood*

## Port Bandwidth Utilization Report

The Port Bandwidth Utilization report is a standardized report generated in Network Director to show . There are two portions of the report: a report header and the report body. The contents of the report header are found in Table 28 on page 41.

### Table 28: Port Bandwidth Utilization Report Header

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Port Bandwidth Utilization report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2013 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned when the report was created. |
| Scope | The report is generated from this view and object in the network.<br>• *View*—Can be a Logical view, Location view, or a Device view of the network.<br>• *Object*—Represents the selected object on which the report is based. |
| Report Filters | Shows the Percentage Utilization Exceeding value specified for the report. Only ports that exceed this percentage of their allocated bandwidth appear in the report. |

The report contains a table for each device that contains ports that exceeded the specified percentage of their allocated bandwidth. The fields in these tables are described in Table 29 on page 41.

### Table 29: Port Bandwidth Utilization Report Fields

| Field | Description |
|---|---|
| Host Name | Host name of the device. |
| IP Address | IP address of the device. |
| Device Type | Device type. |
| Port Name | Port name. |
| Percentage Utilization | Percentage of allocated bandwidth the port used. |

**Related Documentation**

- Understanding the Types of Reports You Can Create on page 7
- Creating Reports on page 13
- Managing Generated Reports on page 18

- Managing Reports on SCP Servers on page 22

## Top Users by Data Usage Report

The Top Users by Data Usage report is a standardized report generated in Network Director. Use this report to identify the users with the highest data usage at the specified node during the specified time frame.

This topic describes:

- Top Users by Data Usage Header on page 42
- Top Users of Data Table on page 42

### Top Users by Data Usage Header

The contents of the report header are found in Table 30 on page 42.

**Table 30: Top 10 Users by Data Usage Report Header**

| Field | Description |
|---|---|
| NETWORK DIRECTOR REPORT: | The type of report; In this case, the Top Users by Data Usage report. |
| Generated On: | The date and time the report ran. The date format is: [Day of the Month] [Month] [Year]. The time format follows the Coordinated Universal Time (UTC). For example: 07 December 2012 11:35 PM PST. |
| Generated By: | The username of the user that generated the report. |
| Report Name | The name of the report assigned by the user when the report was created. |
| Scope | The report is generated from this view and node in the network. Perspective can be Logical view, Location view, or Device view of the network. Node represents the selected object that the report is based. |
| Report Filters | The count specified for the report generation. The default count is 10 users. |

### Top Users of Data Table

The body of the Top Users by Data Usage report is a snapshot of the users with the highest data usage. The number of users analyzed and the time interval is determined by the Reporting Options set during report definition. The report sorts users in the table from the user with the highest bandwidth usage to the least highest. The key fields of the table are described in Table 31 on page 42.

**Table 31: Top 10 Users by Bandwidth Report Fields**

| Field | Description |
|---|---|
| User Name | The User ID with the highest bandwidth usage during the specified period. |

Table 31: Top 10 Users by Bandwidth Report Fields *(continued)*

| Field | Description |
|---|---|
| Client MAC Address | The MAC address of the client. |
| Number of Sessions | The total sessions during this time period. |
| Total Data Used | The bandwidth used in megabytes. |

**Related Documentation**

- *Top Sessions by MAC Address Monitor*