Cisco Prime Network 5.0 Operations Report User Guide

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2018 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Overview of Prime Network Operations Reports** 1-1

Introducing Operations Reports 1-1

Primary Features 1-1

Report Types 1-2

Data Types on which Reports Can be Run 1-2

Logging Into Operations Reports 1-3

Overview of the Operations Reports Home Page 1-3

CHAPTER 2 **Operations Reports Administration and Setup** 2-1

Overview of Operations Reports Architecture 2-1

Setting Up Operations Reports 2-2

Managing User Access Rights for Operations Reports 2-3

Granting User Permissions for Reports 2-3

Enabling Reports to be Sent by E-mail 2-4

Troubleshooting Tasks 2-5

Checking the Status of AVM 44 2-5

Stopping/Starting Operations Reports Processes 2-5

Resolving POODLE Vulnerability in Prime Network 2-6

Monitoring Log Files 2-7

Manually Refreshing Operations Reports to Show VNE Changes 2-8

Manually Reloading Report Folders to Show New Reports 2-8

Managing Infobright Database Operations 2-8

Starting/Stopping the Infobright Database 2-9

Stopping the Writing of Information to the Database 2-9

Enabling/Disabling Infobright Backup Process 2-10

Controlling When Operations Reports Data is Purged 2-10

Monitoring Infobright Data Logs 2-10

Backing Up and Recovering the Infobright Database 2-11

How the Infobright Database Backup Works 2-11

Checking that Backups are Taking Place 2-12

Changing Settings for Purging Infobright Backups 2-12

Recovering the Infobright Database 2-13

CHAPTER 3 **Using Prepackaged Reports** 3-1

Generating Reports 3-1

Generating Customizable Prepackaged Reports 3-2

Generating Read-Only Prepackaged Reports 3-2

Refreshing Prepackaged Read-Only Reports 3-4

Prepackaged Data Center Reports 3-4

Prepackaged Fault Reports 3-6

Non-Network Reports 3-10

Prepackaged Mobility Reports 3-11

Prepackaged Network Service Reports 3-12

Prepackaged Physical Inventory Reports 3-15

CHAPTER 4 **Creating New Interactive Reports** 4-1

Creating a New Report 4-1

Refreshing Interactive Reports 4-3

Choosing a Data Source to Determine the Report Content Type 4-5

CHAPTER 5 **Customizing Reports** 5-1

Customizing Data in Reports 5-3

Grouping Data in Reports 5-3

Changing the Data Presentation in Reports 5-4

Reordering Columns 5-4

Sorting Data in Reports 5-4

Formatting Interactive Reports 5-4

Changing the Report Template 5-5

Changing the Size and the Orientation of a Reports 5-5

Changing the Font Style 5-5

Filtering Interactive Reports 5-6

Adding a Filter 5-6

Creating Advanced Filters 5-6

Applying Quick Filters 5-7

Editing Prompts 5-8

Applying a Summary Function 5-9

Additional Useful Customization Options 5-9

CHAPTER 6 **Scheduling Reports** 6-1

Scheduling a Report 6-1

Scheduling a Read-Only Prepackaged Report 6-1
Scheduling a Customizable Prepackaged Report 6-2
Creating a Custom Schedule Interval 6-3
Deleting Schedules 6-5
Viewing the Status of Generated and Scheduled Reports 6-6
Tasks that you can Perform from Workspace 6-7

APPENDIX A **Predefined Data in Data Sources** A-1
Data Center Reports A-2
Fault Reports A-4
Mobility Application Reports A-9
Network Service Report A-17
Physical Inventory Reports A-18

Overview of Prime Network Operations Reports

Note The distribution of Operations Reports is no longer available. Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

.Operations Reports is an optional add-on component to Cisco Prime Network that provides extended reporting functionality. It provides a wide range of prepackaged reports that you can run for your various operational needs. It also allows you to create your own reports or customize reports according to your own requirements.

This section contains the following topics:

- Introducing Operations Reports, page 1-1
- Logging Into Operations Reports, page 1-3
- Overview of the Operations Reports Home Page, page 1-3

Introducing Operations Reports

Cisco Prime Network Operations Reports processes and stores a large amount of data relating to faults, device inventory, technologies, and so on. It enables you to access this data and evaluate it by generating meaningful reports which can help you understand your deployments better and make better business-critical decisions. This section contains the following topics:

- Primary Features, page 1-1
- Report Types, page 1-2
- Data Types on which Reports Can be Run, page 1-2

Primary Features

The key features of Operations Reports are:

- Intuitive, interactive, drag-and-drop web GUI.
- Prepackaged reports for fault, physical inventory, data center and mobility, some of which can be customized.
- Ability to create new interactive reports.

- High performance report generation - minimum time to process large amounts of data and generate reports.
- Extensive report customization options. Data can be added, removed, filtered, grouped, sorted, and formatted.
- Range of report output formats - Microsoft Excel, HTML, PDF, RTF, and CSV.
- Report scheduling and e-mail notification.

Report Types

Operations Reports provides a set of prepackaged reports and also allows you to create new reports. Operations Reports introduces the concept of interactive reports; interactive reports are reports that can be customized for your own individual needs. All new reports and some of the prepackaged reports are customizable, therefore they are interactive reports.

- Prepackaged Reports - Operations Reports provides a set of predefined reports that are based on the most common needs of Prime Network users, in the areas of fault, physical inventory, mobility and data center. When you start working with Operations Reports, it is recommended that you browse through the available prepackaged reports to see which ones meet your needs.
  - Customizable prepackaged reports—Since many of the prepackaged reports are customizable, you could use a prepackaged report as a starting point and then customize it according to your own requirements by adding or removing data, grouping data, filtering data, and so on.
  - Read-only prepackaged reports—Some of the prepackaged reports cannot be customized. These read-only reports tend to contain a graphic display of data in the form of graphs and charts, in addition to tabular data, giving you a different perspective of the data.
- New Reports—You can create new reports from scratch if none of the prepackaged reports meet your needs. This involves selecting the type of data to be displayed in the report (fault, inventory, and so on) and then dragging and dropping data parameters into the report to create columns of data. Once you have added your data, you can organize it as required by grouping, filtering, formatting, and so on.

Data Types on which Reports Can be Run

Using Operations Reports, you can generate reports to view data on fault, physical inventory, data center, network service, and mobility features of your network. For example, you can generate a report to view the mean time taken to close tickets. The report presents data of the type of tickets that were generated, the clearance mode (cleared by user or by network), the number of tickets of each type, the minimum time, the maximum time and the mean time taken to close each type of ticket.

Logging Into Operations Reports

Before you Begin:

Ensure that you are using either one of the following web browser to launch the Operations reports:

- Apple Safari 5.x
- Google Chrome 19
- Microsoft Internet Explorer 8, 9 and later versions
- Mozilla Firefox 13 and 14

Operations Reports is launched from Prime Network web client. To log into the Operations Reports portal:

Step 1 Open an Prime Network-supported web browser and enter:
https://<*gateway-IP*>:<*port-number*>**/prime-network-reports**

Where,

- Gateway-IP—gateway IP of the Operations Reports portal
- Port-number—SSL port number that was configured during installation. The default SSL port is 8445.

Note Use an Operations Reports-supported browser as your default web browser with caching and cookies enabled.

Prime Network login window appears.

Step 2 Enter your username and password.

If you are an administrator logging in for the first time, enter the username and the password that you configured for Prime Network.

Step 3 Click **LogIn**.

Step 4 Accept the self-signed, untrusted security certificates.

In Firefox, if you accept the security certificates, they do not reappear upon subsequent logins.

In Internet Explorer, if you accept the security certificates without placing them in the trusted certificate store, they reappear upon subsequent logins. If you place the certificates in the trusted store, they do not reappear upon subsequent logins.

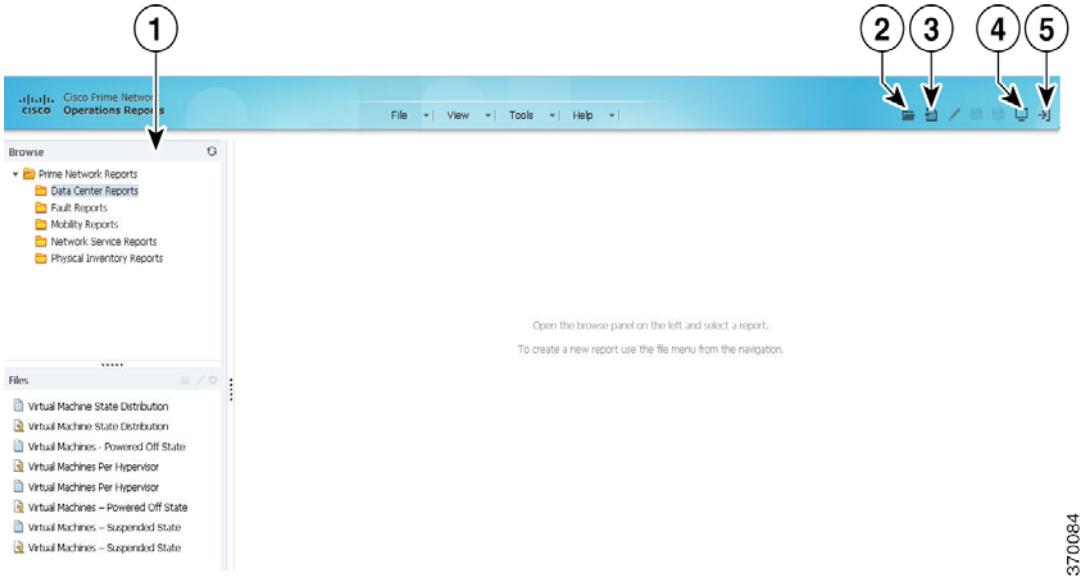
The username that you use for logging in, is displayed below the time stamp in each report that you open.

Step 5 Click on Operations Report to launch the reports console.

Overview of the Operations Reports Home Page

After logging into Operations Reports, the home page is blank. To see the available report folders and start working, open the left navigation pane by dragging its border.

Figure 1-1 Operations Reports—Home Page



The following table helps you understand the key elements in the home page:

Table 1-1 Home Page Icons—Description

	Item	Description
1	Left navigation pane	Contains the report folders and the report files.
2	Open Reports icon	Allows you to open reports.
3	New Interactive Report icon	Allows you to create new reports.
4	Workspace icon	Allows you to switch to Workspace, which provides a snapshot view of scheduled reports and their individual status.
5	Toggle icon	Allows you to expand and collapse the left navigation pane.

The left navigation pane lists the reports that are available in Operations Reports. The types of reports are available as folders in the Browse pane, and upon choosing a folder, the corresponding reports are displayed in the Files pane below. The left navigation pane displays the following:

Figure 1-2 Left Navigation Pane

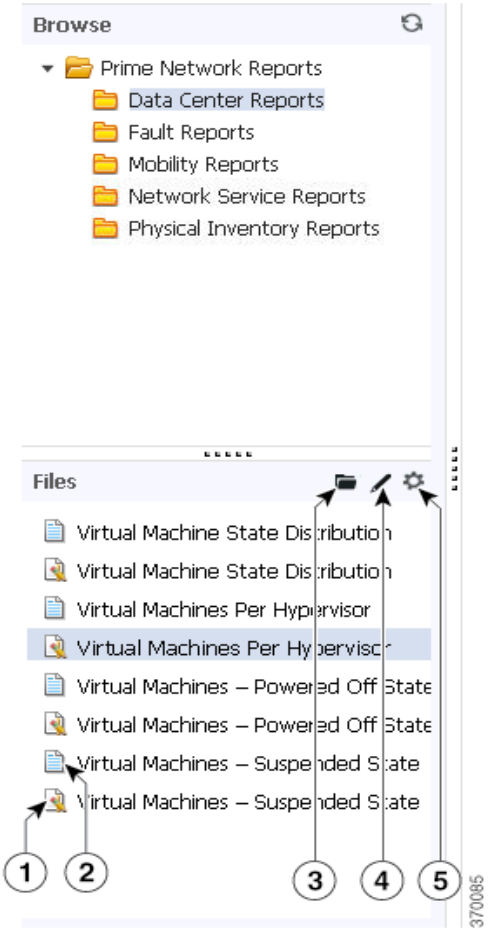


Table 1-2 Navigation Pane Items—Description

	Item	Description
1	Customizable (interactive) Report icon.	This icon indicates that the report is either a newly-created report or is a customizable prepackaged report
2	Read-only prepackaged report icon.	This icon indicates that the report is read-only.
3	Open Folder icon	Allows you to open the selected report.
4	Edit icon	Allows you to customize new reports and customizable prepackaged reports.
5	Options icon	Allows you to perform several operations on the selected report, including opening the report in a new window, running it in background, deleting it, sharing it with others, scheduling it, and viewing its properties. **Note** The Run In Background option is available only for customizable report. You can view the list of customizable reports that are chosen to run in background in the My Workspace page (View > Workspace).

Operations Reports Administration and Setup

This section is for administrators who are responsible for setup, maintenance, and troubleshooting of Prime Network Operations Reports. It contains the following topics:

- Overview of Operations Reports Architecture, page 2-1
- Setting Up Operations Reports, page 2-2
- Troubleshooting Tasks, page 2-5
- Managing Infobright Database Operations, page 2-8
- Backing Up and Recovering the Infobright Database, page 2-11

Overview of Operations Reports Architecture

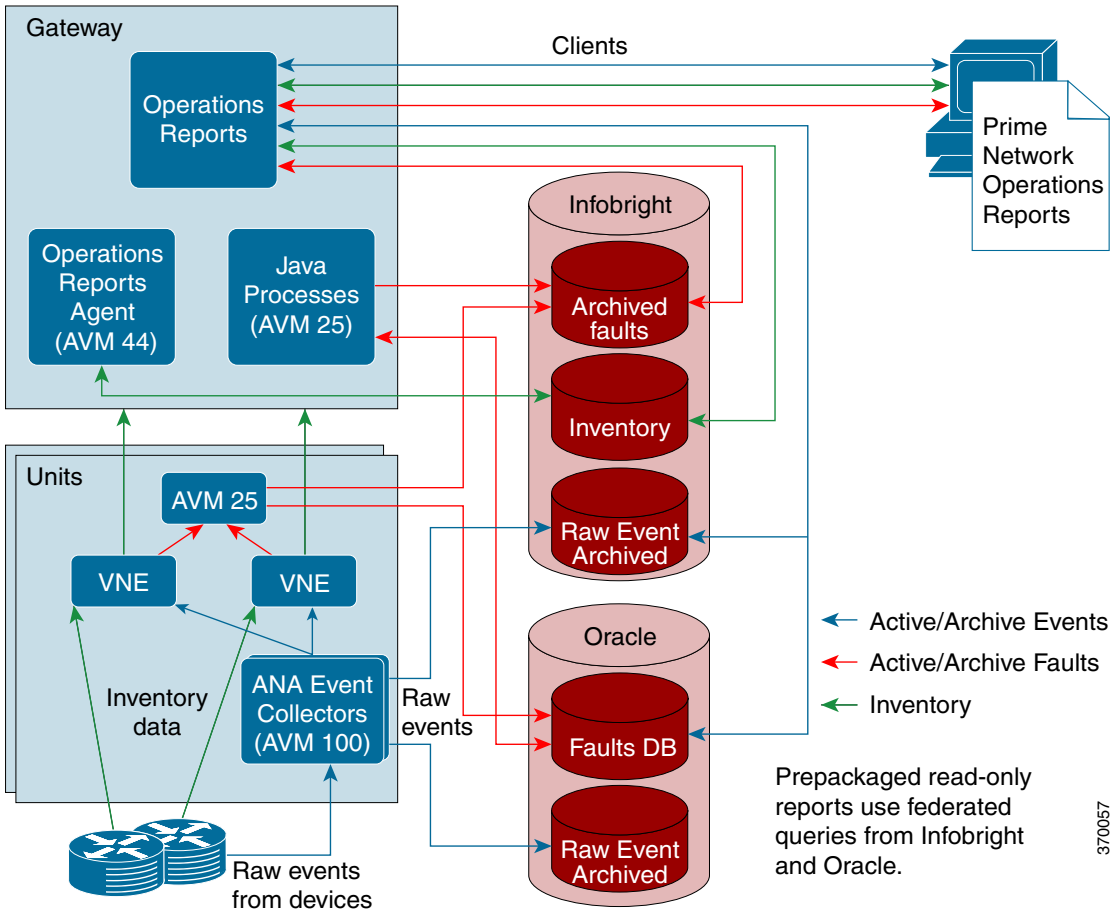
Within Prime Network, Operations Reports has a dedicated AVM (AVM 44) that processes the information received from the VNEs and sends it to the Operations Reports agent on the gateway, and from there to the Infobright database.

Operations reports fetches data as described below:

- The inventory data is handled by AVM 44, which reads and writes from Infobright database.
- The raw events that are sent by AVM 100 are processed by the VNEs and are sent to AVM 25; AVM 25 then writes the data to both Oracle and Infobright databases. AVM 25 that is present in the gateway performs a two-way communication with the fault database component in Oracle and then writes the archived faults data to Infobright database. Operations Reports uses the data that is available in Infobright database to generate reports. The archived events are read from Infobright database and the active events are read from the Oracle database.
- AVM 100 writes the raw events to both Oracle and Infobright databases. The raw events are read from Infobright database.

The following diagram illustrates how Prime Network components interact with Operations Reports and with the Infobright database.

Figure 2-1 Prime Network Operations Reports Architecture



It takes up to five minutes for changes made in the Prime Network GUI clients to be reflected in Operations Reports. For example, when a VNE is added to the system, it is not shown in Operations Reports until the VNE is in one of the following states: OPERATIONAL, PARTIALLY_DISCOVERED, or CURRENTLY_UNSYNCHRONIZED. This could take up to five minutes. Other changes to devices, such as port up/down, might take less time to be reflected in the reports.

Upon adding or deleting VNEs, it takes approximately 30 minutes for the Device Selector list to be updated; to manually refresh and view the changes, see Manually Refreshing Operations Reports to Show VNE Changes, page 2-8.

Setting Up Operations Reports

This section describes the tasks that the administrator needs to perform when setting up Operations Reports. It includes the following topics:

- Managing User Access Rights for Operations Reports, page 2-3
- Enabling Reports to be Sent by E-mail, page 2-4

Managing User Access Rights for Operations Reports

Operations Reports uses SSO (Single Sign On). User authentication is performed using the same method being used by the other Prime Network components (internal or LDAP).

Operations Reports uses the same RBAC (Role-Based Access Control) facilities as are used in the rest of Prime Network—device scopes and user access rights. Users can only see Operations Reports data for devices that are in their device scope. Users have permissions for certain actions depending on their user role (Administrator, Configurator, and so on). Administrators have full permissions and can grant permissions to other user role, as described in Granting User Permissions for Reports, page 2-3.

Granting User Permissions for Reports

For each report folder or individual report, the administrator can determine which actions can be performed by the various user roles (Configurator, Viewer, and so on). By default, Administrators have full permissions and all other user roles are allowed to execute reports.

An example of granting permissions on the folder level might be if you want to prevent certain users from viewing and accessing data center reports. In this case, you would remove permissions on the folder level. The folder will not be visible to those users.

On the individual report level, you might want to add privileges allowed for a certain type of user, for example, allow a Configurator user to delete reports.

Note All reports inherit the Execute permission that is set at the respective folder level. For a non-admin user, if the Execute permission at report level is unchecked, and the Execute permission for the folder is checked, the folder is visible, but the report is not visible. However, if the Execute permission is unchecked at folder level and is checked at the report level, both the folder and the report are not visible.

To assign user permissions:

Step 1 In the Browse pane, right-click on the folder or report for which you want to grant permissions and select **Properties**.

Step 2 In the Properties dialog, click the **Share** tab.

Step 3 Select the user role for which you want to grant permissions, and check the actions you want to allow for that user role for the selected report or folder.

Step 4 Click **OK**.

Enabling Reports to be Sent by E-mail

When scheduling prepackaged read-only reports, users have the option to send the report to a specified recipient by e-mail. The administrator must set up Operations Reports to communicate with the SMTP server in order to enable this functionality.

To enable the e-mail facility:

Step 1 Locate and open the email_config.xml file under the $PRIME_NETWORK_HOME/pentaho/server/biserver-ee/pentaho-solutions/system/smtp-email/email_config.xml

Step 2 Configure the SMTP server details. Figure 2-2 shows a sample email_config.xml file.

Step 3 Save the file.

Step 4 In Operations Reports, choose **Tools > Refresh > System Settings** to update the system with your changes.

Step 5 After you complete the configuration, you must restart the server using ctlscript.sh restart under the

$PRIME_NETWORK_HOME/pentaho/ctlscript.sh restart

Figure 2-2 Sample SMTP Configuration File

```
<?xml version="1.0"?>
- <email-smtp>
        <!-- The values within <properties> are passed directly to the JavaMail API. For a list of valid properties see
        http://java.sun.com/products/javamail/javadocs/index.html -->
    - <properties>
            <!-- This is the address of your SMTP email server for sending email. e.g. smtp.pentaho.org -->
        <mail.smtp.host>144.254.72.80</mail.smtp.host>
            <!-- This is the port of your SMTP email server. Usually this is 25. For GMail this is 587 -->
        <mail.smtp.port>25</mail.smtp.port>
            <!-- The transport for accessing the email server. Usually this is smtp. For GMail this is smtps -->
        <mail.transport.protocol>smtp</mail.transport.protocol>
            <!-- Usually this is 'false'. For GMail it is 'true' -->
        <mail.smtp.starttls.enable>false</mail.smtp.starttls.enable>
            <!-- Set to true if the email server requires the sender to authenticate -->
        <mail.smtp.auth>false</mail.smtp.auth>
            <!-- This is true if the email server requires an SSL connection. Usually 'false'. For GMail this is 'true' -->
        <mail.smtp.ssl>false</mail.smtp.ssl>
            <!-- Run Email Send Test -->
        <mail.run.send.test>true</mail.run.send.test>
            <!-- Output debug information from the JavaMail API -->
        <mail.debug>false</mail.debug>
            <!-- For GMail this is 'false' -->
            <!--mail.smtp.quitwait>false</mail.smtp.quitwait-->
    </properties>
        <!-- The is the address of your POP3 email server for receiving email. e.g. pop.pentaho.org -->
        <!-- It is currently not used -->
    <mail.pop3/>
        <!-- This is the default 'from' address that emails from the Pentaho BI Platform will appear to come from e.g.
        joe.pentaho@pentaho.org -->
    <mail.from.default>pn40@cisco.com</mail.from.default>
        <!-- This is the user id used to connect to the email server for sending email It is only required if email-authenticate is set to true
        This is never sent or shown to anyone -->
    <mail.userid/>
        <!-- This is the password used to connect to the email server for sending email It is only required if email-authenticate is set to
        true This is never sent or shown to anyone -->
    <mail.password/>
</email-smtp>
```

370233

Troubleshooting Tasks

This section describes the tasks that the administrator might need to perform when troubleshooting problems with Operations Reports. It includes the following topics:

- Checking the Status of AVM 44, page 2-5
- Stopping/Starting Operations Reports Processes, page 2-5
- Resolving POODLE Vulnerability in Prime Network, page 2-6
- Monitoring Log Files, page 2-7
- Manually Refreshing Operations Reports to Show VNE Changes, page 2-8
- Manually Reloading Report Folders to Show New Reports, page 2-8

Checking the Status of AVM 44

AVM 44 is dedicated to Operations Reports. It transfers the inventory data to Infobright database. If AVM 44 is down, running inventory reports will fail. These reports would need to be rerun when AVM 44 is up again.

To check the status of AVM 44:

Step 1 Log into the gateway server as *pnuser*.

Step 2 Enter the following command to show the status of all the gateway processes, including AVM 44:

 # networkctl status.

Stopping/Starting Operations Reports Processes

As part of your troubleshooting activities, you might want to stop the Operations Reports processes. There are two processes that should be stopped: Jetty and Bootstrap.

Note When the processes are stopped, the Operations Reports Web pages are unavailable.

To stop the Operations Reports processes:

Step 1 Log into the Prime Network gateway as pnuser and make sure you are in the Prime Network home directory.

Step 2 Stop the Operations Reports script:

```
cd ~/pentaho
./ctlscript.sh stop
```

Step 3 Identify the Operations Reports Jetty process ID:

```
pn40# ps -ef | grep jetty | grep -v grep
```

The process ID is identified in the output. In the example below, it is 10174.

```
pn40     10174 10148 16 16:01 pts/3    00:00:08 /export/home/pn400/pentaho/java/bin/java -
```

Step 4 Stop the process:

```
pn40# kill -1 process-id; sleep 1
```

Step 5 Verify that the process is no longer running using the following command. You should get no response.

```
pn40# ps -ef | grep jetty | grep -v grep
```

Step 6 Identify the Operations Reports Bootstrap process ID (Tomcat process):

```
pn40# ps -ef | grep Bootstrap | grep -v grep
```

The process ID is identified in the output. In the example below, it is 20784.

```
pn40    20784     1 10 15:44 ?        00:01:30 /export/home/pn400/pentaho/java/bin/java -
```

Step 7 Stop the process:

```
pn40# kill -1 process-id; sleep 1
```

Step 8 Verify that the process is no longer running using the following command. You should get no response.

```
pn40# ps -ef | grep Bootstrap | grep -v grep
```

Before starting a new Operations Reports script from the Pentaho server, ensure that you stop the Operations Reports that is running using the following script **./ctlscript.sh stop** or the **kill** command.

To start the Operations Reports processes:

Step 1 Log into the Prime Network gateway as pnuser and make sure you are in the Prime Network home directory.

Step 2 Start the Operations Reports script:

```
cd ~/pentaho
./ctlscript.sh start
```

You must be able to launch Operations Reports successfully after starting the processes.

Resolving POODLE Vulnerability in Prime Network

POODLE vulnerability potentially allows sensitive information to be obtained from the remote host with SSL or TLS-enabled services. Prime Network supports services that can enable TLS fallback Signaling Cipher Suite Value (SCSV) mechanism and disable SSLv3 to resolve the POODLE vulnerability.

The TLS fallback SCSV mechanism prevents version rollback attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.This impact processes on port numbers 1311 and 8445.

To enable TLS services, perform the following steps:

Step 1 Log into the Prime Network gateway as pnuser and make sure you are in the Prime Network home directory.

Step 2 Install Pentaho in the Prime Network gateway server. The remote host supports the use of SSL ciphers that offer high-strength encryption (256 bits) SSL ciphers.

Step 3 Check if Pentaho is running using the following commands:

```
ctlscript.sh stop
ctlscript.sh start
```

Step 4 Change the browser settings:

- In Internet Explorer, choose **Setting > Internet Options > Advanced**.
  In the **Advanced** window, select the **SSL 2.0** option under **Security**.
- In Mozilla Firefox, perform the following steps to enable SSLv3:
  a. Enter **about:config** in the address bar of the Mozilla Firefox browser.
  b. Open the detailed list of configuration parameters.
  c. Check if the value for the **security.tls.version.min** option is **0** to turn on the support for SSLv3.
  d. Search for the **security.ssl** option and change the value from **false** to **true**. The value for all ciphers do not include **aes_256** in the name.
- In Mozilla Firefox, perform the following steps to enable TLS:
  a. Enter **about:config** in the address bar of the Mozilla Firefox browser.
  b. Open the detailed list of configuration parameters.
  c. Check if the value for the **security.tls.version.min** option is **1** to turn on the support for TLSv1.
  d. Search for the **security.ssl** option and change the value from **true** to **false**. The value for all ciphers do not include **aes_256** in the name.
  e. View the Prime Network monitoring graphs using the port number 1311.
  a. View the Prime Network reports using the port number 8445.

Monitoring Log Files

Table 2-1 lists the Operations Reports log files that are created and stored. You can view these files using any text editor.

Table 2-1 Gateway Server Log Files

Gateway Server Log File	Found in the Server...	Component
44.out	Gateway server	Operations Reports
From the folder, the Infobright integration zip file is extracted to: primenw_integration_<*date*>.log	Gateway server	Infobright database installation log
/usr/local/infobright/IBRestore/Log/IBRestore_*ddmmyy_hhmmss*.log	Infobright database server	Infobright database restore log
/usr/local/infobright/data/brighthouse.log /usr/local/infobright/data/bh.err	Infobright database server	Infobright database log
/usr/local/infobright/data/Old_Log	Infobright database server	Infobright database old logs

Manually Refreshing Operations Reports to Show VNE Changes

When VNE changes are made in Prime Network, for example, a new VNE is added, it takes approximately 30 minutes before the new device appears in the device selector in Operations Reports. Administrators can manually refresh the system so that the VNE changes are reflected in the Operations Reports GUI.

To manually refresh Operations Reports:

Step 1 Choose **Tools > CDA Cache Manager**.

The CDA Manager launches.

Step 2 Click on **Cached Queries**, and then click **Clear Cache**.

Step 3 Check that the new device now appears in the device selector when creating or generating a report.

Manually Reloading Report Folders to Show New Reports

If you create a new report, it will be added to the specified folder in the Browse pane. However, it will not be visible to other users on the same server unless you do a manual reload.

To manually reload report folders:

Step 1 Choose **Tools > Refresh > Repository Cache**.

Step 2 Check that your new report is visible to other users in the relevant report folder.

Managing Infobright Database Operations

The Infobright database is dedicated to Prime Network Operations Reports. It can be installed on the gateway server or on a separate server.

The following data is stored in the Infobright database under schema **pnibdb**:

- Archived fault database information—Data that has been moved to the archive partitions in the Oracle database (NETWORKEVENT, ALARM, TICKET, NEWTRAPEVENT, NEWTRAPVALUE).
- Raw events in the event archive (HP_TRAP, HP_SYSLOG).
- Inventory information used by Operations Reports. Inventory information is sent to the Infobright database by the Operations Reports engine (AVM 44), which runs on the gateway.

The data for the Network Service Reports is obtained from the Oracle database. However, unlike the Oracle database, the **pnibdb** schema does not have active and archive partitions. All the data is kept in a single table. The Infobright database is regularly backed up by Prime Network, as described in Backing Up and Recovering the Infobright Database, page 2-11. Data is purged by default after 180 days, but this setting can be changed during installation or at a later stage, as described in Changing Settings for Purging Infobright Backups, page 2-12.

Starting/Stopping the Infobright Database

Note Make sure that the Prime Network system is operational before stopping the database.

To stop/start the database:

Step 1 Log into the database as the root user.

Step 2 Enter the following command:

```
/etc/init.d/mysqld-ib stop
or
/etc/init.d/mysqld-ib start
```

Stopping the Writing of Information to the Database

To stop writing data to the database:

Step 1 Log into the Prime Network gateway as pnuser.

Step 2 Enter the following command:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 persistency/nodes/infobright/enable false
```

Step 3 Restart the Prime Network gateway:

```
# cd $ANAHOME/Main
# networkctl restart
```

Enabling/Disabling Infobright Backup Process

This setting is defined during installation.

To change the setting for writing data to backup files:

Step 1 Log into the database as pnuser.

Step 2 Enter the following command:

```
runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 persistency/nodes/infobright/enableBackupFiles
true/false
```

Step 3 Restart the Prime Network gateway:

```
# cd $ANAHOME/Main
# networkctl restart
```

Controlling When Operations Reports Data is Purged

To protect system stability and performance, Prime Network purges historical data from the Infobright database after 180 days (default). This setting can be changed during installation or at a later stage.

Note The settings in **Global Settings > Report Settings** do not affect Operations Reports.

To change the default setting that determines when data is purged from the Infobright database:

Step 1 Log into the gateway as *pnuser* and change to the Main directory.

Step 2 Check the current data purge setting for the Infobright database and change the arch_history value (in days) as required:

```
runRegTool.sh -gs 127.0.0.1 get 0.0.0.0 persistency/nodes/infobright/arch_history
180
```

Step 3 Restart AVM 11 using **networkctl**.

Monitoring Infobright Data Logs

Infobright data logs are stored on the Prime Network gateway server in the following location:

/usr/local/infobright/data
bh.err
brighthouse.log

Log files are rotated daily. Old files are kept under /usr/local/infobright/data/Old_Log, using the following naming convention:

<file_name>.YYYY-MM-DD

Old logs are kept for 30 days, then deleted.

Backing Up and Recovering the Infobright Database

This section describes the Infobright database backup and restore mechanism and provides procedures for basic tasks that the administrator might need to perform. It contains the following topics:

- How the Infobright Database Backup Works, page 2-11
- Checking that Backups are Taking Place, page 2-12
- Changing Settings for Purging Infobright Backups, page 2-12
- Recovering the Infobright Database, page 2-13

How the Infobright Database Backup Works

Infobright database backups are enabled during installation. Because Infobright data is continuously backed up, you cannot change the backup timing or perform a manual backup.

The working directory for creation and processing of backup files is the “ibdlp” directory in persistency.xml, located on the Prime Network gateway and units. The location of this directory is specified during installation. To identify the location of the working directory, enter:

cd Main; ./runRegTool.sh localhost get persistency/nodes/infobright/ibdlp

The following sub-directories are created under the ibdlp directory:

- DLP_Active_Files
- DLP_Input_Files
- DLP_Log_Files
- DLP_Output_Files
- DLP_Rjct_Files

The flow of the Infobright database backup is as follows:

1. Prime Network processes, such as auto-archive, AVM 25 and AVM 100, write data to the Infobright database and generate a text file in the DLP_Active_Files directory for each fault and event persistency (EP) table (HP_TRAP, HP_SYSLOG, NETWORKEVENT, ALARM, TICKET, NEWTRAPEVENT, NEWTRAPVALUE).
2. The text file is closed after one hour and moved to the DLP_Input_Files directory.

3. Every ten minutes, a cron job DLP process generates a compressed Infobright backup file from the closed text file and places it in the DLP_Output_Files directory. It also creates a log file under the DLP_Log_Files directory. If the cron job DLP process fails, a RJCT file is generated and placed in the DLP_Rjct_Files directory, and a system event is generated.
   This cronjob is configured under prime-network crontab:
   $SHEERHOME/Main/unix/cron/every_10_minutes.main.gateway.cmd DLPProcessExecuter
4. A cron job SCP process transfers the backup file from the DLP_Output_Files directory to the backup directory on the database server (ibbackup). The path to this directory is specified during installation.
   This cronjob is configured under root crontab:
   */10 * * * * /var/adm/cisco/infobright/move_dlp_files.sh >/dev/null 2>&1

Checking that Backups are Taking Place

You can verify that backups are happening by checking the backup directory specified during installation. Backups will begin appearing 1-2 hours after events noise starts on the Infobright database server.

To identify the location of the backup directory, use this command:

cd Main; ./runRegTool.sh -gs 127.0.0.1 get 0.0.0.0 persistency/nodes/infobright/ibbackup

We recommend that you maintain a copy of the backup files in an external storage device if one of the following apply:

- You prefer to retain a longer backup history than the one configured in the bkp_history parameter.
- If the backup directory cannot accommodate all the files due to lack of space.
- You prefer to save a duplicate version of the backup files to recover from a disk failure.

Changing Settings for Purging Infobright Backups

By default, backups are purged after 180 days.

To change the settings for purging Infobright backups:

Step 1 Log into the gateway and change to the Main directory.

Step 2 Check the current backup purge setting for Infobright backups:

```
./runRegTool.sh -gs 127.0.0.1 get 0.0.0.0 site/persistency/nodes/infobright/bkp_history
```

Step 3 To change the setting, specify the number of days after which backups should be purged.

```
# ./runRegTool.sh localhost 127.0.0.1 set 0.0.0.0
site/persistency/nodes/infobright/bkp_history value
```

Step 4 Log into the Infobright DB server as root user. From the following script, edit the **mtime +number_of_days** to reflect the new setting:

```
/var/adm/cisco/infobright/ibbackup_clean.sh.
```

Recovering the Infobright Database

The Infobright recovery procedure can be used to load backup files into a fresh Infobright database. To do this, prepare the following:

- A backup directory containing all your backup files.
- A fresh installation of the Infobright database.

To recover the Infobright database:

Step 1 Rename the **ibbackup** directory or save it to a different location, to prevent the directory from being removed during the uninstall procedure. For example:

```
mv ibbackup ibbackup_old.
```

Step 2 Reinstall the Infobright database. This creates a fresh database, which is required for the recovery process.

Step 3 Log into the Infobright database server as the Infobright UNIX root user, and move to the following directory:

```
# cd /var/adm/cisco/infobright
```

Step 4 Start the recovery script:

```
# ./ib_recovery.sh
```

You will be prompted for the following information:

- The Infobright schema name. Use the default (**pnibdb**).
- The path to the directory containing your backup files (see Step 1).

The script will list the available date ranges for the recovery operation.

Step 5 Choose the recovery option you require.

If you want to:	Choose the following:
Recover all the backed up data	**1. FULL LOAD**
Recover only backed up data from a specified time period	**2. PARTIAL LOAD**

Step 6 If you chose PARTIAL LOAD, enter the start and end time when prompted.

Restarting the Recovery Process After a Recovery Failure

To restart the recovery process after an interruption or recovery failure:

Step 1 Start the recovery script:

```
# ./ib_recovery.sh
```

Step 2 Choose **3. RESUME A FAILED LOAD SESSION**.

Step 3 Enter the same information (schema and backup directory) as you did for the interrupted/failed recovery.

Step 4 When the script displays the previous recovery ID, type, and start time, confirm the choice. (The script automatically uses the information from the last recovery operation.)

Step 5 Check the recovered tables for duplicates.

a. Start the recovery script:

```
# ./ib_recovery.sh
```

b. Choose **4. CHECK DUPLICATES**.

- If duplicates are found in a production system, repeat the recovery process.
- If duplicates are found in a test setup, you can rerun the recovery script with option **5. TRUNCATE FAULT AND EVENT ARCHIVE (EP) TABLES - Truncate tables in preparation for load.**" and then repeat the recovery process.

c. Enter the same information (schema and backup directory) as you did for the interrupted restoration.

Recovery Log Files

For each operation (full load, partial load, resume failed operation, truncate tables), a log is created and placed in /usr/local/infobright/IBRestore/Log/IBRestore_*ddmmyy_hhmmss*.

If the recovery process fails, you can investigate further by querying the following Infobright tables under pnibdb schema:

- PNIB_RECOVERY_INFO - Holds one row for each recovery run
- PNIB_RECOVERY_LOG - Holds many rows for each recovery run, with detailed information about the activities and files involved.

Backup and Restore Customized Reports

To backup and restore Customized reports:

Step 1 Copy the primenetwork-reports folder to your local server.

```
Example: $ANA_HOME/pentaho/server/biserver-ee/pentaho-solutions/primenetwork-reports
```

Step 2 Rename the ibbackup directory or save ibbackup directory to a different location. This is to prevent the directory from being removed during uninstallation.

```
Example: mv ibbackup ibbackup_old.
```

Step 3 Re-install the Prime Network, Oracle and Operations Reports.

Step 4 After re-installation, remove the primenetwork-reports directory.

```
For example, remove the primenetwork-reports from
$ANA_HOME/pentaho/server/biserver-ee/pentaho-solutions/primenetwork-reports.
```

Step 5 Paste the primenetwork-reports directory.

Note You must paste the primenetwork-reports directory which you already have on your local machine to the location "$ANA_HOME/pentaho/server/biserver-ee/pentaho-solutions/"

Step 6 Change the primenetwork-reports folder permission to pnusername:ana

```
For example, if pn user name is pn50, then the permission should be pn50:ana.
```

Step 7 To recover the database follow the steps mentioned in the Recovering the Infobright Database procedure.

Step 8 Launch the Prime Network Operations reports by manually entering the following URL in your browser address field:

https:// < gateway-IP >:< port-number >/ prime-network-reports/Login and view the Customized report.

If the Customized report is not available, do the following

Click **Tools > Refresh > Repository Cache** to view your customized report under the Files pane.

Note Files pane is located at the left bottom of the home page.

Using Prepackaged Reports

Operations Reports provides many prepackaged reports that cover a wide range of data available in Cisco Prime Network. The following categories of prepackaged reports are available:

- Data Center Reports
- Fault Reports
- Mobility Reports
- Network Service Reports
- Physical Inventory Reports

Some of the prepackaged reports are customizable, allowing you to tweak them to meet your organization's needs.

In addition, some of the prepackaged reports allow you to drill down to more granular details. For example, if you ran the Device Administration report, device details are displayed in the report, with each IP address hyperlinked. Clicking the IP address opens a new report with device details. This report can be opened only through a read-only prepackaged report. Additionally, the read-only prepackaged reports can be scheduled and viewed in a preferred format.

Note You cannot delete prepackaged reports.

This section contains the following topics:

- Generating Reports, page 3-1
- Prepackaged Data Center Reports, page 3-4
- Prepackaged Fault Reports, page 3-6
- Prepackaged Mobility Reports, page 3-11
- Prepackaged Network Service Reports, page 3-12
- Prepackaged Physical Inventory Reports, page 3-15

Generating Reports

The procedure to generate a report depends on the type of report you choose. Customizable prepackaged reports are denoted by a small pencil icon next to the report name in the left navigation pane. A plain report icon indicates that the report is ready-only. To see the image, see Figure 1-2.

This section contains the following topics:

- Generating Customizable Prepackaged Reports, page 3-2
- Generating Read-Only Prepackaged Reports, page 3-2
- Refreshing Prepackaged Read-Only Reports, page 3-4

Generating Customizable Prepackaged Reports

To generate a report:

Step 1 Double-click the report from the left navigation pane.

Step 2 If you are viewing Fault reports, you must first set the period for which you need the fault data to be reported. Click the **Prompts** icon and set the **From** and **To** dates.

Step 3 Click **View Report.**

If the Output type is PDF, and if you are using the Google Chrome browser, ensure to do the following:

1. Choose *chrome://plugins/*.
2. In the **Chrome PDF Viewer** area, toggle the mode from **Enable** to **Disable**.
3. In the Operations Reports window, click **View > Refresh.**
4. Click **View Report** to view and download, or Print the selected report in the Reporting pane.

Step 4 If you wish to customize the report to suit your requirement, from the left navigation pane, choose the report, and click the **Edit** icon. The customizing options are now available. For more information, see Customizing Reports, page 5-1.

Generating Read-Only Prepackaged Reports

To generate a report:

Step 1 From the left navigation pane, choose the report you prefer to run.

Step 2 Enter the parameters, as required. From the example shown in Figure 3-1 for a report Virtual Machines per Hypervisor, the details required are the devices for which a report must be generated, the output type, and the number of pages the report must span.

Note If you are generating Fault reports, you must select the period for which the fault data must be reported.

A report can be generated in one of the following formats:

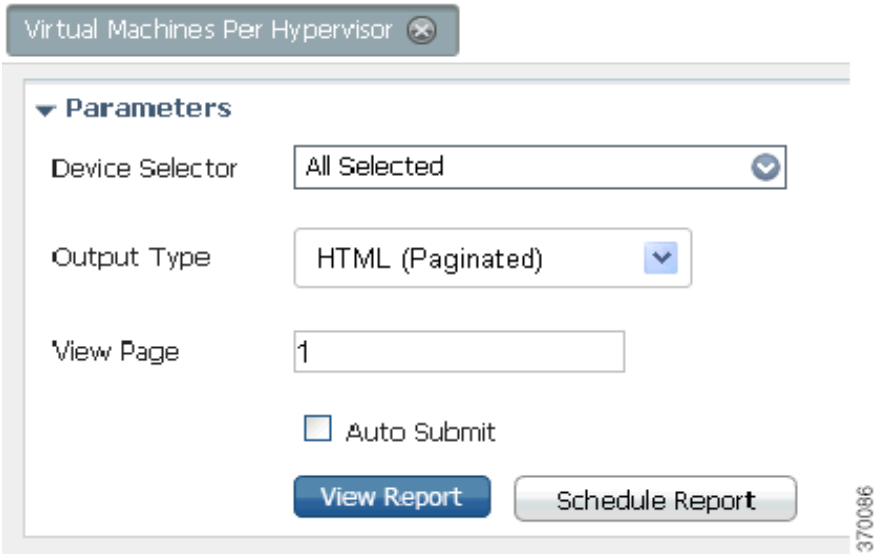
- HTML—Displays the report in a browser window. HTML is the default format. The report contains only one HTML page with the report data.
- HTML (Paginated)—Some reports that represent voluminous data have the option of HTML paginated view for better usability. If you selected this option, the report is split into several pages. The first page opens by default. To view the subsequent pages, enter the page number in the **View Page** field.

- PDF—Displays a PDF version of the report.

Note If you are using the Google Chrome browser, you must ensure that Chrome PDF Viewer is in the disable mode. To disable the Chrome PDF Viewer, choose *chrome://plugins/* and toggle the Chrome PDF Viewer to Disable mode. After you complete the setup, you should refresh your selected report area in the right pane (Click **View > Refresh**), to view and download the PDF 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.
- RTF—Creates an RTF version of the report that you can either save to a specific location or view using another application, such as Microsoft Word.

Figure 3-1 Parameters Window



Step 3 Click **View Report.**

Alternatively, check the **Auto Submit** check box to generate the report as you select the parameters.

Operations Reports generates and presents a latest report. Depending on the type of report, the data may be presented in a bar chart, pie chart, table, or a trend diagram.

If there is no connection to the database, while generating read-only prepackaged report, the following message appears:

```
Error processing component.
```

Refreshing Prepackaged Read-Only Reports

By default, prepackaged read-only reports are updated with the latest changes in database when you open the report from the left navigation pane. If new devices are added, the devices appear in the Device Selector list after one hour of generation of the report for the first time. To view the updated list of devices in the Device Selector, close and reopen the report.

However, it takes up to five minutes for changes made in the Prime Network GUI clients to be reflected in Operations Reports. For example, when a VNE is added to the system, it is not shown in Operations Reports until the discovery is complete which could take up to five minutes. Other changes to devices, such as port up/down, might take less time to be reflected in the reports. After the expiry of 5 minutes, click **View Report** for the report to be updated with the relevant data.

Prepackaged Data Center Reports

Using prepackaged data center reports, you can view data center inventory details such as that of VM and host. It can also be used to view vital statistics of the host and VM; the reports present data on VMs based on state, based on the hypervisor it is associated with, or based on their current state such as powered off state or suspended state. The host and VM statistics are updated every 15 minutes. This section lists the data center reports that are provided with Operations Reports and provides a general summary of the content of each report.

Report Name	Description
Customizable Reports	
Virtual Machine State Distribution	Generates a report of virtual machines based on state. Provides the VM details such as VM IP address, VM State, MAC address, VM version. Using this report, you can view the following fields as well: • Fault Tolerance Enabled • VM Up time • VM Communication State • VM Lifecycle State
Virtual Machine Per Hypervisor	Generates a report of the number of virtual machines associated with a hypervisor. This provides host details, hypervisor details such as version, start time, software type, number of VMs, and the associated VM count.

Report Name	Description
Virtual Machines - Powered Off State	Provides a report on the number of virtual machines which are powered off. Using this report, you can view the following fields of a virtual machine: • Virtual Data Center Name • Host Name • VM Name • VM IP Address • VM Description • MAC Address • VM State • Virtual CPU • Fault Tolerance Enabled • VM Up time • UUID • VM Communication State • VM Lifecycle State
Virtual Machines - Suspended State	Provides a report of the virtual machines that are operationally down. Using this report, you can view the following fields of a virtual machine in suspended state: • Virtual Data Center Name • Host Name • VM Name • VM IP Address • VM Description • MAC Address • VM State • Virtual CPU • Fault Tolerance Enabled • VM Up time • UUID • VM Communication State • VM Lifecycle State
Read-Only Reports	

Report Name	Description
Virtual Machine State Distribution	Generates pie charts that depict the distribution of devices by their state. It also displays the device name, VM name, IP address, VM state, and UUID. The number of devices that you selected when generating the report is displayed below the pie chart. Click the respective device state in the pie chart to filter and view the details of devices that are in a particular state. The selected filters appear in the beginning of the table that displays the device details. Click the X link that appears next to a filter to remove that filter.
Virtual Machine Per Hypervisor	For the selected devices, generates a report on the number of virtual machines associated with each hypervisor. Provides information on type of hypervisor, name, description, and the number of VMs associated.
Virtual Machines - Powered Off State	For the selected devices, generates a report on the number of virtual machines that in the state 'Powered Off'. Provides information on name of device, VM name, IP address, VM state, and UUID.
Virtual Machines - Suspended State	For the selected devices, generates a report on the virtual machines in the state 'Suspended'.

Prepackaged Fault Reports

Fault reports help you understand the various types of faults that arise in the network. Fault report include various reports on network event and non-network events. Non-network events reports are listed in Table 3-1.

The reports help you understand your deployments and the state of operations better. Using the data that the reports present, network operations center (NOC) managers are better positioned to take decisions that can increase the efficiency of the operations.

Some of the reports can be used for daily management of NOCs while others can be used for long-term planning. For example, using the Daily Average and Peak report, you can understand when the number of events peaks. This could be directly linked to another network activity such as an installation or addition of network elements. If this pattern occurs for an extended period, it may indicate the need to perform capacity planning such as upgrade the hardware availability in the network.

However, reports such as Archived Event Count per Device helps capacity planning, configuration changes analysis, service planning, and service changes analysis. An analysis of the events for a certain period on a certain number of devices, may be indicative of a systemic problem in some of the devices. This may be a symptom of an underlying issue such as device maintenance. The NOC managers may have to look at the mean time to replace the hardware equipment in the operation center. For example, if the pattern of events occurs every 18 months instead of a planned window of 20 to 24 months, it may mean that the devices must be replaced once in 18 months.

Customizable reports present data on archived events/tickets. These events or tickets are not active and are the ones that are already cleared. The data present historical trend of events.

Read-only prepackaged reports present both active and archive fault data.

This section lists the fault reports that are provided with Operations Reports and provides a general summary of the content of each report.

Report Name	Description
Customizable Reports	
Archived Event Correlation Statistics	Provides a report of the average, minimum, and maximum number of events that were correlated to each ticket type for a given period. Based on a ticket type, the report displays the lowest, average, and highest number of events correlated.
Archived Event Count by Severity per Device	Generates a report on the event count based on the severity of archived event.
Archived Event Count by Type per Device	Generates a report on the count of each type of archived event.
Archived Syslog Count by Device	Generates a report on the number of archived syslogs for devices.
Archived Syslog Count by Type	Provides a report on the number of archived syslogs by type for a given period.
Archived Syslog Count by Type per Device	Provides a report on the number of archived syslogs by type for each device for a given period.
Archived Trap Count by Device	Generates a report on the number of archived traps by device.
Daily Count of Archived Events per Type	Provides a report on the daily count of archived events for every type for each device for a selected period.
Daily Standard Event Count	Provides a report on the daily count of standard events per detection type for a selected period.
Standard Event Count by Device	Provides a report on the number of standard events by device for a selected period.
Standard Syslog	Provides a report that lists all standard syslogs with severity, device on which the syslog was raised, and total events.
Read-Only Report	
Threshold—Crossing Syslogs	Provides a report that lists the count of events, per syslog type, that has crossed the threshold limit, which was set when generating the report. For example, if the threshold is set to 10, the count of events less than 10 are filtered from the detailed report and the count of filtered events is displayed as Ignored Count. So, the total event count will be the sum of ignored count and the count of events that has crossed the threshold.

Report Name	Description
Daily Average and Peak	Provides a graphical representation of the count of number of events per day. The sampling period can be set to seconds, 10 seconds, minute, hour, or day. For example, if you select the sampling rate to be 10 seconds, the day's duration is split into 10-second intervals, and the number of events occurring in those intervals are represented in the graph. The peak is the highest number of events recorded in a 10-second interval, and average is the total number of events divided by the number of 10-second intervals seen on that day. **Note** Changing the sampling rate does not alter the naming of Y-axis. Despite selecting 10 seconds as sampling rate, the Y-axis defaults to Count of Events per Day. However, the values represented are dynamic and change according to the sampling rate selected. The graph indicates where the activity has been the highest and the lowest. The peak rate of events could be attributed to a particular reason or combination of events. For example, an increase in the number of events at a particular point in a day could be due to external events. The administrator can use this report to determine if the events normalize after the external event is cleared. An example of an external event could be construction equipment interfering with fiber optical lines. Also, if the number of events increases at a particular point in the day, it could indicate a heavy load due to over staffing at that period. To normalize the events, the staff working have to be assigned different shifts.
Events Distribution	Generates pie charts representing the number of events based on devices, severity, and fault category. This report provides a high-level view of where the events arise from. You can identify the event in one of the 11 categories such as Communications, Quality of Service. Based on category of events and their severity, the NOC administrators use the data represented by this report for planning purposes. For example, an increase in the number of Communication events over a particular period may be because of a high number of staff during that period. This may require replanning on allocation of the staff. Similarly, a high number of events in Quality of Service may indicate the need to revisit the configuration policies and to reduce the number of events coming in.
Incoming Events Distribution	Displays a bar chart of the incoming event trend distributed by severity for a selected period. This is a micro-level view of events that are recorded on a daily basis to determine if the day-to-day functioning of the network is as expected.
Incoming Tickets Distribution	Generates a bar chart depicting the distribution of tickets by maximum severity of event for a selected period. This report presents the number of tickets that are incoming on a daily basis, and the number of tickets that are cleared. Using this, the efficiency of staff can be evaluated.

Report Name	Description
Mean Time to Close Tickets	Generates a bar chart of the mean time to resolve tickets for a selected period. This represents the average time taken to resolve a ticket, with the highest time taken to resolve a ticket being the first item. Using this, you can determine which tickets took the longest to close. The time taken is arranged in descending order. The time taken to close a ticket is calculated based on the last modification time, which is the time of the ticket being cleared, and then archived. If the time taken to close tickets is too long, the administrator can analyze the operation procedures involved in closing tickets, and, if required, enhance maintenance operation. **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.
Most Common Syslogs	Generates a pie chart of the syslogs for the selected period. Represents the following data: • Syslog Mnemonic • Count • Severity • First Occurrence Time • Last Occurrence Time Using this report, an administrator can determine the most common syslogs, and check the policies that are configured on network elements to handle the syslogs. If the number of syslogs received are high, with no action being taken on them, the administrator can change the policy to not forward the syslogs to the devices.

Report Name	Description
Ticket Trend	Provides a graphical representation of incoming and archived ticket trend for a selected period. Archived ticket means that the ticket has been acknowledged and cleared. The ticket gets closed one hour after it was cleared if no other related event occurs. This ticket is also archived.
Upgraded Events vs. Standard Events	Provides a report that lists the daily count of each of the following types of upgraded events and standard events for the selected period: • Syslogs • Traps • Tickets • Correlated events • Uncorrelated events • Nonnetwork events • Network-originated events • Network-originated events and services events Use this report to compare the daily number of upgraded and standard events.

Non-Network Reports

Non-network reports covers report for audit, provisioning, security, and system event details. All of these are customizable reports.

Table 3-1 Audit, Provisioning, System, Security Event Reports (Non-Network Reports)

For this non-network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Customizable Reports			
Audit event details: • Severity, timestamp, description • Username, originating IP address • Command details: name, parameters,	Detailed Audit Events	No	Yes
Provisioning Event Details: • Severity, event ID, date and time, description, location • Username, device username, status.	Detailed Provisioning Events	No	Yes

Table 3-1 Audit, Provisioning, System, Security Event Reports (Non-Network Reports)

For this non-network event information:	Use this report:	Can you choose devices?	Can you specify a time period?
Security Event Details: • Severity, event ID, date time, description, location • Username, originating IP address	Detailed Security Events	No	Yes
System Event Details: • Severity, event ID, time, description, location,	Detailed System Events	No	Yes

Prepackaged Mobility Reports

Using prepackaged mobility reports, you can view the details of mobility services that are configured on a device. You can view high-level data of the Access Point Names (APN) that are configured on the various devices, and the other services that are configured. For example, you can view the visiting profiles of the various APNs of the devices chosen. A report with roaming profile and device name can help an administrator determine the APNs that have a specific roaming profile. This helps in planning prior to any configuration changes, such as change of roaming profile.

This section lists the mobility reports that are provided with Operations Reports and provides a general summary of the content of each report.

Report Name	Description
Customizable Reports	
Mobility Gateway Applications	Provides a report of the mobility services configured per device along with the associated service name and the context name.
Read-Only Report	
APNs by Device	This report can also be used to ascertain the APNs that are present in the various devices to facilitate capacity and service planning. This report allows you to compare the various APN properties that are configured on the various APNs in a particular device. Provides a report of Access Point Names configured on devices. Depicts the following data: • Context Name • APN Name Provides APN details upon clicking the APN name listed in the report. To compare the APN properties configured on different APNs, click the APN name from the report, and then compare the properties.

Report Name	Description
Devices by APN	Generates a report of list of devices configured with an Access Point Name. Since each APN can be identified with a service for an enterprise customer, and APNs are configured on a range of gateways, the report can be used to understand which device provides a particular service and how the device can be optimized further. The following details are displayed: • APN Name • Device Count Provides APN details of the APN in a device upon clicking the APN name listed in the report.
Mobility Gateway	Generates a report that specifies if the following mobility services are configured on the selected devices. If a service is configured, the service is marked with Yes against the device on which it is configured. • Serving Gateway • Packet Data Network Gateway • Mobility Management Entity • Home Agent • Packet Data Serving Node • Evolved Packet Data Gateway • Gateway GPRS Support Node • Serving GPRS Support Node

Prepackaged Network Service Reports

Using the Network Service reports, you can generate reports to view virtual connection details with filters such as EVC or map name. The reports also display details such as, layer 2 VPN name and customer label (business tag). The Virtual Connection Summary generates a report with additional details, such as Edge EFPs associated with the EVC or Layer 2 VPN, and EFT fragment name and type.

Using the Network Service reports, you can also view all the services that are created and associated with maps.

Using Network Pseudowire report, you can view network pseudowire information with additional filters such as name, type, or map name. The Network Pseudowire Summary report presents additional information such as pseudowire details and type, pseudowire edge, Ethernet flow point, or switching entity.

The VPLS information presents VPLS/H-VPLS information which you can filter using a VPLS/H-VPLS name or map name, customer labels (business tags), or maps containing the VPLS/H-VPLS instance.

Report Name	Description
Customizable Reports	
Virtual Connection Detailed	Provides a detailed report with the following information for each virtual connection : • Virtual connection or Layer 2 VPN name • Business tag assigned to the virtual connection or layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Virtual connection 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 following: • Virtual connection name • EVC name • Virtual connection business tag • EVC business tag • Map name
Network Pseudowire Detailed	Provides a detailed report with the following information for each network pseudowire: • 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 following: • Pseudowire name • Pseudowire type • Business tag • Map name

Report Name	Description
VPLS Detailed	Provides a detailed report with the following information for each VPLS or H-VPLS instance: • 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 following: • VPLS or H-VPLS name • Business tag • Map name
Read-Only Reports	
Virtual Connection Summary	Provides a summary of the following information for each Virtual connection: • Virtual connection or Layer 2 VPN name • Business tag assigned to the Virtual connection or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Virtual connection or Layer 2 VPN You can filter report content by specifying part or all of the following: • Virtual connection name • EVC name • Virtual connection business tag • EVC business tag • Map name

Report Name	Description
Network Pseudowire Summary	Provides a summary of the following information for each network pseudowire: • 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 following: • Pseudowire name • Pseudowire type • Business tag • Map name
VPLS Summary	Provides a summary of the following information for each VPLS or H-VPLS instance that is associated with a map: • 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 the report content by specifying part or all of the following: • VPLS or H-VPLS name • Business tag • Map name

Prepackaged Physical Inventory Reports

Using Physical Inventory Reports, you can view the current status of your physical devices. For example, to gain a comprehensive view of the different module types configured in the network, you can run Module Type Distribution report. This report lists all modules types (modules and submodules) with hardware serial number, and the software and hardware version of a device. To view further details of a module type, click the respective slice in the pie chart.

To know the modules that run software that are moving towards end of life state, run the Module Summary by Version report. The report can further be filtered to view the required software versions.

Device Administration report presents a general overview of the physical inventory in the network.

This section lists the physical inventory reports that are provided with Operations Reports and provides a general summary of the content of each report.

Report Name	Description
Customizable Reports	
Device Polling Approach	Generates a report on the distribution of devices based on the polling approach. Presents information on device name, polling group, and the polling approach.
Device Polling Approach Summary	Generates a report on the consolidated number of devices that are governed by a polling approach.
Device Summary	Provides details of devices for every device series. For every device series, provides device information on name, type, IP address, communication state, number of chassis, number of modules, and number of ports.
Hardware Detailed	For every device, generates a report on the modules, sub-modules, and the module status.
Module Summary by Device	Presents a report on the module and sub-module details for every chassis and device type. Details include type, serial number, software version, and hardware version.
Module Summary by Type	Generates a report on device details for every chassis, module, and sub-module type. Provides device information such as device IP, module serial number, hardware and software version.
Software Summary by Device	For every device, presents a report on the details of software such as software version, image file, serial number.
Software Summary by Version	For every software version, presents details of associated devices. Details include device type, IP address, serial number, image type.
Read-Only Report	
Device Administration Report	Generates pie charts that depict the distribution of devices by operational status, scheme, and polling group. The number of device series and device vendor that you selected when generating the report are displayed below the pie chart. Click the respective slice in a pie chart to filter and view the details of devices that fall under that particular operational status, scheme, and polling group. The selected filters appear in the beginning of the table that displays the device details. Click the X link that appears next to a filter to remove that filter. In the operational status, devices with Connection Failed, Operational, Maintenance, Not Operational state are displayed in the pie chart.
Device Type Distribution	Generates a bar chart depicting the number of devices by device type. The number of device series and device vendor that you selected when generating the report are displayed below the bar chart. Click the respective bar and the hyperlinked device IP to filter and view the device details. Click the Remove Chart Filter link to remove the filter.

Report Name	Description
Device Unreachable	Provides details of devices with connection failed state in the form of a pie chart. The number of devices that you selected when generating the report is displayed below the pie chart. From the pie chart, click the device status to filter and view the details of every device that belongs to the respective device status. The following details appear: • Name • IP Address • SNMP Protocol • SNMP Protocol State • SNMP Protocol State Since • Telnet Protocol • Telnet Protocol State Click the Remove Chart Filter link to remove the filter.
Module Type Distribution	Generates a bar chart of the distribution of all modules by module types. The number of devices, device series, device vendor, and device type that you selected when generating the report are displayed below the bar chart. Click the bar that represents a particular slot type to filter and view module details. To view the device details, click the hyperlinked device IP address. Click the Remove Chart Filter link to remove the filter.
Software Distribution	Provides a bar chart of the distribution of all devices by software version. The number of device series and device vendor that you selected when generating the report are displayed below the bar chart. Click the bar that represents a particular software type to filter and view the software details. To view the device details, click the hyperlinked device IP address. Click the Remove Chart Filter link to remove the filter.

Creating New Interactive Reports

Operations Reports allows you to create your own reports with the data of your choice. This is useful when the data you need is more specific than what is represented by a prepackaged report. For example, the Mobility Gateway prepackaged reports provide a snapshot view of the services configured on selected devices but they do not provide full details of the services. You can create a new report that includes these details.

The first step in creating a new report is to select the data source on which the report will be based, which will determine what type of information that will be available for inclusion in the report. Then, you can drag and drop the required information into the report, and group and filter it as required. Operations Reports provides live rendering of the report which means that you can see the report layout as you build it.

Once you have created your new report, you can save it in the relevant report folder - Fault, Data Center, Mobility, or Physical Inventory. You can export the report to a format of your choice, including HTML, PDF, CSV, or Excel. On the new report you create, you can add templates, filter, group, and sort data further. Formatting changes can be made on the fly.

All the reports that you create are available in the location it was saved to at the time of creation.

Note You cannot delete interactive reports and the folders.

This section contains the following topics:

- Creating a New Report, page 4-1
- Choosing a Data Source to Determine the Report Content Type, page 4-5

Creating a New Report

To create a new interactive report, follow the steps below. To illustrate the procedure, we will create an example Mobility report to display details of the LTE services in the network.

Step 1 From the Operations Reports home page, go to **File > New > Interactive Report**.

The Select Data Source dialog box appears.

Step 2 Select the Data Source that is appropriate for your report, and click **OK**. To determine the data source that is appropriate for the report you need, see Choosing a Data Source to Determine the Report Content Type, page 4-5.

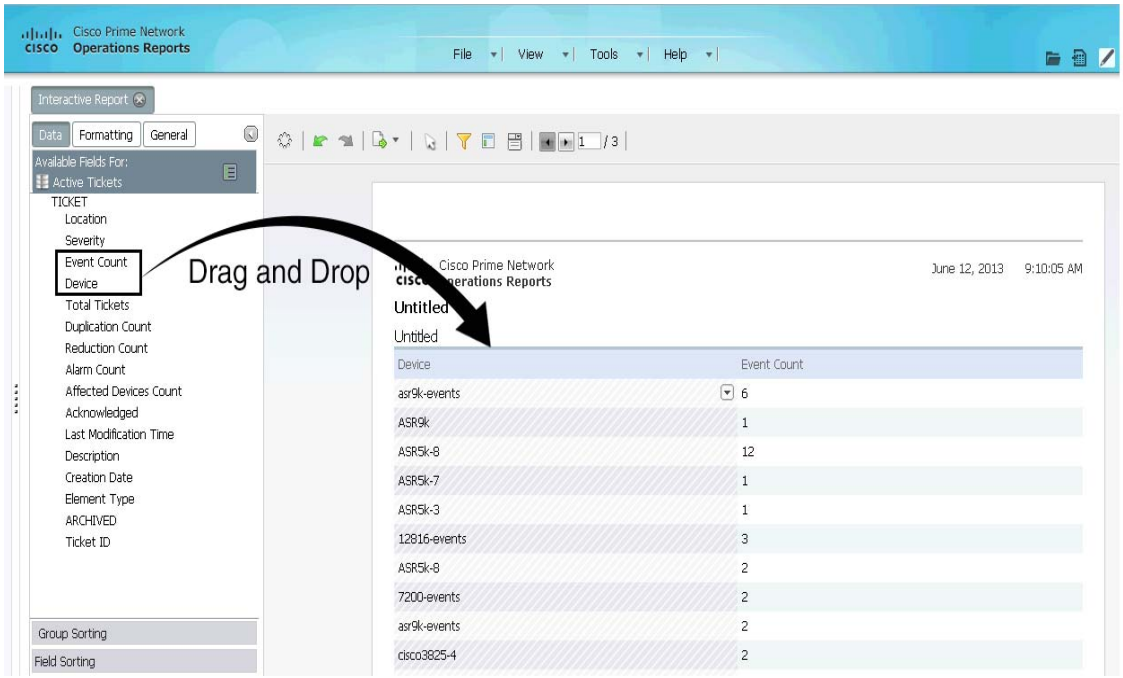
To generate an LTE services report, choose LTE.

The Interactive Reporting page appears.

Step 3 To add your first column, click and drag a field from the **Browse** pane and onto the report pane. You can add as many columns as you require to the report. Repeat this step until you have all the columns of your report in place. For Portrait layout, we recommend that your report contains not more than 7 columns; for Landscape layout, limit the number of columns to up to 12 columns.

Tip If you want to make sure subsequent columns appear in correct order, drag and drop the columns, as required**.** Click the **Undo** or **Redo** buttons in your toolbar, if required.

Figure 4-1 Creating New Interactive Report



You can save your report at this point or continue customizing it. For information on customizing reports, see Customizing Reports, page 5-1.

For this example LTE services report, drag the parameters Device Name, SAE Gateway Service Name, Context Name, Packet Data Network Gateway (PGW) service name, and Serving Gateway (SGW) onto the report. The report displays the SAE gateway, SGW, PGW that are configured for a particular context in each device.

Step 4 Click the **Save** icon on the toolbar.

The Save dialog box appears.

Step 5 In the File Name text box, enter a file name for your report.

Step 6 Browse to locate the folder in which to save your report. The path to the folder which will contain your report appears in the Location text box. You cannot save a report in the root directory.

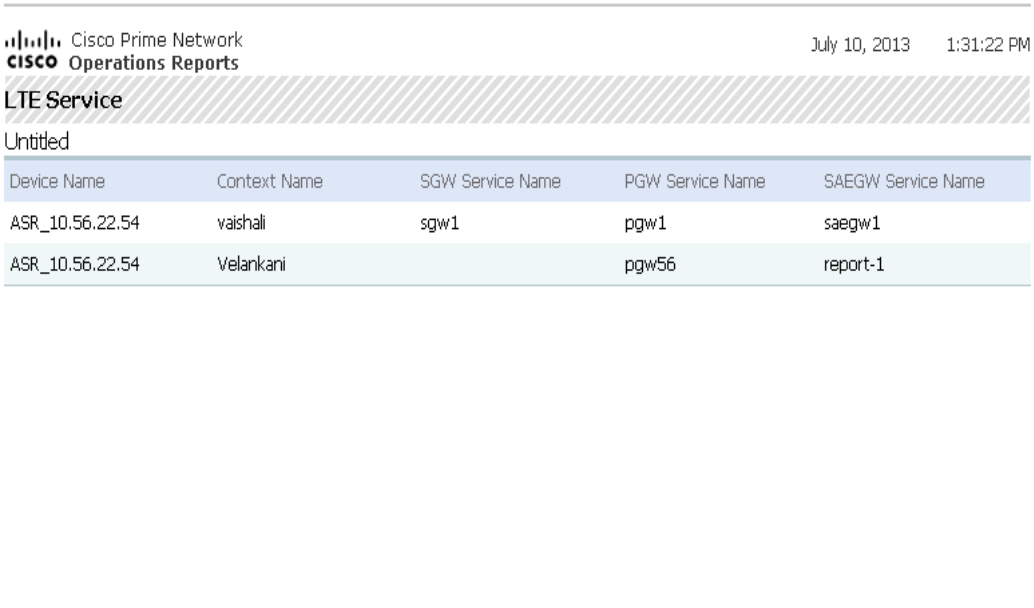
Step 7 Click **Save**.

Step 8 By default, the title of an interactive report reads **Untitled**. To change the title, double-click the word **Untitled** on the upper left corner of the report. Perform the same procedure to change the footer of a report.

Step 9 You can apply templates, change the format and the layout of the report you created. For more information, see Changing the Report Template, page 5-5.

The generated LTE report appears as depicted in Figure 4-2.

Figure 4-2 LTE Service Report—Example



Refreshing Interactive Reports

By default, interactive reports are updated with the latest changes in database when you open the report from the left navigation pane. If new devices are added, the devices appear in the Device Selector list after one hour of generation of the report for the first time. To view the updated list of devices in the Device Selector, close and reopen the report.

However, it takes up to five minutes for changes made in the Prime Network GUI clients to be reflected in Operations Reports. For example, when a VNE is added to the system, it is not shown in Operations Reports until the discovery is complete which could take up to five minutes. Other changes to devices, such as port up/down, might take less time to be reflected in the reports. After five minutes, click **View Report** for the report to be updated with the relevant data.

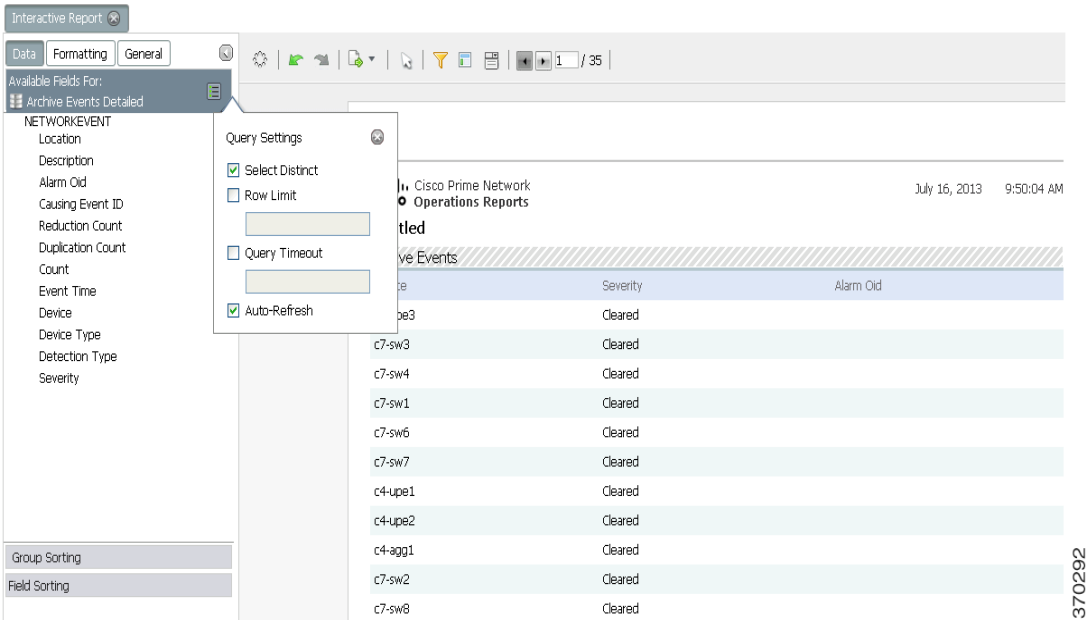
If you prefer the report to be created as you generate and perform the customization, enable the auto refresh option. When you disable the Auto Refresh mode, you can design your report layout first, including calculations and filtering, without querying the database until you are done. Once the report layout is complete, you can re-enable Auto Refresh. Data retrieval will occur once and your report will

display the requested data. Disable auto refresh if you want to reduce the number of queries executed against the data source or if you know that the data source returns data slowly. Follow the procedure given below to enable auto refresh:

Step 1 Open the interactive report. From the left navigation pane, select the **Query Settings** icon.

Step 2 Enable **Auto Refresh.**

Figure 4-3 Enabling Auto Refresh Option



Important Notes to Consider

- If the state of devices is Operational or Partially Discovered or Currently Unsynchronized, the reports contain all device-related details. However, if the state of the device is Discovering, the report contains only the entry for the device. All others details are populated once the device reaches one of the states that is final. To view the device in the device selector drop-down list, close and reopen the report. The device details are updated.
- While creating new reports, you must ensure that the report parameters are related. For example, if you are creating a report to understand the relationship between device connection and Packet Data Serving Node (PDSN) service, you can drag an associated field such as Foreign Agent (FA) service. This creates a report with the PDSN and the related FA services that are configured on a particular device. However, if you wish to view the Home Agent (HA) services that are configured, you must create a new report. Since FA service and HA service are not related, creating a report with two unrelated columns will not present any usable data.
- Create separate reports for data that represent different details. For example, to view the port attributes of modules and submodules, two different reports must be created—one representing port attributes and modules, and another report representing submodules and the its port attributes.

Choosing a Data Source to Determine the Report Content Type

Interactive reports rely on data sources to determine the type of content that will be displayed in the report. Operations Reports provides a predefined set of data sources, each of which extracts from the database a different set of parameters that can be included in the report. From this master list of parameters, you can choose those you want to use in your report. For example, using the model Active Tickets, you can view the following data of active tickets (tickets that are not archived): Location, Severity, Event Count, Device, Count, Duplication Count, Reduction Count, Alarm Count, Affected Devices Count, Acknowledged, Last Modification Time, Description, and Date/Time. This section describes the content that each data source provides and maps the data sources to the relevant report type - fault, physical inventory, mobility, or data center. To view the data that can be represented by each data source, see Appendix A, "Predefined Data in Data Sources".

Note The functionality to create a new Data Source has not been tested and validated on Prime Network 4.2.2 Operations Reports.

Table 4-1 Data Sources to Create New Interactive Reports

Report Category	Maps to Data Source	Description
Physical Inventory	Device	Generates a report on devices that are monitored. Provides information on the following: • Device details such as type, IP address, vendor, series. • Management state of the device such as SNMP state, SNMP enabled state, SNMP protocol. • Telnet connectivity of the device • XML status; includes XML state, XML state description, and XML state since when.
	Module	Generates a report on the module details such as: • Device details. • Chassis details such as name, shelf serial number, shelf status. • Module details such as name, type, software version, hardware version, number of ports. • Sub-module details such as name, type, software version, hardware version, and number of ports. **Note** To generate meaningful reports with module and sub-module data, you must include one of the following combinations: – Module name and module details or sub-module details – Module name and sub-module name. A combination of module details and sub-module details will not render a meaningful report.
	Hardware Inventory	Provides a report on the hardware inventory details: • Device details such as type, IP address, vendor, series. • Chassis details such as name, shelf serial number, shelf status. • Module details such as name, type, software version, hardware version, number of ports, sub module name. • Port details including name, operational status, admin status, connector type, port ID. • Sub-module port details such as sub-module port alias, port location, connector type, pluggable port state.

Table 4-1 Data Sources to Create New Interactive Reports (continued)

Report Category	Maps to Data Source	Description
Mobility	Mobility Applications	Generates a report on mobility applications for the following details: • Device details • Chassis details • Mobility applications—provides details of the configured service • APN charging characteristics such as home profile, home bit behavior, visiting profile, visiting bit behavior. • APN QoS Up/Down link details including negotiation link, peak data rate, rate limit, committed data rate.
	Code Division Multiple Access (CDMA)	For the selected CDMA service, generates a report on the following: • Device details • PDSN service name • APN details such as name, accounting mode, context name, active charging rule base, L3 to L2 address policy.
	CDMA-Systems Architecture Evolution (SAE)	Generates a report on the following for the selected CDMA-SAE service: • CDMA-SAE details including PDSN name, SGW name, FA name. • Device details • APN details such as name, accounting mode, context name, active charging rule base, L3 to L2 address policy.

Table 4-1 Data Sources to Create New Interactive Reports (continued)

Report Category	Maps to Data Source	Description
	Long Term Evolution (LTE)	For the selected LTE, the report displays the following: • Device details • Serving gateway details such as name, status, Egress protocol, accounting policy. • Packet Data Network Gateway (PGW) details such as name, status, QCI QoS mapping table, new call policy. • Mobile management entity (MME) details • APN details such as name, L3 to L2 address policy, accounting mode, IP header compression.
	Universal Mobile Telecommunication System (UMTS)	For the selected device, presents data on the following: • Device details • Gateway GPRS support node • Serving GPRS support node • APN details
	EPC	Displays the following information: • Device details • Serving gateway details • Packet Data network gateway details • Gateway GPRS support node details • SAE gateway details • APN details • MME details
Data Center	Data Center Inventory	Presents a report on the inventory; for the selected vCenter, represents the following: • vCenter details • Host Name • Host statistics • Virtual machine details • Virtual machine statistics

Table 4-1 Data Sources to Create New Interactive Reports (continued)

Report Category	Maps to Data Source	Description
Faults	Archived Events Detailed[1]	For the selected device, displays event details such as location, alarm ID, count, device type, severity.
	Active Events	For a selected device, provides a list of all active events, with details such as duplication count, reduction count.
	Active Tickets	For the selected device, generates a report on the number of active tickets, location, severity, alarm count, duplication and reduction count.
	Archive Events	For a selected device, presents details on the event type, count, first and last occurrence, severity, device, device type.
	Archive Tickets	For the selected device, generates a report on the number of active tickets, location, severity, alarm count, duplication and reduction count.
	Standard Events	For the selected device, displays information such as, event count, reduction count, duplication count, causing event ID, severity, and location.
Network Service	Virtual connection	For each Virtual connection, the report displays: • Virtual connection or Layer 2 VPN name • Business tag assigned to the Virtual connection or Layer 2 VPN instance • EVC name • Business tag assigned to the EVC • Maps containing the Virtual connection or Layer 2 VPN • Edge EFPs associated with the EVC or Layer 2 VPN • EFD fragment names • EFD fragment type
	Network pseudowire	For the selected pseudowire, the report displays the network pseudowire name, type, business tag, and map name.
	VPLS	For the selected VPLS, the report displays the VPLS name, business tag, and map name.

1. Archived means that the event/ticket has been cleared, closed, and removed.

Customizing Reports

This section explains the customization options that are available for interactive reports. The major customization tasks that you can perform are:

- Customizing Data in Reports, page 5-3
- Grouping Data in Reports, page 5-3
- Adding a Filter, page 5-6
- Applying Quick Filters, page 5-7
- Formatting Interactive Reports, page 5-4

To customize a report, select the report in the left navigation pane or open the report, then click the **Edit** icon. The report opens in edit mode. Note that when you are creating a new report, the same customization options are available to you.

Note To be able to save a customized report, you must select the report and click Edit. While you can perform some customization by not being in edit mode, you will not be able to save the changes after you are done. After completing the customization, we recommend that you save the report using the Save As functionality. Saving the report as is changes the name of the report to a default file name (without the file name extension).

Figure 5-1 provides a snapshot view of customization options available.

Figure 5-1 Customizing Options

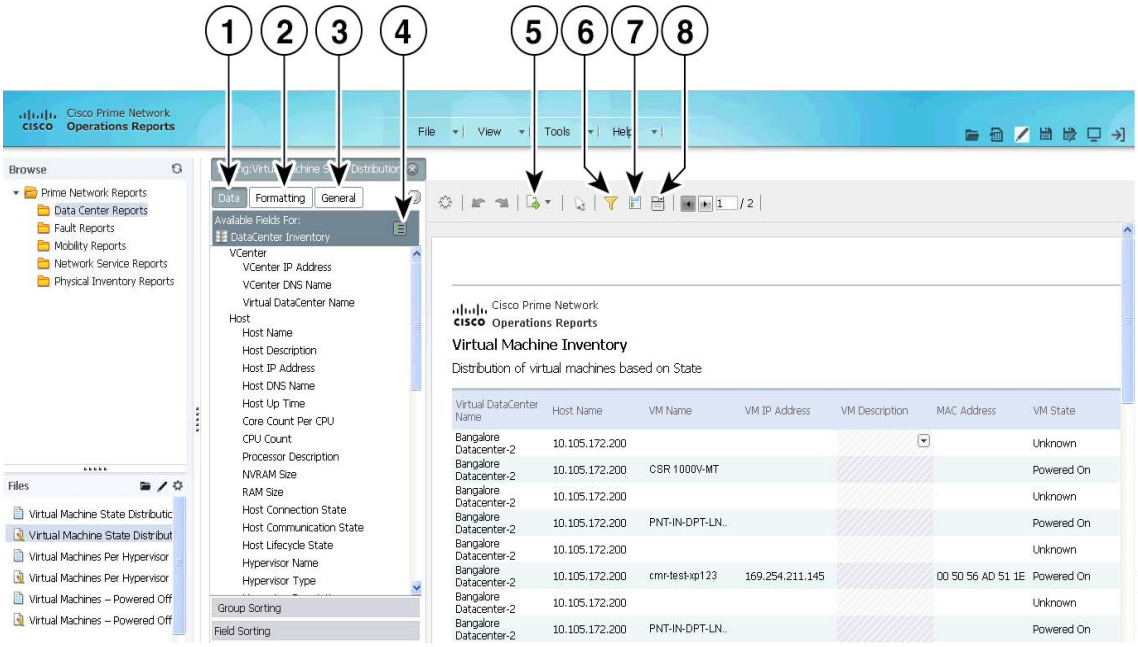


Table 5-1 Customizing Reports—Icons Description

	Item	Description
1	Data tab	Contains all the fields that can used in the report selected.
2	Formatting tab	Allows you to customize the report by applying formatting options such as font type, size, color, background color. For more information, see Changing the Font Style, page 5-5.
3	General tab	Allows you to change report template and orientation. For more information, see Changing the Report Template, page 5-5 and Changing the Size and the Orientation of a Reports, page 5-5.
4	Query Settings icon	Allows you enable options such as auto-refresh, maximum row in a report. For more information, see Additional Useful Customization Options, page 5-9.
5	Export icon	Allows you to export your report to be saved at an external location.
6	Filter icon	Allows you to create basic and advanced filters. For more information, see Adding a Filter, page 5-6.

Table 5-1 Customizing Reports—Icons Description (continued)

	Item	Description
7	Layout icon	Allows you to view the layout of the report. This is useful when you need to view and rearrange groups.
8	Prompts icon	Allows you to apply a quick, simple filter to the report. For more information, see Applying Quick Filters, page 5-7.

Customizing Data in Reports

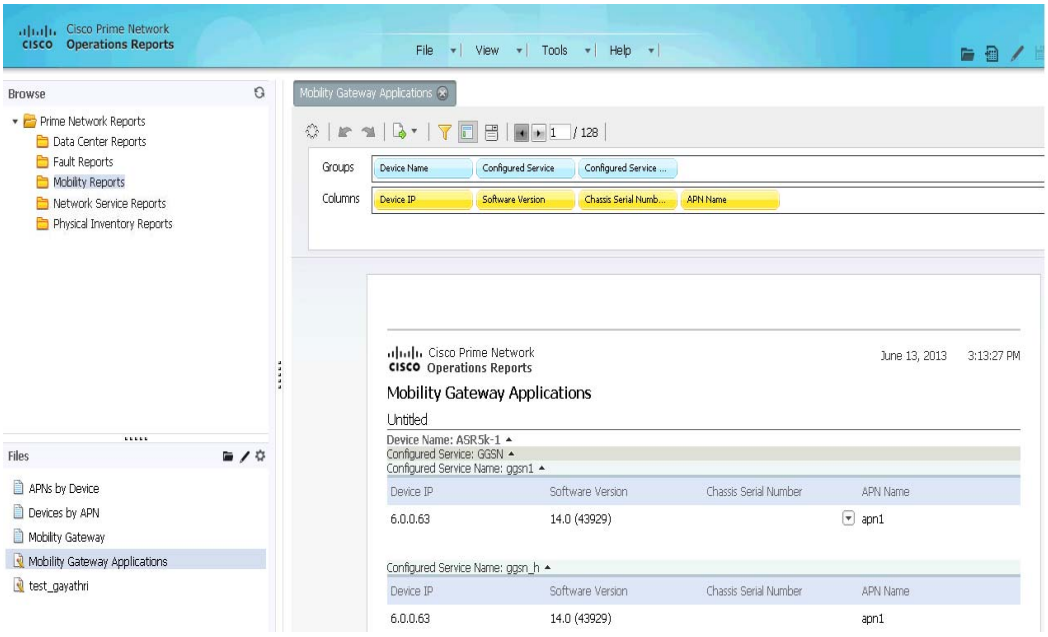
To customize a report, select the report in the left navigation pane or open the report. When you click the **Edit** icon, the data available in the corresponding data source of the report loads. You can customize the report data by dragging and dropping the required fields from the Data tab.

Grouping Data in Reports

You can group the data in your report by one or more fields. For example, you could group your data by device type, severity, or location. From the following example (Figure 5-2), the group names are placed in the following order: Device Name, Configured Service, and Configured Service Name.

The Device Name contains a groups of Configured Services, which in turn contain groups of entries for Configured Service Names. The list of devices is arranged in ascending order and each device data is reported serially.

Figure 5-2 Grouping Report Data—Example



Follow the procedure below:

Step 1 Click the **Layout** icon.

A field to add groups and the available columns in the report appear.

Step 2 Drag and drop the fields to the **Groups** field. The report immediately rearranges based on the grouping specified.

If you need to group the data in your report by more than one field, drag and drop the required fields. If more than one field is present, the groups are arranged in sets. The first field in the group is the super set of the second field.

Step 3 To delete the group name, click the name of the group from the **Groups** field, and drag and drop in the recycle bin that appears. When you delete a group, the related column is deleted also from the table.

Changing the Data Presentation in Reports

Reordering Columns

This section describes the procedure to adjust and reorder the columns in your report.

To reorder your column, select the column you want to move and drag it to your desired location. Alternatively, select the column you want to move, click the down-arrow and select **Move** (Right or Left) from the menu.

To adjust your column width, select the column, then click on the vertical line that divides your column headers. A small arrow appears. Move the arrow left or right to adjust your column width.

Sorting Data in Reports

Step 1 To sort the data available in your report, click the small down-arrow icon next to the column name.

Note If the down arrow is not available, you must enable the menu options from **General tab > Preferences > Enable Menu Buttons**.

Step 2 Click **Sort > Ascending/Descending**.

Formatting Interactive Reports

You can specify how your reports are formatted and presented. The following topics help you perform the task.

Changing the Report Template

Step 1 From the left navigation pane, choose **General** tab.

Step 2 Browse through the available templates using the left and right arrows. Select the template of your preference and confirm. The template Left Indented - Jade contains the product name, Cisco Prime Network Operations Reports, on the header.

Step 3 Click **Select**.

The Select dialog box with all the available options of templates appears. Choose the template. The template is applied to the report.

Changing the Size and the Orientation of a Reports

Step 1 From the left navigation pane, choose **General > Page Setup**.

The Page Setup dialog box appears.

Step 2 Choose the correct page format and orientation for your report from the list. The page margin measurements are available in the lower portion of the dialog box. You can adjust the measurements as needed. We recommend that you choose the landscape option if the number of fields in your report are many.

Step 3 Click **OK** to save the changes.

Changing the Font Style

After you generate a report, you can change the font, the color, and the font size of the report contents. You can later copy and paste the formatting from one column to another column within the same report. On an interactive report, from the left navigation pane, choose **Formatting**.

Step 1 On an interactive report, select the column for which you want the formatting to be applied. To select multiple columns, select the columns with the **Ctrl** key pressed.

Step 2 From the left navigation pane, select **Formatting**. Set the formatting specification for the table. The formatting is instantly applied.

To copy the format from one column to another:

Step 1 Select the column from which the format is to be copied.

Step 2 Click the **Copy** icon.

Step 3 Choose the column on to which the formatting has to be applied.

Step 4 Click the **Paste** icon.

The formatting is applied.

Filtering Interactive Reports

Some reports are very long, and may run into several pages. However, not all details represented in the report may interest you. You can filter the report to specifically view the information that you need.

Adding a Filter

After you generate a report, you can filter the contents of the report based on the columns present in the report. To create a filter:

Step 1 Click the **Filter** icon.

The filter pane opens.

Step 2 From the left navigation pane, from the **Data** tab, drag and drop the fields (that are already available in the report as columns) to the Apply Filter pane.

The **Filter on** *Field Name* appears.

Step 3 From the **Filter on** *Field Name,* specify the condition based on which the filter has to be applied. Enter a parameter name that describes the filter name.

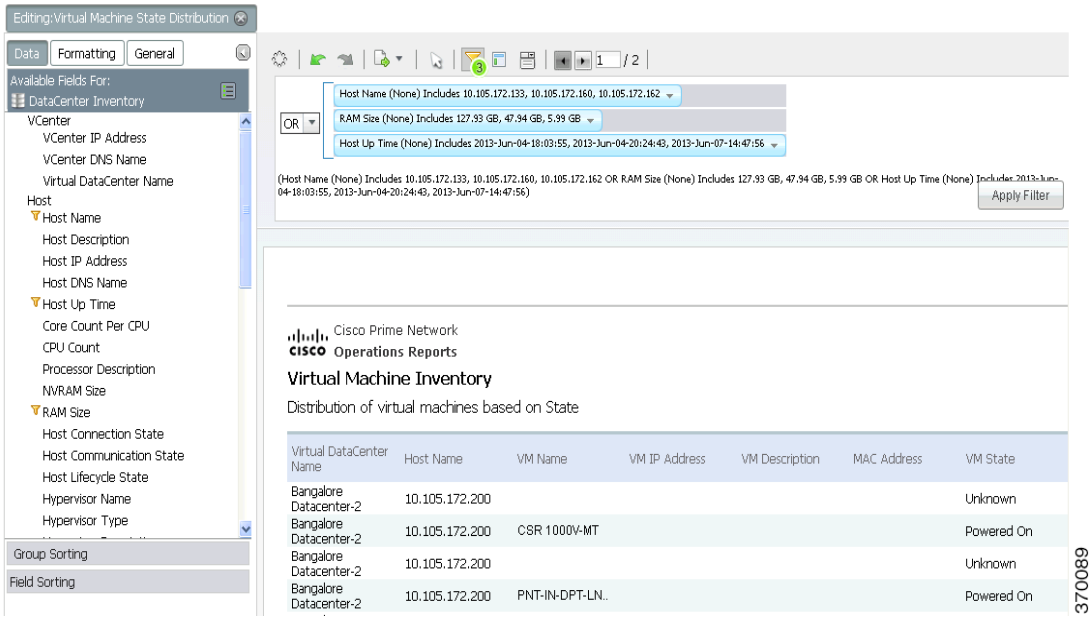
To narrow down the filter parameters, and to specify your exact requirement, choose the **Select from a List** option. For example, if you want to filter the report for a few types of devices, drag the Device Type field, and from the **Select from List** option, choose the types of devices to be included, and move them to the **Currently (Included)** pane. The filter is now applied only on the device types specified.

Step 4 Click **OK.**

Creating Advanced Filters

After you create filters using the steps explained in Adding a Filter, you can customize the filter to exclude and include data in the combination that you set. For example (Figure 5-3), from the Virtual Machine State Inventory report, you can set the filter to view report details of one of the following fields: Host Name (with specific name), RAM Size (that you can specify), Host Up Time (specify a period). You can also give an ‘AND’, ‘OR’ operator with a few more conditions that must be filtered with the above-mentioned conditions.

Figure 5-3 Filtering Reports—Example



Perform the following steps to customize the filter for advanced settings:

Step 1 Create a filter as outlined in the section Adding a Filter.

Step 2 From the fields that are listed in the filters pane, create advanced filters by creating a hierarchy. From the down arrow displayed on the filter parameter, choose the position of the parameter. Click **Move Up** or **Move Down**, as required.

Step 3 If you prefer a parameter to be an AND operator of another parameter, click the down arrow of the first parameter and choose **Indent**.

For example, if you want to view report details of Host Name of a specific RAM Size, move the Host Name up, and indent RAM Size. If you desire to view the details of a host with Host Name and Host Up time parameters, move Host Name up and indent Host Connection State.

Step 4 Repeat the procedure for the filters you have chosen.

Step 5 From the master AND, OR operator, choose as required.

For example, if you desire to filter based on both (Host DNS Name and RAM Size) and (Host Name and Host Connection State), choose the AND operator from the drop-down list on its right.

Applying Quick Filters

Prompts are quick filters that are used without adding specific restrictions. You can filter the data based on any data field available on the left navigation pane. However, you cannot specify 'And'/'Or' options.

To create a prompt, click the **Prompts** icon, and drag and drop the fields from the left navigation pane.

For example, if you set the prompt for VM Device State and Number of Devices, you can see the number of devices for a specific VM device state. Prompts are especially useful when you want to add a From and To date before you begin generating customizable prepackaged fault reports.

Note To add a prompt for a range of days (with From and To dates options), drag the Date field twice. This creates two options from which you can select the From and To date.

Upon adding prompts, the report is filtered to reflect the prompts, and a refreshed report appears. If you select the prompt for VM Device State (with the state Suspended selected), the devices whose VM device state is suspended appears.

The structure added in Prompts reflects in the Filter option as well.

Editing Prompts

You can edit the prompts that you have created for reports. Editing the prompts functionality allows you to choose the methods of selecting prompt options such as radio buttons, check box, or text box. You can also specify the first value that needs to be selected by default. To edit a prompt, follow the procedure below:

Step 1 Select a Prompts. From the data tab, choose the required parameters and drag and drop to the Prompts field.

Step 2 After the data field is added, mouse over on the prompt. A pencil icon appears. Click the pencil icon.

The **Prompt for** *data field* window appears.

Step 3 Enter a name for the prompt.

Step 4 Choose a **Type of Control;** this decides the modality of selection of items in the prompts.

If you choose the control type List, you can specify the number of values that are displayed when you begin choosing the items listed in the Prompts field.

Step 5 Choose a **Data Type**. The following options are available:

- Metadata List—Select this data to enable the prompts feature to work against a database. If you choose Metadata List, select the Data Source that the report runs against.
- Static List—This option is not supported in Prime Network 4.2.2 Operations Reports.

Step 6 From the Control Properties pane, choose the options as required:

- Initially Selected—This allows you to specify the value that is selected from the list by default
  - Use First Value—By default, selects the first value from the available list
  - Specify—Specify the value that should be selected by default when you click Prompt.

Step 7 Click **OK**.

Applying a Summary Function

You can view a summary of the report generated for numerical values from the column, group or the entire report. The summary feature can be applied to columns to view the sum of values listed; for example, the total number of modules. You can also count the number of rows present in the report by using the Count option.

From the column that contains numerical values, perform the following:

Step 1 Right-click the column and choose **Summary**

Step 2 Choose an option based on the options in the table below:

Table 5-2 Summary Functions Description

Function Name	Description
None	No summary function assigned.
Average	Calculates the average of the selected column.
Count	Counts the items in a group or report, but does not require a numeric value.
Max	Identifies the highest or largest value in a column.
Min	Identifies the lowest or smallest value in a column.
Sum	Calculates a total sum of the group or report (group level, and running total in the report footer).

Additional Useful Customization Options

- Setting a row limit—You can limit the number of rows that are displayed in your report. From the **Data** tab, click the **Query Settings** icon. Check **Row Limit** option, and specify the number of rows. This feature is especially useful to avoid out of memory errors or processes that consume too many resources on the database server.

  Note The row limit that you set is applicable only for the current session. You must set the row limit for a report each time when you open that report in a session.

- Including duplicate entries—By default, reports filter out duplicate entries for clones or items with same entries such name, description. If you have several items such as chassis or devices with the same description or name, only one entry is displayed. In such a case, you run the risk of missing critical data. To view all entries, click the **Query Settings** icon, and then uncheck **Select Distinct.**
- Setting a timeout—You can specify number of seconds for which a query (to generate a report) runs before a timeout occurs. This feature is especially useful to avoid out of memory errors or processes that consume too many resources on the database server. From the **Data** tab, click the **Query Settings** icon. Check **Query Timeout** and enter the period in seconds.

- Eliminating duplicate entries—From the Data tab, click the **Query Settings** icon to prevent the report from displaying duplicate values in columns. Enabling this option will list the different (distinct) values in a table, exclusively.
- Changing the column name—Double-click the column name and in the pop-up dialog box, enter the new column name and press **Enter.**
- Exporting a report—Click the **Export** icon and select your export file type: PDF, Excel, CSV or HTML. Exported files can be saved locally on your computer.
- To enable menu buttons and show tips—The menu options to sort data, move columns, create a summary are available in individual columns of the generated report. To be able to view the options, from **General tab > Preferences**, click **Enable Menu Buttons**. To be able to view tips, from **General tab > Preferences**, click **Show tips** or **Show tips on startup**.
- Including date and page numbers in the report—Double-click the Cisco Prime Network text that appears next to the Cisco logo at the top of the report, and in the pop-up dialog box, click **Date** and **#/Pages**.

Scheduling Reports

Using Operations Reports, you can schedule reports to be generated at a later time or to recur periodically. You can also have the report sent to a configured e-mail address upon generation. The scheduled reports can be viewed in a preferred format such as HTML, PDF, CSV, or Excel. The reports that are scheduled are available from the My Workspace view. This view contains the schedules, the generated reports, and the status of schedules.

This section contains the following topics:

- Scheduling a Report, page 6-1
- Deleting Schedules, page 6-5
- Viewing the Status of Generated and Scheduled Reports, page 6-6

Scheduling a Report

Using the Schedule option, you can configure Operations Reports to generate periodic reports without your intervention. Based on the inputs you specify, Operations Reports generates reports at the specified date and time. By default, the intervals available in Operations Reports are: run once, run every *X* seconds, minutes, hours, daily, weekly, monthly, and yearly. For example, you can set the report to be run the first Sunday of every month for a specified period. Before you schedule a new report, you must create and save the report; you cannot create a schedule as you create a new report. The scheduling procedure is different for interactive (customizable) reports and read-only reports. This section contains the following topics:

- Scheduling a Read-Only Prepackaged Report, page 6-1
- Scheduling a Customizable Prepackaged Report, page 6-2
- Creating a Custom Schedule Interval, page 6-3

Scheduling a Read-Only Prepackaged Report

Only admin-level users can schedule a read-only prepackaged report. If you are a non-admin user, you cannot create schedules for read-only prepackaged reports. You can only subscribe to schedules that the administrator has already created.

Step 1 From the left navigation pane, double-click a report and then in the **Parameters** pane, click **Schedule Report.**

The New Schedule window opens.

Step 2 From the New Schedule window, specify the schedule settings:

- Name—Enter a name for your schedule. This is the name that appears to non-admin users at the time of subscription.
- To (E-mail)—The e-mail address to which the report must be sent after generation. As a prerequisite, you must configure an e-mail server for Operations Reports to send the reports to. For more information, see Enabling Reports to be Sent by E-mail, page 2-4.

Tip We recommend that you set the output type to one of the following output types: PDF, CSV, or Excel. If you choose the HTML option, a link to the HTML report is sent to your mailbox. To be able to open and view the report, you must have an active session of Operations Reports open.

- Subscription—(Applicable only to non-admin users) From the **Subscription** drop-down list, select an appropriate schedule. The Subscription drop-down list displays the schedules that the administrator has created for the specific report you have selected. Skip to Step 4.

Step 3 From the **Recurrence** drop-down list, choose a recurrence option and set the options for the relevant fields that appear upon selection. If you wish to customize the recurrence interval, choose **Cron.** For more information on configuring a Cron setting, see Creating a Custom Schedule Interval, page 6-3

Step 4 Click **OK**.

Note If you selected the output type as HTML (Paginated), only the first page that appears if you clicked View Report is scheduled. For example, if you clicked View Report, and details of 10 devices appear in the first page of the report, upon scheduling, details of only those 10 devices appear. To be able to view the full report, we recommend that you choose the output type as HTML.

Scheduling a Customizable Prepackaged Report

Schedules for customizable prepackaged reports are private and cannot be shared for other users to subscribe to. You cannot have customizable prepackaged reports sent to a configured e-mail address.

Step 1 From the left navigation pane, right-click a report, and choose **Schedule**.

The New Schedule window opens.

Step 2 From the New Schedule window, specify the schedule settings:

- Name—Enter a name for your schedule.
- Group—Enter the type of report such as Data Center Report or Fault Report. The name of the group reflects in the file system. If a group name already exists, the report is placed in the existing folder. Otherwise, a new folder is created in the file system.
- Description—Enter an appropriate description.

Step 3 From the **Recurrence** drop-down list, choose a recurrence option and set the options for the relevant fields that appear upon selection. If you wish to customize the recurrence interval, choose **Cron.** For more information on configuring a Cron setting, see Creating a Custom Schedule Interval, page 6-3

Note The time you select here is the time displayed on the client. Upon scheduling a report, the job is listed in the Workspace. The time displayed in the Workspace is the corresponding gateway time of the report.

Step 4 Click **OK.**

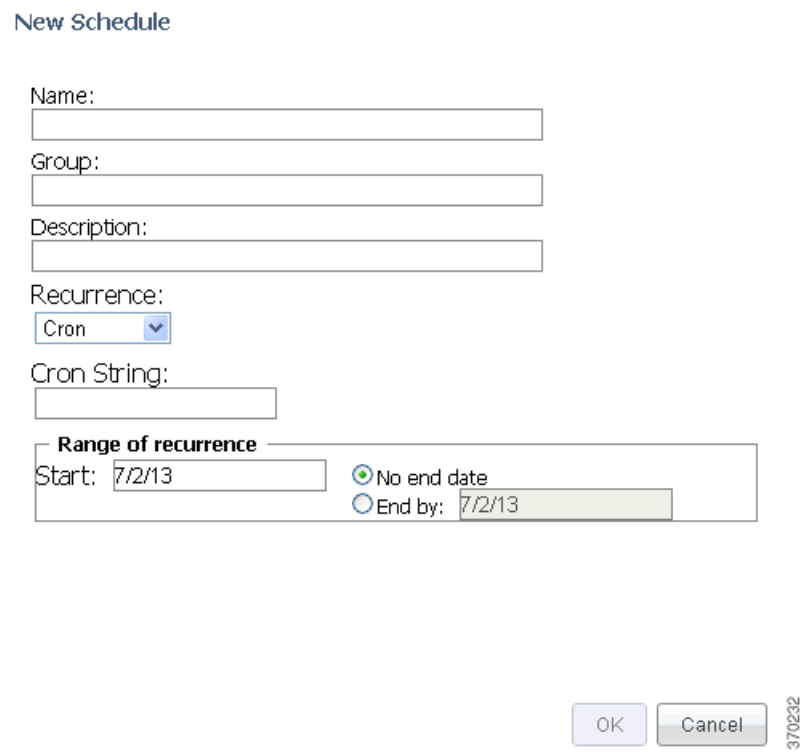
Creating a Custom Schedule Interval

By default, the intervals available in Operations Reports are: run once, run every *X* seconds, minutes, hours, daily, weekly, monthly, and yearly. However, if you require the report schedule to be more specific, such as the every two hours only on the last Thursday of every month, you can create a Cron schedule, which is a custom schedule interval.

Step 1 The procedure to create a schedule depends on the type of report. To begin creating a schedule, see Scheduling a Report, page 6-1.

Step 2 (From the New Schedule dialog box) At the time of creating a recurrence for the schedule, choose **Cron.**

Figure 6-1 Creating a Cron Recurrence



Step 3 In the Cron String field, enter a cron string.

The format is the same for every cron string. The value must be listed in the order: *seconds minutes hours day of month month day of week year.* A space separates each attribute.

The permitted values for attributes are:

Table 6-1 Cron Recurrence—Values Permitted

Time Value	Attributes
Seconds and minutes	0 to 59
Hours	0 to 23
Days	1 to 31; alternatively you can use three-letter values for the day of week (MON, TUE, WED, THU, FRI, SAT, SUN
Months	1 to 12; alternatively, you can use a three-letter values for the month (JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC)
Week	1 to 7
Year	Four-digit year

For example, if you prefer to set a schedule that recurs every two hours between 10:00 AM and 08:00 PM, every day from July 27, 2013 to August 5, 2013, you must set the following cron string:

```
0 0 10-20*/2 27-7 6-8 ? 2013
```

Where,

- 0—Indicates 0 second
- 0—Indicates 0 minute
- 10-20—Indicates 10:00 AM to 8:00 PM
- */2—Indicates every two hours; wherein, * denotes ‘every’, and /2 denotes that the period is split every 2 hours. '
- 27-7—Indicates July 27
- 6-8—Indicates August 6; the date on which the schedule ends
- ?—Indicates that the day of week is skipped
- 2013—Indicates year

Step 4 Click **OK**.

A cron recurrence is scheduled.

Important notes to consider before setting a cron recurrence:

- An asterisk (*) indicates all values, so an asterisk in the minute field would mean that the report runs once every minute.
- You can specify a range of values with the - (dash) operator, and you can specify multiple individual values with a comma.
- If you need to skip a value in the day of month and day of week field from a cron job, you can use the question mark (?) character. This indicates that this value has been skipped.
- If you need to split values, introduce the slash (/) character. This means "every," —so */15 would mean "Every 15."

- In the day of month field, you can use the # character to indicate a certain instance of a day of the month, for instance the second Friday of the month would be 6#2.
- You can use an uppercase L in the day of month and day of week field to indicate "Last," as in the last day of the week. An uppercase C in either of these fields means "Calendar," and combined with a number means that the report should execute a the interval indicated by the C number according to the loaded calendar. A uppercase W in the day of month attribute means "Weekday," which only encompasses Monday through Friday.

Table 6-2 represents the values that are admissible for each value.

Table 6-2 Customizing Intervals—Attribute Conditionals

Attribute	Conditionals and Operators
Seconds	, - * /
Minutes	, - * /
Hours	, - * /
Day of the Month	, - * ? / L W C
Month	, - * /
Day of the Week	, - *? / L C #
Year	, - * /

Deleting Schedules

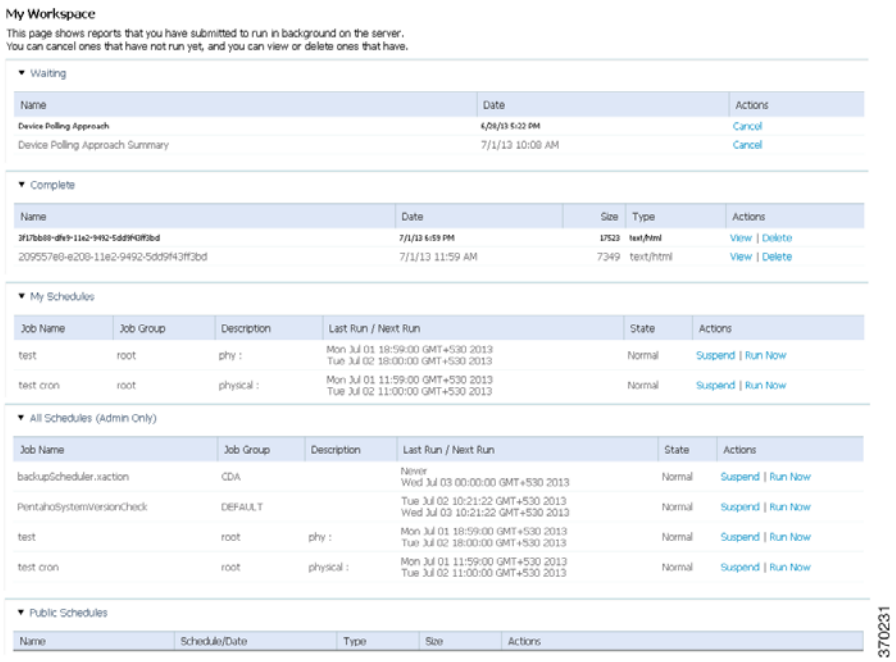
You can delete a schedule that you created if your administrative privileges permit this. We recommend that you first suspend the schedule and then delete it from your workspace. You can restart the schedule after the delete process completes.

- To delete a schedule of a read-only report—From **Public Schedules**, click the **Delete** button next to the name of the schedule. The schedule is deleted.
- To delete a schedule of a customizable prepackaged report or a new report—From the **Complete** folder, click the top-level Delete button next to the schedule. Clicking the **Delete** button available next to the report deletes only the report.

Viewing the Status of Generated and Scheduled Reports

You can view the reports that you generated and the status of the reports you scheduled from **View > Workspace.** My Workspace is a graphical overview of the reports you have created and scheduled. The name of a report displayed in the workspace is the name you enter while scheduling a report.

Figure 6-2 My Workspace View



When you schedule a report, the report is located in one of the panes in the Workspace view. The location of the report in one of the panes is based on the type of report (read-only prepackaged report, customizable prepackaged report, or new report) and the status of its schedule.

Read-Only Prepackaged Report

If you scheduled a read-only prepackaged report:

- Upon scheduling—Appears in the All Schedules pane; appears in Public Schedule with options such as Run Now, Run and Archive, Edit, and Delete activated.
- After completion—Generated report is stored in the server directory. To view the report, from the folder in which you have installed Operations Reports, navigate to the following folder: /server/biserver-ee/pentaho-solutions/system/content/prime-network-report. If you are a non-admin user, you cannot access the server directory. In that case, we recommend you get the report sent as an e-mail attachment.

Customizable Prepackaged Reports and New Reports

- Upon Scheduling—Appears in the All Schedules pane. Also appears in the Waiting pane with the schedule details listed with an option to cancel the report before it is run.
- After completion—Appears in Complete pane with options to view and delete the report.

Workspace Panes

- All Schedules—This pane is viewable only by admin users. This is a list of all reports that are scheduled for your user account. This also contains a log of the schedules that were executed in the past. This lists customizable prepackaged reports, read-only prepackaged report, and new reports that are scheduled. This contains only the schedule details and not the reports. You can initiate a report to be run immediately by clicking **Run Now.**
- Public Schedules—This lists the schedules of only the read-only prepackaged reports. If you are an admin user, this lists all of the read-only prepackaged report schedules you created for the other non-admin users to subscribe to. As a non-admin user, this lists all the read-only prepackaged schedules that you have subscribed to; you (non-admin user) cannot create a new schedule or edit existing schedules for read-only prepackaged report. Run, run and archive, delete, edit.
- Waiting—This category lists all schedules of interactive reports that you have created to run in the future. Clicking **Cancel** will delete the schedule. This section also lists the schedules that are repetitive.
- Complete—This lists the new reports and the customizable prepackaged reports that were generated using a schedule job. Every time the schedule executes, it overwrites the report's previous entry in the Complete list. The names of the reports are specified as an alphanumeric string; click **View** to know the report details.
- My Schedules—This category contains a list of schedules specific to your user account. This will be identical to your Waiting list unless you have suspended any of your schedules. This contains only customizable prepackaged reports and new reports. After completion, move to Complete. The entry will be deleted from my schedule.

You can suspend or run reports that you created or have access to. Click the appropriate button to perform an action.

Tasks that you can Perform from Workspace

From the Workspace, based on the pane in which the report resides, some of the following actions can be performed:

- View—Allows you to view a report. The format of the report is specified next to the name of the report.

Note If you specified the format CSV, the file indicates that it is an unknown file; however, if you open the file with a supported tool such as Microsoft Excel, the file opens as a CSV file.

- Run Now—Runs the report and creates and another entry for the name of the report with the state Running. This is available in My Scheduled pane.
- Run and Archive—This runs in the background and creates a copy in the server.
- Delete (from the Public Schedules pane)—The report is deleted before it runs. If you clicked Run and Archive, the background activity stops abruptly. However, reports that are already saved in the server will remain.
- Suspend—Suspends a report that is running. This job can later be resumed.

Predefined Data in Data Sources

Interactive reports rely on data sources for information. Data sources are models that allow you to connect to the database information to be presented in reports. Each model comprises a set of predefined data that can be viewed from an interactive report. This appendix lists the predefined data that is available for each data source.

This appendix contains the following sections:

- Data Center Reports, page A-2
- Fault Reports, page A-4
- Mobility Application Reports, page A-9
- Network Service Report, page A-17
- Physical Inventory Reports, page A-18

Data Center Reports

Table A-1 Data Center Report—Data Sources

Report Name	Available Fields
Data Center Inventory	vCenter: • VCenter IP Address • VCenter DNS Name • VCenter Name Host • Host Name • Host Description • Host IP Address • Host DNS Name • Host Up Time • Core Count per CPU • Processor Description • NVRAM Size • RAM Size • Host Connection State • Host Communication State • Host Lifecycle State • Hypervisor Name • Hypervisor Type • Hypervisor Description • Hypervisor State • Hypervisor Software Type • Hypervisor Start Time • Hypervisor Version • VM Count

Table A-1 Data Center Report—Data Sources (continued)

Report Name	Available Fields
	Host Statistics • Host CPU Usage • Host Disk Usage • Host Memory Usage • Host Active Guest Memory Usage • VM Lifecycle State Virtual Machine • VM Name • VM IP Address • VM Version • VM State • VM Description • VM DNS Name • UuID • Virtual CPU • VM Up Time • Fault Tolerance Enabled • MAC Address • VM Lifecycle State • VM Communication State Virtual Machine Statistics • VM CPU Usage • VM Disk Usage • VM Memory Usage • VM Active Guest Memory Usage

Fault Reports

Table A-2 Fault Reports —Data Sources

Report Name	Available Fields
Active Events	Network Events: • Alarm OID • Causing Event ID • Date • Date and Time • Device • Detailed Description • Detection Type • Duplication Count • Event ID • Element Type • Event Count • Event Type • First Occurrence • Last Occurrence • Location • Reduction Count • Severity • Ticket ID

Table A-2 Fault Reports —Data Sources (continued)

Report Name	Available Fields
Active Tickets	Ticket: • Acknowledged • Alarm Count • Average # Correlated Events • Affected Devices Count • Date and Time • Device • Description • Duplication Count • Event Count • Element Type • Highest # Correlated Events • Last Modification Time • Location • Lowest # Correlated Events • Reduction Count • Root Event Time • Severity • Tickets Count • Ticket ID
Archive Events	Network Events: • Detection Type • Date • Date and Time • Device • Event ID • Event Type • Event Count • Element Type • First Occurrence • Last Occurrence • Severity • Ticket ID

Table A-2 Fault Reports —Data Sources (continued)

Report Name	Available Fields
Archive Tickets	Ticket: • Acknowledged • Alarm Count • Average # Correlated Events • Affected Devices Count • Date and Time • Device • Description • Duplication Count • Event Count • Element Type • Highest # Correlated Events • Location • Last Modification Time • Lowest # Correlated Events • Reduction Count • Root Event Time • Severity • Tickets Count • Ticket ID

Table A-2 Fault Reports —Data Sources (continued)

Report Name	Available Fields
Archive Events Detailed	Network Events: • Alarm OID • Causing Event ID • Date • Date and Time • Device • Detailed Description • Detection Type • Duplication Count • Event ID • Event Type • Element Type • Event Count • Location • Reduction Count • Severity • Ticket ID
Audit Events	• Severity • Event Count • Timestamp • Description • Username • Originating IP address • Command details: name, parameters, signature
Provisioning Events	• Severity • Event Count • Timestamp • Description • Username • Status

Table A-2 Fault Reports —Data Sources (continued)

Report Name	Available Fields
Security Events	• Severity • Event Count • Event ID • Date Time • Description • Location • Username • Originating IP address
System Events	• Severity • Event Count • Event ID • Time • Description • Location,
Standard Events	Standard Events: • Causing Event ID • Date • Date and Time • Detailed Description • Detection Date • Detection Type • Device • Duplication Count • Element Type • Event Count • Event ID • Event Type • Location • Reduction Count • Severity

Mobility Application Reports

Table A-3 Mobility Application Reports —Data Sources

Report Name	Available Fields
Code Division Multiple Access (CDMA)	Device: • Device Name • Device IP • Device Type • Context Name CDMA: • Packet Data Serving Node (PDSN) Service Name • Foreign Agent (FA) Service Name • Home Agent (HA) Service Name Access Point Name (APN): • APN Name • Accounting Mode • Selection Mode • Allocation Type • Active Charging Rule Base • IP Header Compression • L3 to L2 Address Policy • APN Business Tag • APN New Call Policy

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
CDMA-SAE	Device: • Device Name • Device IP • Device Type • Context Name CDMA SAE: • PDSN Name • SGW Name • FA Name • EPDG Name • MME Name • HA Name • PGW Name APN: • APN Name • Accounting Mode • Selection Mode • Allocation Type • IP Header Compression • L3 to L2 Address Policy • APN New Call Policy • Active Charging Rule Base • APN Business Tag

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
LTE	Device: • Device Name • Device IP • Device Type • Context Name System Architecture Evolution Gateway (SAEGW) • SAEGWService Name • SAEGW Business Tag • SAEGW Status Serving Gateway (SGW) • SGW Service Name • SGW Status • SGW Mag Service • IMA Authorization Service • Egress Context Name • SGW New Call Policy APN: • APN Name • Accounting Mode • Selection Mode • Allocation Type • Active Charging Rule Base • IP Header Compression • L3 to L2 Address Policy • APN Business Tag • APN New Call Policy

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
Mobility Applications	Device: • Device Name • Device IP • Device Type • Device Software Version • Context Name Chassis • Chassis Serial Number • Shelf Serial Number Mobility Applications • Configured Service • Configured Service Name APN: • APN Name • Accounting Mode • Selection Mode • Allocation Type • Active Charging Rule Base • IP Header Compression • L3 to L2 Address Policy • APN Business Tag • APN New Call Policy APN Charging Characteristics • Home Bit Behavior • Home Profile • Visiting Bit Behavior • Visiting Profile • Roaming Bit Behavior • Roaming Profile • All Bit Behavior • All Profile • Use RADIUS Returned • Use GGSN APN QoS Down Link • Down Link QCI Name

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
	• Down Link Negotiate Limit • Down Link Peak Data Rate • Down Link Committed Data Rate • Down Link Rate Limit • Down Link Burst Size Auto Readjust • Down Link Burst Size Auto Readjust Duration • Down Link Peak Burst Size • Down Link Guaranteed Burst Size • Down Link Exceed Action • Down Link Violate Action APN QoS Up Link • Up Link QCI Name • Up Link Negotiate Limit • Up Link Peak Data Rate • Up Link Committed Data Rate • Up Link Rate Limit • Up Link Burst Size Auto Readjust • Up Link Burst Size Auto Readjust Duration • Up Link Peak Burst Size • Up Link Guaranteed Burst Size • Up Link Exceed Action • Up Link Violate Action

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
SGSN with IuPS and	Device • Device Name • Device IP • Context Name Serving GPRS Support Node (SGSN) • SGSN Name IuPS • IuPS Name • IuPS Status • IuPS Business Tag • IuPS PLMN ID Radio Network Controller (RNC) • RNC ID • RNC Status • RNC PLMN ID Routing Area Code (RAC) Location Area Code (LAC) • LAC • RACs

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
UMTS	Device: • Device Name • Device IP • Device Type • Device Software Version • Context Name Gateway GPRS Support Node (GGSN) • GGSN Service Name • GGSN Status • Local IP Address • GTPU Service Name • Accounting Server Timeout • Authentication Server Timeout • PLMN Policy • GGSN New Call Policy Serving GPRS Support Node (SGSN) • SGSN Service Name APN: • APN Name • Accounting Mode • Selection Mode • Allocation Type • Active Charging Rule Base • IP Header Compression • L3 to L2 Address Policy • APN Business Tag • APN New Call Policy

Table A-3 Mobility Application Reports —Data Sources (continued)

Report Name	Available Fields
EPC	EPC • Device Name • Device IP • Device Type • Context Name System Architecture Evolution Gateway (SAEGW) • SAEGWService Name • SAEGW Business Tag • SAEGW Status Serving Gateway (SGW) • SGW Service Name • SGW Status • SGW Mag Service • IMA Authorization Service • Egress Context Name • Accounting Policy • Accounting GTTP Group • SGW Accounting Mode • Egress Protocol • SGW New Call Policy Packet Data Network Gateway (PGW) • PGW Service Name • PGW Status • QCI QoS Mapping Table Name • GGSN Service Name • LMA Service Name • EGTP Service Name • Session Delete Delay Timeout • PGW New Call Policy Gateway GPRS Support Node (GGSN) • GGSN Service Name • GGSN Status • Local IP Address • GTPU Service Name • Accounting Server Timeout

Network Service Report

Table A-4 Network Service Report—Data Sources

Report Name	Description
Virtual Connection	Virtual Connection • Virtual Connection Name • Virtual Connection Business Tag • EVC Name • EVC Business Tag • Map Names • EVC Terminating EFPs • Flow Domain Fragments • Fragment Type
Network Pseudowire	Pseudowire • Network Pseudowire Name • Network Pseudowire Type • Network Pseudowire Business Tag • Map Name • Detail Name • Detail Type
VPLS	VPLS • VPLS Name • VPLS Business Tag • Map Names • Detail Name • Detail Type

Physical Inventory Reports

Table A-5 Physical Inventory Reports —Data Sources

Report Name	Available Fields
Device	Device: • Device Name • Device IP • Device Up Since • Device Scheme • Device Type • Device Series • Device Vendor • Device Business Tag • Location • Device Package Name • Product Type • Polling Group • Polling Approach • Sending Alarms • Serial Number • Software Version • System Name • Image File • Number of Modules • Number of Chassis • Number of Ports • Number of Devices

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
	Management State: • Communication State • Communication State Policy • Investigation State • Investigation Description • Investigation State Since • Maintenance Status SNMP Connectivity: • SNMP State • SNMP Enabled • SNMP Protocol • SNMP State Description • SNMP State Since Telnet Connectivity • Telnet State • Telnet Enabled • Telnet Protocol • Telnet State Since XML Details • XML State • XML State Description • XML State Since HTTP Connectivity • HTTP State • HTTP Description • HTTP State Since

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
	• Authentication Server Timeout • PLMN Policy • GGSN New Call Policy Serving GPRS Support Node • SGSN Service Name Mobility Management Entity (MME) • MME Service Name Evolved Packet Data Gateway (EPDG) • EPDG Service Name • APN • APN Name • Selection Mode • Allocation Type • Active Charging Rule Base • L3 to L2 Address Policy • IP Header Compression • APN Business Tag • APN Accounting Mode • APN New Call Policy

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
Hardware Inventory	Device: • Device Name • Device IP • Device Series • Device Type • Device Business Tag Chassis • Chassis Name • Chassis Business Tag • Chassis Description • Chassis Serial Number • Shelf Business Tag • Shelf Description • Shelf Serial Number • Shelf Status Module • Module Name • Module Description • Module Status • Module Serial Number • Module Type • Module Hardware Version • Module Business Tag Sub Module • Sub Module Name • Sub Module Description • Sub Module Status • Sub Module Serial Number • Equipment Type[1] • Sub Module Type • Sub Module Hardware Version • Sub Module Business Tag

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
	Port • Port Alias • Port Status • Port Operation Status • Port Admin Status • Port Type • Port Location • Port Connector Description • Port Connector Type • Port Connector Serial Number • Port Pluggable Type • Associated Pluggable[1] • Pluggable Port State • Port Managed • Port Sending Alarms • Port Business Tag • Port PID Sub Module Port • Sub Module Port Alias • Sub Module Port Status • Sub Module Port Operation Status • Sub Module Port Admin Status • Sub Module Port Type • Sub Module Port Location • Sub Module Port Connector Description • Sub Module Port Connector Type • Sub Module Port Connector Serial Number • Sub Module Port Pluggable Type • Sub Module Pluggable Port State • Sub Module Port Managed • Sub Module Port Sending Alarms • Sub Module Port Business Tag • Sub Module Port PID

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
Module	Device: • Device Name • Device IP • Device Series • Device Type • Device Business Tag • Number of Modules Chassis: • Chassis Name • Chassis Business Tag • Chassis Description • Chassis Serial Number • Shelf Business Tag • Shelf Description • Shelf Serial Number • Shelf Status Module: • Module Name • Module Description • Module Serial Number • Module Status • Module Type • Module Software Version • Module Hardware Version • Module Business Tag • Number of Ports Sub Module • Sub Module Name • Sub Module Description • Sub Module Serial Number • Sub Module Status • Equipment Type[1] • Sub Module Type

Table A-5 Physical Inventory Reports —Data Sources (continued)

Report Name	Available Fields
	• Sub Module Software Version • Sub Module Hardware Version • Sub Module Business Tag • Number of Sub Module Ports

1. These fields will have a valid values only for Cisco Linkwood devices.