

SteelCentral™ NetProfiler and NetExpress User's Guide

Version 10.9.x

January 2017

The logo for Riverbed, featuring the word "riverbed" in a bold, orange, lowercase sans-serif font. A small registered trademark symbol (®) is located at the top right of the letter "d".

© 2017 Riverbed Technology, Inc. All rights reserved.

Riverbed®, SteelApp™, SteelCentral™, SteelFusion™, SteelHead™, SteelScript™, SteelStore™, Steelhead®, Cloud Steelhead®, Virtual Steelhead®, Granite™, Interceptor®, Stingray™, Whitewater®, WWOS™, RiOS®, Think Fast®, AirPcap®, BlockStream™, FlyScript™, SkipWare®, TrafficScript®, TurboCap®, WinPcap®, Mazu®, OPNET®, and Cascade® are all trademarks or registered trademarks of Riverbed Technology, Inc. (Riverbed) in the United States and other countries. Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed or their respective owners.

F5, the F5 logo, iControl, iRules and BIG-IP are registered trademarks or trademarks of F5 Networks, Inc. in the U.S. and certain other countries. Linux is a trademark of Linus Torvalds in the United States and in other countries. VMware, ESX, ESXi are trademarks or registered trademarks of VMware, Incorporated in the United States and in other countries.

Portions of SteelCentral™ products contain copyrighted information of third parties. Title thereto is retained, and all rights therein are reserved, by the respective copyright owner. PostgreSQL is (1) Copyright © 1996-2009 The PostgreSQL Development Group, and (2) Copyright © 1994-1996 the Regents of the University of California; PHP is Copyright © 1999-2009 The PHP Group; gnuplot is Copyright © 1986-1993, 1998, 2004 Thomas Williams, Colin Kelley; ChartDirector is Copyright © 2007 Advanced Software Engineering; Net-SNMP is (1) Copyright © 1989, 1991, 1992 Carnegie Mellon University, Derivative Work 1996, 1998-2000 Copyright © 1996, 1998-2000 The Regents of The University of California, (2) Copyright © 2001-2003 Network Associates Technology, Inc., (3) Copyright © 2001-2003 Cambridge Broadband Ltd., (4) Copyright © 2003 Sun Microsystems, Inc., (5) Copyright © 2003-2008 Sparta, Inc. and (6) Copyright © 2004 Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, (7) Copyright © Fabasoft R&D Software; Apache is Copyright © 1999-2005 by The Apache Software Foundation; Tom Sawyer Layout is Copyright © 1992 - 2007 Tom Sawyer Software; Click is (1) Copyright © 1999-2007 Massachusetts Institute of Technology, (2) Copyright © 2000-2007 Riverbed Technology, Inc., (3) Copyright © 2001-2007 International Computer Science Institute, and (4) Copyright © 2004-2007 Regents of the University of California; OpenSSL is (1) Copyright © 1998-2005 The OpenSSL Project and (2) Copyright © 1995-1998 Eric Young (eay@cryptsoft.com); Netdisco is (1) Copyright © 2003, 2004 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; SNMP::Info is (1) Copyright © 2003-2008 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; mm is (1) Copyright © 1999-2006 Ralf S. Engelschall and (2) Copyright © 1999-2006 The OSSP Project; ares is Copyright © 1998 Massachusetts Institute of Technology; libpq++ is (1) Copyright © 1996-2004 The PostgreSQL Global Development Group, and (2) Copyright © 1994 the Regents of the University of California; Yahoo is Copyright © 2006 Yahoo! Inc.; pd4ml is Copyright © 2004-2008 zefer.org; Rapid7 is Copyright © 2001-2008 Rapid7 LLC; CmdTool2 is Copyright © 2008 Intel Corporation; QLogic is Copyright © 2003-2006 QLogic Corporation; Tarari is Copyright © 2008 LSI Corporation; Crypt_CHAP is Copyright © 2002-2003, Michael Bretterkieber; Auth_SASL is Copyright © 2002-2003 Richard Heyes; Net_SMTP is Copyright © 1997-2003 The PHP Group; XML_RPC is (1) Copyright © 1999-2001 Edd Dumbill, (2) Copyright © 2001-2006 The PHP Group; Crypt_HMAC is Copyright © 1997-2005 The PHP Group; Net_Socket is Copyright © 1997-2003 The PHP Group; PEAR::Mail is Copyright © 1997-2003 The PHP Group; libradius is Copyright © 1998 Juniper Networks. This software is based in part on the work of the Independent JPEG Group the work of the FreeType team.

This documentation is furnished "AS IS" and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as "commercial computer software documentation" and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

Individual license agreements can be viewed at the following location: https://<appliance_name>/license.php

This manual is for informational purposes only. Addresses shown in screen captures were generated by simulation software and are for illustrative purposes only. They are not intended to represent any real traffic or any registered IP or MAC addresses.



Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: <http://www.riverbed.com>

Part Number
712-00060-21

Contents

Introduction.....	1
About This Guide	1
Types of Users	1
Organization of This Guide	2
Document Conventions	2
Product Dependencies and Compatibility	3
Hardware and Software Dependencies.....	3
Ethernet Network Compatibility	3
SNMP-Based Management Compatibility	4
Contacting Riverbed	4
Internet.....	4
Riverbed Support.....	4
Professional Services.....	4
Documentation	4
 Chapter 1 - Overview.....	 5
Overview of NetProfiler and NetExpress appliances	5
Information sources	6
NetFlow, sFlow, and IPFIX sources	7
Behavior analysis.....	8
Alerting and notification.....	9
Alerting.....	9
Notification.....	10
Security profiles.....	10
Host groups.....	10
Interface groups	11
Application tracking	12
Traffic reporting.....	12
Shortcuts page	12
Traffic Report pages	13

Quick report box	13
Left-clicking	13
Right-clicking	13
User interface.....	14
Home pages	14
Other GUI pages.....	19
Getting help	21
Chapter 2 - Configuration	23
Accessing the user interface	24
User interface preferences	24
Data section	24
Autocomplete section	25
Date and Time Formatting section	26
Miscellaneous section.....	26
Selecting preferred interfaces	26
Account management	27
User accounts.....	27
Remote authentication and authorization	31
ODBC DB Access	37
Passwords	37
Integration.....	37
Mitigation	37
Flow log	38
Flow log disk space allocation	38
Flow log disk space balancing.....	39
Reporting time frames	39
Packet capture (NetExpress only).....	40
Adding a capture job	41
Managing capture jobs	43
Exporting a packet capture file.....	46
SSL decryption (NetExpress only)	47
Requirements	47
Security considerations.....	48
Configuring SSL decryption.....	48
Port synchronization (NetExpress only).....	50
Service Response Time (SRT) metrics	51
Default SRT settings	51
NetProfiler export (NetExpress only).....	52
NetProfilers tab.....	52
Exported Interfaces tab.....	53
Flow data forwarding (NetExpress only)	54
Licenses (hardware-based models only).....	55

Packet Analyzer licensing.....	56
Licenses (virtual editions only)	56
General settings	57
Management Interface Configuration.....	58
Name Resolution	58
Aux Interface Configuration (NetExpress only)	60
Static Routes (NetExpress only).....	62
Monitor Interface Configuration (NetExpress only)	62
Packet Deduplication (NetExpress only).....	62
Time Configuration	63
Module Addresses (Enterprise NetProfiler only)	63
Data Sources (NetExpress only).....	64
SNMP MIB Configuration	65
Outgoing Mail Server (SMTP) Settings	66
Inside Address Configuration	66
Security Module Configuration	66
Report Data Management.....	67
Baseboard Management Controller Settings (Models xx70 only)	67
Service Management	69
Chapter 3 - Monitoring Services	71
Overview	71
Service dashboard.....	71
Service Health widget.....	73
Service Health by Location widget	74
Service Map widget.....	75
Service reports	75
Overall Performance Report.....	76
Service Performance Report.....	78
Service Incident Report	81
Location Performance Report.....	84
Location Incident Report	86
Managing services	89
Chapter 4 - Definitions	93
Applications.....	93
General applications	94
URL applications	98
Auto-recognized applications	100
Host groups	102
Host grouping pages	102
Defining host groups	104
Managing host group types	107
Interface groups	108
Port names	109

DSCP	110
Sensors/NetSharks and SteelHeads	111
WAN	112
Chapter 5 - Enterprise Integration	113
SteelHead QoS Shaping.....	113
Export SteelHead statistics to NetProfiler or NetExpress	114
Grant access to the SteelHead REST API	115
Poll the SteelHead	117
Verify configuration information.....	118
Vulnerability scanning	119
Types of vulnerability scans	120
Configuring automatic scans	120
Manually initiating a vulnerability scan	122
External links	122
Host switch port discovery	123
API access.....	123
Identity sources.....	124
Load balancers	124
DHCP integration	125
Lease data file format	125
Transfer mechanism	126
Update intervals.....	127
Chapter 6 - System Verification.....	129
System information.....	129
Flow statistics	130
Storage status.....	135
Data sources.....	136
Device & Interface tab.....	140
Interfaces tab	142
Devices tab	143
Synchronization tab.....	143
Preferred Interfaces tab.....	146
Audit trail.....	146
Report Criteria	146
Report results.....	149
Activity Types and Subtypes	154
Shutdown/Reboot	161
Update.....	161
Backup	162
Backup Status	163

Excluded file types	163
Backup location	163
Encryption Password	164
Notification	164
Running the backup operation	164
Restore operation	164
Chapter 7 - Service Policies	165
Overview	165
The Services Policies page	166
Configured Policies section	166
Tune Policies section	168
Chapter 8 - Performance and Availability Policies	173
Overview	173
Types of policies	173
Managing policies	174
Managing configured policies	174
Creating or Editing Performance and Availability policies	175
Creating new performance and availability policies	177
Tuning a policy	178
Application Availability policies	178
Application Performance policies	180
Link Congestion policies	180
Link Outage policies	183
Chapter 9 - User-defined Policies	185
Overview	185
Alerting	186
Pre-defined policies	186
Defining policies	187
Chapter 10 - Security Policies	189
Overview	189
Security event detection	190
Security profiles	192
Types of security profiles	192
Changing security profiles	192
Tuning alerting	193
Alerting thresholds	194
Specifying alerting thresholds	194
Requirements for matching an alerting rule	195

Precedence of alerting threshold rules	195
Tools for managing alerts	195
Notifications of security events	196
Chapter 11 - Health Policies	197
Overview	197
Data Source Problem	198
Hardware Problem	198
Module Problem	199
Storage Problem	199
Chapter 12 - Notifications	201
Overview	201
Adding recipients	202
Assigning notifications to recipients	203
Chapter 13 - Reporting	205
Overview	206
Report Layouts	207
Report Criteria	207
Report Format	208
Report menu	214
Quick reports	214
Shortcuts to reports	216
Built-in reports	216
Custom reports	218
Service reports	219
Traffic reports	219
Report Criteria section	219
“Report by” options	220
Traffic report section	222
WAN Optimization reports	223
Site reports	223
Intersite reports	223
Overall reports	224
Top Talkers	224
Report Criteria section	224
Traffic Report section	225
Event reports	225
Report Criteria section	225
Event Report section	226

Event Details reports	228
Viewing with an Event Viewer account	228
SteelHead QoS shaping policy reports	229
Running a report	229
SteelHead QoS Summary reports	230
SteelHead QoS Shaping reports	232
SteelHead QoS Shaping report for an aggregated class	232
SteelHead QoS Shaping report for a site	235
SteelHead QoS Shaping report for a class at a specified site	237
Active Directory Users reports	240
Report Criteria section	240
Report section	240
Saved reports	241
Reports section	241
Templates section	241
General Information reports	242
Application Information reports	242
Interface Information reports	243
Device Information reports	246
Interface Group Information reports	246
Host Information reports	247
Host Group Information reports	248
Server Information reports	249
Switch Information reports	249
Network Segment Information reports	250
DSCP Information reports	251
BGP AS Information reports	252
Investigation reports	253
Service Level Objective reports	253
Performance Investigation reports	254
95th Percentile report	255
SDN (Software-defined Networks) Reports	256
VXLAN technology	256
VXLAN Summary Report	257
Virtual Network Information Report	259
Tunnel Endpoint Information Report	261
VoIP reports	265
VoIP Performance report	265
VoIP Dependencies - Signaling report	266
VoIP Dependencies - Calls report	267
Audit Trail reports	267
Analyzing packet information with Packet Analyzer	268
Prerequisites	268
Analyzing NetShark or NetExpress packet information	269
Exporting NetShark packet information	270
Packet reporting and export with Cascade Sensor	270

Viewing Sensor packet information	271
Exporting Sensor packet information	271
Chapter 14 - Mitigation	273
Introduction	273
Switch Mitigation	274
Router Mitigation	274
Using the mitigation feature	276
Trusted hosts setup	276
Switch mitigation setup	277
Column descriptions	278
Modifying switch setups	279
Router mitigation setup	279
Column descriptions	279
Modifying and testing router setups	280
Enabling mitigation plan generation	280
Managing mitigation actions	281
Activating mitigation actions	282
Deactivating mitigation actions	283
Managing mitigation plans	283
Working with Plans and Actions	284
Chapter 15 - Appliance Security	287
Overview	287
Password Security	288
Security Compliance	289
Operational modes	289
Accounts	293
Access	294
Encryption Key Management	296
Displays and controls on the page	296
Replacing Keys and Certificates	298
Replacing SSH keys	298
Regenerating an SSH key pair	298
Changing SSH key pair	299
Replacing SSL certificates	299
Replacing the MNMP SSL certificate	300
Replacing the Identityd SSL certificate	304
Replacing the Apache SSL certificate	308
SSL certificate requirements	309
Appendix A - SNMP Support	311
Trap summary	311

Variables common to all NetProfiler and NetExpress traps	312
Additional trap variables	314
Denial of Service/Bandwidth Surge trap variables	314
Suspicious Connection trap variables.....	314
New Server Port trap variables.....	315
Performance, Availability, and User-defined trap variables	315
Service trap variables	315
SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliance MIB.....	316
Versions 1 and 2c.....	316
Version 3.....	316
Examples	316
Appendix B - Restoring a system	319
Requirements	319
Platform compatibility.....	320
Password-less access	320
Link speed	321
Password.....	321
Licenses	321
Before you begin	321
Restoring a Standard NetProfiler.....	321
Restoring an Enterprise NetProfiler	323
Restoring a NetExpress	324
Appendix C - Securing the Environment.....	327

Introduction

The *SteelCentral™ NetProfiler and NetExpress User's Guide* describes both the hardware-based and virtual editions of the NetProfiler and NetExpress. The virtual editions operate the same as their hardware-based counterparts except for a small difference in licensing. This is described in [Chapter 2, “Configuration.”](#)

Read this introduction for an overview of the information provided in this guide, the documentation conventions used throughout, the hardware and software dependencies, additional reading, and contact information. This introduction includes the following sections:

- [“About This Guide,”](#) next
- [“Product Dependencies and Compatibility”](#) on page 3
- [“Contacting Riverbed”](#) on page 4

About This Guide

The *SteelCentral™ NetProfiler and NetExpress User's Guide* describes how to configure, manage and use the SteelCentral™ NetProfiler and SteelCentral™ NetExpress. It describes configuring the products on the network, defining what is to be monitored, defining usage policies, alerting on policy violations, and reporting on traffic volumes and policy violations.

The products differ in their capacities for handling and storing flow data. They also differ in their options for receiving data from flow data sources. This guide identifies the differences between the products where they impact the procedures or functionality being described. Otherwise, all products are referred to as simply “the product” or “the system” throughout the guide.

Types of Users

This guide is written for network operations and security operators, administrators, managers and analysts. It assumes that you have at least a basic understanding of networking and network management concepts.

Organization of This Guide

The *SteelCentral™ NetProfiler and NetExpress User's Guide* includes the following chapters:

- [Chapter 1, “Overview,”](#) an overview of the features.
- [Chapter 2, “Configuration,”](#) configuring the appliance to be accessible on the network to authorized users.
- [Chapter 3, “Monitoring Services,”](#) defining and monitoring network services.
- [Chapter 4, “Definitions,”](#) how to define applications, groups, port names and DSCP markings so that they can be tracked, reported, and alerted on.
- [Chapter 5, “Enterprise Integration,”](#) main features for integrating the appliance into the core infrastructure of your network.
- [Chapter 6, “System Verification,”](#) how to ensure that the appliance are properly configured before you begin routine operational use.
- [Chapter 7, “Service Policies,”](#) managing the policies created to monitor service performance metrics.
- [Chapter 8, “Performance and Availability Policies,”](#) capabilities for monitoring the performance and availability of your network.
- [Chapter 9, “User-defined Policies,”](#) capabilities for monitoring violations of network usage policies.
- [Chapter 10, “Security Policies,”](#) capabilities for monitoring violations of network security policies.
- [Chapter 11, “Health Policies,”](#) capabilities for alerting users to the existence of hardware and software problems.
- [Chapter 12, “Notifications,”](#) capabilities for notifying users or groups of users when network behavior triggers an alert.
- [Chapter 13, “Reporting,”](#) reporting features.
- [Chapter 14, “Mitigation,”](#) capabilities for mitigating the affects of malicious or misconfigured traffic.
- [Chapter 15, “Appliance Security,”](#) password security, security compliance, and encryption key management.
- [Appendix A, “SNMP Support,”](#) traps and access to the MIB.
- [Appendix B, “Restoring a system,”](#) backing up the SteelCentral™ NetProfiler and SteelCentral™ NetExpress logs and restoring the system from the backup copy.

Document Conventions

This guide uses the following standard set of typographical conventions to introduce new terms, describe command syntax, and so forth.

Convention	Meaning
<i>italics</i>	Within text, new terms and emphasized words appear in italic typeface.
boldface	Within text, commands, keywords, identifiers (names of classes, objects, constants, events, functions, program variables), environment variables, filenames, GUI controls, and other similar terms appear in bold typeface.
Courier	Information displayed on your terminal screen and information that you are instructed to enter appears in Courier font.
< >	Within syntax descriptions, values that you specify appear in angle brackets. For example: interface <ipaddress>
[]	Within syntax descriptions, optional keywords or variables appear in brackets.

Convention	Meaning
{ }	Within syntax descriptions, required keywords or variables appear in braces. For example: {delete <filename> upload <filename>}
	Within syntax descriptions, the stroke (pipe) symbol represents a choice to select one keyword or variable to the left or right of the symbol. (The keyword or variable can be either optional or required.)

Product Dependencies and Compatibility

This section provides information about product dependencies and compatibility. It includes the following sections:

- [“Hardware and Software Dependencies,”](#) next
- [“Ethernet Network Compatibility”](#) on page 3
- [“SNMP-Based Management Compatibility”](#) on page 4

Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliances.

Riverbed SteelCentral™ Component	Hardware and Software Requirements
chassis	19 inch (483 mm) two or four-post rack.
user interface	Secure Sockets Layer (SSL) capable browser. The user interface has been successfully tested using Microsoft Internet Explorer 9, 10 and 11; Mozilla Firefox ESR 38.5.x; and Chrome. Note: JavaScript and cookies must be enabled in your Web browser.
command line interface	A computer with a Secure Shell (ssh) client that is connected by an IP network to the appliance management interface. Free ssh clients include PuTTY for Windows computers, OpenSSH for Linux.

Ethernet Network Compatibility

The appliance supports the following types of Ethernet networks:

- Ethernet Logical Link Control (LLC) (IEEE 802.2 - 2002)
- Fast Ethernet 100 Base-TX (IEEE 802.3 - 2002)
- Gigabit Ethernet over Copper 1000 Base-T and Fiber 1000 Base-SX (LC connector) (IEEE 802.3 - 2002)

The management port in the appliance is 10 Base-T/100, Base-TX/1000.

The appliance supports VLAN Tagging (IEEE 802.1Q - 2003). It does not support the Cisco ISL protocol.

All copper interfaces are auto-sensing for speed and duplex (IEEE 802.3 - 2002).

SNMP-Based Management Compatibility

The appliance supports a proprietary Riverbed MIB accessible through SNMP. Both SNMP v1 (RFCs 1155, 1157, 1212, and 1215) and SNMP v3 are supported.

SNMP support allows the appliance to be integrated into network management systems such as Hewlett Packard OpenView Network Node Manager, BMC Patrol, and other SNMP-based network management tools.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

Internet

You can find out about Riverbed products through our Web site at **<http://www.riverbed.com>**.

Riverbed Support

If you have problems installing, using, or replacing Riverbed products contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, please open a trouble ticket at **<https://support.riverbed.com>** or call 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States.

Professional Services

Riverbed has a staff of professionals who can help you with installation assistance, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services go to **<http://www.riverbed.com>** or email **proserve@riverbed.com**.

Documentation

We continually strive to improve the quality and usability of our documentation. We appreciate any suggestions you may have about our online documentation or printed materials. Send documentation comments to **techpubs@riverbed.com**.

CHAPTER 1 Overview

This chapter provides an overview of SteelCentral™ NetProfiler and SteelCentral™ NetExpress features. It includes the following sections:

- [“Overview of NetProfiler and NetExpress appliances,”](#) next
- [“Information sources”](#) on page 6
- [“Behavior analysis”](#) on page 8
- [“Alerting and notification”](#) on page 9
- [“Security profiles”](#) on page 10
- [“Host groups”](#) on page 10
- [“Interface groups”](#) on page 11
- [“Application tracking”](#) on page 12
- [“Traffic reporting”](#) on page 12
- [“User interface”](#) on page 14
- [“Getting help”](#) on page 21

This chapter assumes you have installed the appliance and performed the installation verification. For installation information, see the installation guide.

Overview of NetProfiler and NetExpress appliances

The NetProfiler and NetExpress appliances provide continuous visibility into the performance and behavior of the computers, applications, and users on your network. Each appliance collects information from a variety of sources, analyzes network behavior, and reports current and historical network usage. It also alerts you to significant changes in the behavior of the network or individual elements of the network.

The information that the appliance provides is useful for managing:

- Services
- Performance and availability
- Security
- Regulatory compliance

- WAN optimization
- Change management databases
- Data center migrations and consolidations

Information sources

The appliance collects traffic, application, and user data from multiple sources, including:

- Cascade Sensor
- Flow Gateway
- NetShark
- AppResponse
- SteelHead (SteelCentral™ NetExpress only)
- NetFlow, sFlow, IPFIX, and Packeteer FDR data sources (SteelCentral™ NetExpress only)
- Microsoft Active Directory domain controllers

The NetProfiler receives NetFlow, SteelFlow Net, sFlow, IPFIX, and Packeteer FDR information that has been sent to a Flow Gateway, in addition to receiving traffic information directly from Sensor, NetShark and AppResponse appliances.

The appliance combines and de-duplicates data from all sources to report both detailed and aggregated information about hosts, ports, interfaces, applications, and users. It also uses this data to identify and alert on changes in network behavior.

Cascade Sensor

Using mirror ports on switches or passive taps on lines, Sensors provide the appliance with statistics for the following network traffic characteristics:

- Connections between hosts on the monitored segments of the network
- Source and destination IP addresses and port numbers used in the connections
- Protocols
- Applications being accessed on hosts
- Traffic volumes in connections, packets, bytes, or bits per second
- Performance metrics

Sensor communications with the appliance are compressed and encrypted.

Flow Gateway

The Flow Gateway is deployed in a local or remote network to receive traffic data from sources at that location, including:

- NetFlow, sFlow, or IPFIX sources
- SteelHead SteelFlow Net sources
- Packeteer FDR sources

It aggregates the data, compresses it, encrypts it, and then transmits it to two NetProfiler or NetExpress appliances. Additionally, it can forward this data in its native format to two other destinations.

NetShark

The NetShark sends the SteelCentral™ NetProfiler and SteelCentral™ NetExpress information about all the traffic it sees on the network. From within the SteelCentral™ NetProfiler user interface, you can access the Packet Analyzer for detailed packet-level analysis.

AppResponse

Riverbed AppResponse appliances can send the SteelCentral™ NetProfiler and SteelCentral™ NetExpress information about all the traffic they see on the network. From within the SteelCentral™ NetProfiler user interface, you can access the Packet Analyzer for detailed packet-level analysis.

SteelHead

The Riverbed SteelHead sends SteelFlow Net to the Flow Gateway and SteelCentral™ NetExpress. The SteelCentral™ NetExpress can receive SteelHead data directly. The SteelCentral™ NetProfiler can receive this data from SteelCentral™ Flow Gateway appliances that are receiving it from SteelHead sources. The NetProfiler or NetExpress uses this flow information to report the traffic flows and WAN performance associated with the SteelHead appliances. The SteelHead can also send Quality of Service Shaping configuration information in SteelFlow Net. The SteelCentral™ NetProfiler and SteelCentral™ NetExpress use this information to report the performance of SteelHead QoS shaping policies.

NetFlow, sFlow, and IPFIX sources

The SteelCentral™ NetExpress can use IPFIX or NetFlow data directly from switches, routers, or other devices installed at key points in the network. The SteelCentral™ NetProfiler can receive this data from SteelCentral™ Flow Gateway appliances. The data source devices must be configured to send their data to the appliance.

The appliance processes data that is compatible with IPFIX and Cisco NetFlow Versions 1, 5, 7, and 9.

Packeteer

The SteelCentral™ NetProfiler and SteelCentral™ NetExpress can obtain information about Layer 7 application traffic from compatible Packeteer devices that are sending Flow Detail Records. The SteelCentral™ NetExpress can receive Packeteer data directly. The SteelCentral™ NetProfiler can receive this data from SteelCentral™ Flow Gateway appliances that are receiving it from Packeteer sources.

Microsoft Active Directory domain controllers

The optional user identity feature relies on data obtained from the security event log of one of more Microsoft Active Directory domain controllers. This data can be sent directly to the appliance or it can be read by a Windows intermediary host that sends it to the appliance.

The appliance interprets this data to track successful and failed login attempts by domain users on hosts within the domain. It associates this user identity information with host information to produce reports that identify users as well as hosts.

Behavior analysis

NetProfiler and NetExpress employ a variety of techniques for analyzing and evaluating network behavior, including:

- Service policies
- Performance and availability policies
- User-defined policies
- Security policies (Security policies are not available if the security analytics module is disabled or not installed.)
- Health policies

When the appliance determines that a policy violation or other significant event has occurred, it displays an alert status, sends an SNMP notification to a management system, or sends an email notification to a specified person or group of people.

The notification includes a link to a detailed report of the network event that triggered the alert. This report is available both on the NetProfiler GUI and on any NMS or SEM product that has been configured to access the NetProfiler reporting features. You can examine the report and determine what action to take.

Whether behavior analysis is based on comparisons to absolute thresholds or on advanced analytics using dynamic modeling of network behavior, the result is the identification of conditions and events that you want to know about.

You can control which events generate alerts by setting tolerance ranges or alerting thresholds for each type of policy. Events that violate one policy may be more important than events that violate another policy, so you may want them to generate higher level alerts or to notify different people. The notification includes a link to a detailed report of the network event that triggered the alert. This report is available both on the appliance GUI and on any NMS or SEM product that has been configured to access the appliance reporting features. You can examine the report and determine what action to take.

The appliance enables you to determine who is notified of what type of events and what level of alert (low, medium or high) is generated for each type of policy violation. The appliance is shipped with several useful policies already defined. You can activate these, adjust them for your network, or use them as examples for creating new policies.

The appliance uses the following steps to analyze network behavior and alert you to significant network events:

1. Network monitoring - receives traffic information from any combination of a variety of sources. Aggregates, de-duplicates and processes traffic data to prepare it for network behavior analysis. Builds profiles of typical network behavior for specified times.

The NetProfiler and NetExpress receive data from Shark or Flow Gateway appliances. The NetExpress can also monitor traffic directly and receive flow data from other sources.

2. Event detection - compares network behavior to usage policies specified on the Behavior Analysis > Policies pages. Analyzes compliance with service policies, performance and availability policies, security policies, and user-defined policies using separate sets of analytics. It assigns each security policy violation event a severity rating number based on the likelihood of it being a threat to network performance, availability or security.
3. Alert generation - checks the severity of each network event against a set of user-defined tolerance ranges or alerting thresholds. When the severity of an event exceeds a tolerance or alerting threshold, the appliance alerts users to the existence of the event by indicating an alert condition and displaying information about the event.
4. Notification - automatically sends email alert messages to designated recipients. Sends SNMP messages to designated security or operations management systems.

5. **Event reporting** - saves details of all events that triggered alerts. Event detail reports can be viewed on the user interface or retrieved by remote management systems for analysis. Refer to the next chapter for descriptions of reporting.

The appliance follows this sequence of actions for service policies, performance and availability policies, security policies, and user-defined policies. However, steps for policy definition and tuning vary, depending on the type and complexity of the policy. These are discussed in the sections that follow.

Alerting and notification

The appliance uses the following mechanisms to notify an operator or management system that a network event has violated a policy.

- **Alert level status displays** - The appliance displays a “High,” “Medium,” or “Low” alert indication in the header at all top-level GUI pages. The alert indication is displayed until the alert condition no longer exists or is temporarily suppressed (“snoozed”) by clicking a control on the event details report for the event.
- **SNMP notifications** - The appliance sends SNMP traps or notification messages to specified network management systems. The management system receiving the notification might display messages or send email itself. It can obtain a URL from the message, which allows it access to a report of the event that triggered the alert. Management systems that will be retrieving Event Detail reports from the appliance based on URLs attached to SNMP notifications should be given a user account and added to the access control list on the Integration > API Authorization page.
- **Email notifications** - The appliance sends email notifications to designated users or management systems.

Alerting

The appliance displays an indication of its alert status at the top of the user interface page. The alert status is one of the following:

- **OK** - The appliance is operating and no alerts are present.
- **Low** - One or more low-severity events are present.
- **Medium** - One or more medium-severity events are present.
- **High** - One or more high-severity events are present.
- **Unknown** - The alert status is unknown when the appliance is offline.

Alerts are triggered by conditions that violate service policies, performance and availability policies, user-defined policies, or security policies.

If the Alert Level indicator at the top of the page is red (High) or yellow (Medium), click the red or yellow indicator to run an Event Report. The Event Report lists events that are triggering alerts. Click the Event ID in the Event List to run an Event Detail Report for an individual event.

You can also investigate the event that triggered the alert by using the Dashboard page, the Report pages, or the Quick report box at the top of the page.

Figure 1-1. Page Header



Notification

You can specify who is to be notified at the time you define a policy. Alternatively, there is a page for modifying or specifying all notifications.

Security profiles

The appliance collects traffic data from the monitored network and aggregates it into security profiles. A security profile can be created for “business hours” or “weekends” or any other time periods you want to specify. Each profile is a mathematically-derived abstraction of the network behavior that is typical for the time periods it represents. Recent statistics play a larger role in the profile than older statistics, with each previous time period having a successively smaller impact on the profile. This allows the appliance to automatically adjust to changes in network traffic patterns over time. It is responsive to new conditions, yet retains a historical perspective of traffic patterns on the network.

The appliance compares new traffic to the corresponding profile to detect anomalous behavior. The definition of anomalous behavior can be tuned to accommodate a wide variety of considerations.

The security profile is available to use for event detection when the appliance has collected sufficient data and a user-definable delay time has ended. There are two types of security profiles:

- Recurring profiles
- Exception profiles

Recurring profiles are developed from traffic during times that occur every week, such as Monday from 8:00 AM to 4:59 PM. Exception profiles are developed from traffic collected during times that occur less frequently than a weekly schedule, such as ends of quarters or holidays.

Both types of profiles can comprise multiple time period specifications. For example, a Recurring profile named “Business hours” might be specified to include traffic from 8:00 AM to 4:59 PM every weekday. An Exception profile called “Ends of Quarters” might be specified to include traffic on March 31, June 30, and so forth.

Recurring profiles are useful for tailoring your system to accommodate known peaks and lulls in weekly traffic. Exception profiles allow you to treat holidays, quarterly events, or one-time promotional event surges differently from normal traffic. Using multiple configurable profiles allows you to set alerting thresholds more closely without significantly increasing false positives.

Host groups

The appliance enables you to assign hosts to groups so that you can track, report and alert on organizationally meaningful categories of traffic, such as traffic by host function or traffic by host location. This allows you to view the traffic of the same hosts from multiple perspectives.

For example, a view categorized by functions might include a host group for web servers, another host group for email servers, and so forth. A second view, categorized by location, might include all hosts in New York in one group, all hosts in London in another group, and so forth.

Groups are defined in terms of IP addresses or address ranges. You can enter these in the GUI or import a text file containing group definitions. Alternatively, you can define a host group based on hosts listed in a report table.

Within any group type (such as “by location” or “by function”), you can assign names that identify the membership criteria for the group. For example, when grouping hosts by their functions, you might assign group names such as:

- Desktops

- Laptops
- Mail_servers
- Web_servers
- Database_servers
- Transaction_servers
- Routers
- Load_balancers
- Firewalls

When the appliance receives traffic flow information from a SteelHead, it automatically creates a host group for each SteelHead site. This enables you to monitor traffic by SteelHead sites.

Interface groups

The appliance tracks interface traffic volumes and utilization percentages. For networks with a large number of interfaces, it is often helpful to aggregate interface statistics into groups for reporting and alerting.

You can define policies for interface groups and generate reports on interface groups.

WAN interfaces can be grouped separately to facilitate tracking and reporting for WAN optimization.

Application tracking

The appliance tracks and reports application traffic. It recognizes three categories of applications:

- General - custom application definitions based on hosts, host groups, protocols, ports or Auto-Recognized applications.
- URL - custom application definitions based on one or more URLs.
- Auto-recognized - libraries of common application definitions. The product is shipped with a library of automatically recognized application definitions. It obtains additional application identification information from the following sources:
 - Sensor - information provided by a Cascade Sensor.
 - AppResponse 11 - information provided by an AppResponse 11.
 - SteelConnect Manager - information provided by a SteelConnect Manager
 - Palo Alto Networks - information provided by a Palo Alto Networks product.
 - AppFlow - information provided by a Citrix product that supports AppFlow.
 - NBAR - requires a Cisco device to be sending Network-Based Application Recognition data to NetProfiler.
 - Packeteer - requires a compatible Packeteer device to be sending Flow Detail Records to NetProfiler.
 - NetShark - information provided by a NetShark.
 - SteelHead - requires the SteelHead to be sending SteelFlow Net information to NetProfiler.

Traffic reporting

The traffic reporting feature supports several approaches to creating reports:

- Shortcuts page
- Traffic Report pages
- Quick report box in header
- Left-clicking
- Right-clicking

Traffic reports can be saved, emailed, exported and printed. They can also be saved as templates and scheduled to run periodically or at a specified time.

Shortcuts page

The Shortcuts page provides links for running predefined reports. These have been predefined as far as practical and named in terms of common tasks to simplify running a report to answer a question about your network.

Traffic Report pages

Traffic reports can be oriented towards hosts, interfaces, or applications. Additionally, an advanced reporting page provides controls for searching profiles or historical logs for time-series data for specified hosts or ports. Each type of traffic report provides controls for specifying the time span of the report and the format of the display.

The report displays include controls for changing the subjects and formats of the reports. Up to ten thousand lines of traffic report data can be exported in comma-separated values (CSV) files for use with other report generating tools or databases. Reports can also be exported as HTML archive files or PDF files.

Quick report box

The Quick report box appears in the header of each top-level page of the GUI. If you want a report about a specific entity, you can enter the entity identifier and value in this box and click Go to produce a report without specifying a query on one of the Report pages.

Left-clicking

Left-clicking a host or host group generates two lists of traffic volumes. These are listed by port for:

- Ports served by the host or host group
- Ports connected to by the host or host group

Left-clicking a service runs a service performance report.

Left-clicking the flow ID on a flow list allows you to perform packet-level analysis using a Packet Analyzer and NetShark appliances.

Right-clicking

Right-click menus enable you to obtain additional information without having to switch contexts or go to the report pages. You can right-click any underlined item in any list or table entry to drill down to additional detail about that item. You can also right-click any traffic graph on the dashboard or on any traffic report to obtain additional detail. Right-clicking a service displays a menu of performance reports that can be run for that service.

The choices for additional information that appear on the right-click menu depend on the item you right-click and the options that you have configured. For example, if you right-click a host and you have vulnerability scanning configured, then you will be able to initiate a vulnerability scan from the right-click menu. If you have external links defined, then the links are listed on the right-click menu, and you can send the item you click to an external program with just one more click. If you have the user identity feature set up, you will be able to run a user report from the right-click menu. If the appliance is receiving information from a Sensor, NetShark or AppResponse appliance, you can get packet-level reports for the host. Additionally, you can specify notes to be associated with hosts for future reference.

Menu choices that are grayed out are either not applicable to the item clicked or else not available because they are not configured.

The report that you generate from the right-click menu retains the context of the report in which you right-clicked the item. If the table item, list item, or graph you right-clicked is on a dashboard widget or traffic report for a particular port, protocol, group, time period, etc., then the drill-down report is limited to those same attributes.

User interface

The main page in the appliance user interface is the Dashboard page. The Dashboard page displays high-level summaries of activity on the monitored network.

The Dashboard page and all other top-level pages of the GUI include a header that displays the:

- Alert level
- Quick report box
- User name under which the browser session is running

Additionally, there is a navigation bar listing the GUI pages that you can go to for detailed information, reports and configuration settings. The privilege level of your user account determines which pages are available in the navigation bar. Those with Administrator accounts can navigate to all pages. Those with other types of accounts can access the pages appropriate to their roles. For a quick display of all available menu options, click the Riverbed logo.

The top-level sections available from the navigation bar include:

- Home
- Services
- Reports
- Behavior Analysis
- Definitions
- Configuration
- System

Home pages

There are three home pages:

- Dashboard - home page for monitoring the network
- Navigate Network - starting point for diagnosing network problems from the perspective of interface performance
- Browse Preferred Interfaces - identify the interfaces having the highest traffic volumes and check their utilization and performance statistics.

Dashboard page

The dashboard page enables you to monitor network performance using your choice of a wide assortment real-time displays. You can:

- Create a dashboard using any of several templates that are pre-populated with content widgets for specific purposes and then customize it to focus on the information you find most useful.
- Create a new dashboard and populate it with the content widgets yourself.
- Share your dashboards with selected users and use dashboards created by other users.
- Define end-to-end application delivery services and monitor their state of health and alert conditions.

- Monitor traffic volumes and use the right-click menu to generate reports on traffic by any of numerous attributes, including flows, hosts, applications, ports, protocols, BGP autonomous systems, DSCP markings, users and interfaces.
- Drill down to the level of packet analysis by accessing other Riverbed devices directly from the right-click menu.

If you prefer to investigate problems from the perspective of the performance of links or interfaces on network devices, go to the Home > Navigate Network page for a hierarchical view of all the network interfaces known to the NetProfiler. There you can run reports on the performance of devices and interfaces.

The Dashboard page is highly customizable. You can create multiple customized versions and switch among them. The Dashboard page has the following main components:

- Navigation panel
- Page controls
- System messages
- Statistics and events displays (widgets)

The permissions associated with the user account determine the actions that can be taken on the Dashboard page.

The product is shipped with dashboards set up for the default administrator account. These are listed in the Dashboards navigation panel on the left side of the page. When you log into the default administrator account, the dashboards are listed under “My Dashboards” because they belong to that account. When you log into any other account, the same dashboards are listed under “Others’ Shared.”

Dashboards that are private to your user account are indicated by an icon representing a single person. Dashboards that you have made public for all users are indicated by an icon representing a group of people. Click any dashboard listed in the Dashboards navigation panel to view it.

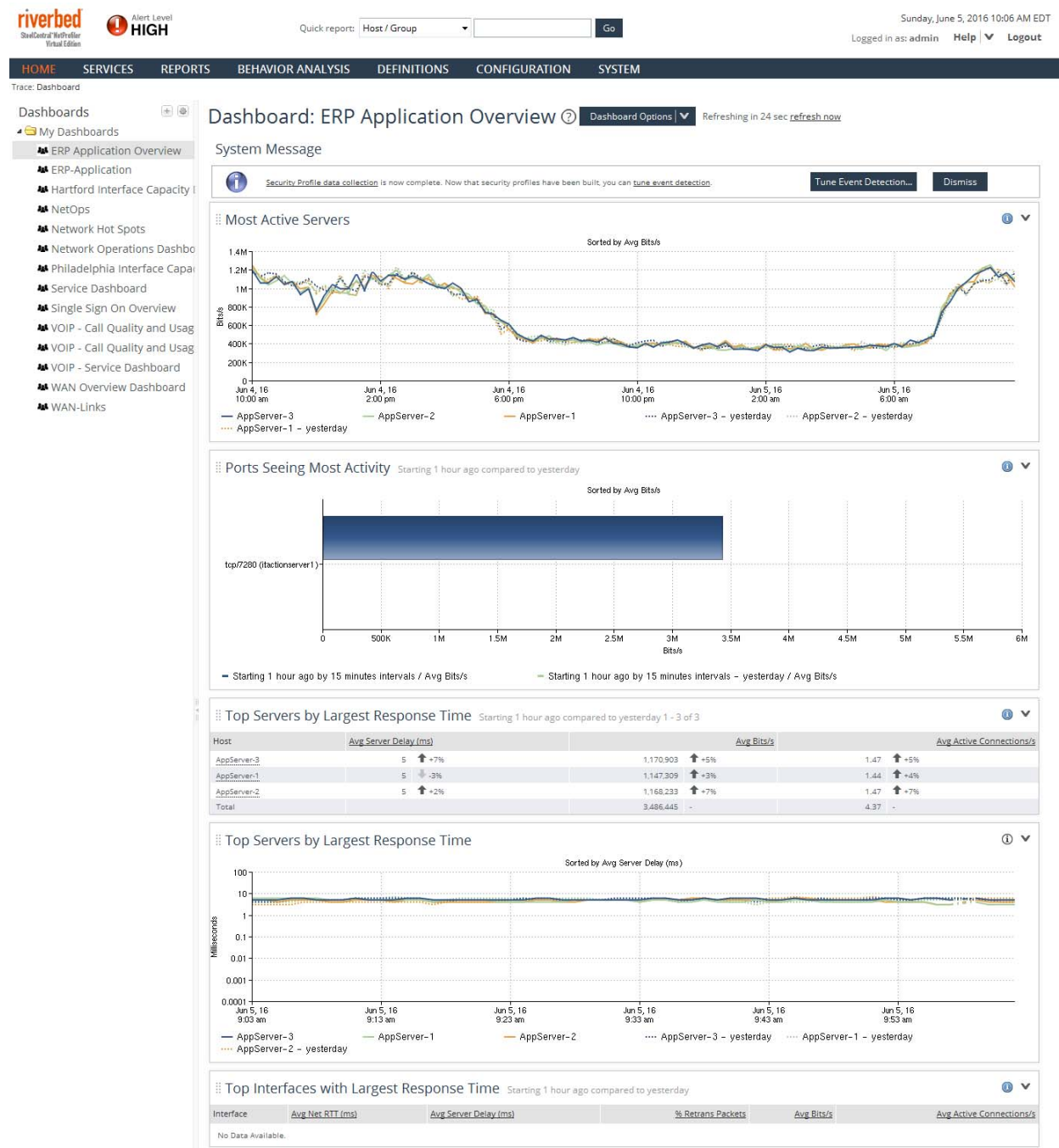
You can copy a dashboard belonging to another user and modify it to suit your needs. You can create your own dashboards and either keep them private (only you see them) or make them public (other users can see them and copy them). You can modify dashboards that you have created or copied from others, but you cannot modify dashboards that belong to other users.

Use the Dashboards Options menu to create a dashboard and to add content (dashboard widgets) to it. Templates are provided with content widgets already selected for different purposes. On the Dashboard Options menu, choose Create Dashboard to open a tool that displays the templates. You can hover your mouse pointer over a template icon to see an enlarged image with labels identifying the metrics the template contains. The templates include:

- New Dashboard - an empty dashboard that you populate with content widgets of your own choosing
- Network Operations Dashboard - top traffic volumes for hosts, ports, applications and application servers
- Service Dashboard - health of network service delivery displayed as overall health by service and health by location; also displays a service map, location map, and list of current service events
- Overall WAN Dashboard - traffic volumes of optimized and non-optimized WAN and LAN traffic and top network interfaces
- VoIP Call Quality and Usage Dashboard - top VoIP-RTP applications, average MOS, average jitter, %RTP loss packets, traffic volume, and a map of host group pairs
- VoIP Quality of Service Dashboard - DSCP usage (EF)
- Response Time Dashboard - response composition, server delay for top application servers and hosts using the web, and top host groups by network round trip time and by server delay

The Dashboard Options menu also enables you to copy, edit, delete, manage, print, email and export dashboards. Refer to the online help system for instructions on how to manage dashboards and dashboard widgets.

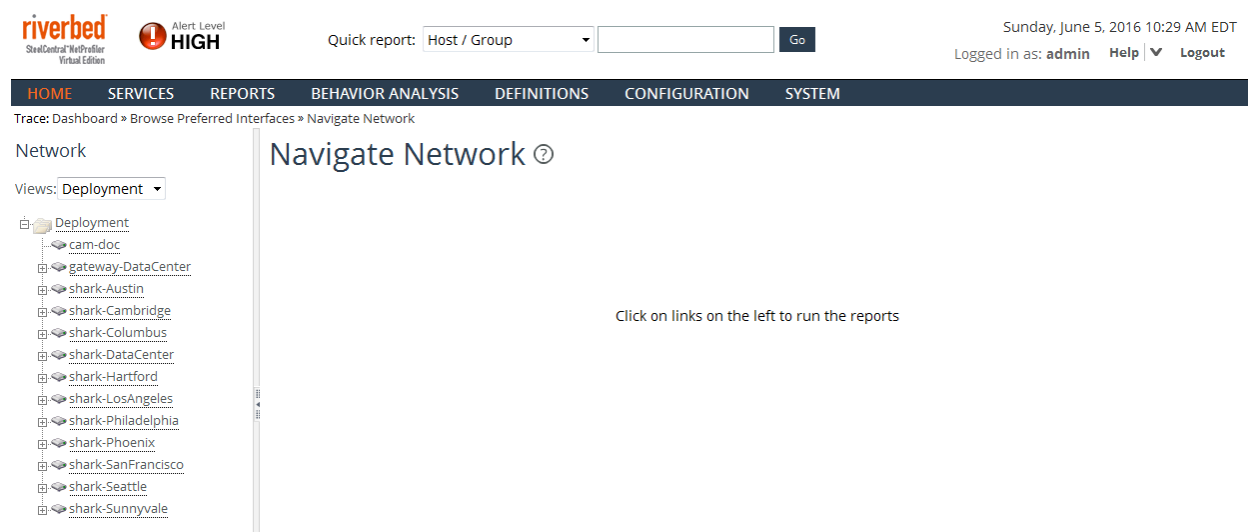
Figure 1-2. Home > Dashboard page



Navigate Network page

The Home > Navigate Network page provides an interface-oriented view of the network. It displays a wide variety of reports about traffic flow collection devices, the devices from which they are collecting flow information, and the interfaces of those devices. The main section of the page displays reports about the devices or interfaces you select in the navigation panel on the left.

If the navigation panel is not visible, double-click or click-drag the hide/display control at the far left of the main display area of the page.

Figure 1-3. Home > Navigate Network page

The navigation panel displays expandable tree hierarchies of all devices and their interfaces known to the NetProfiler or NetExpress appliance. Hover the mouse pointer over a device or interface to display a popup message with information about it. Left-click a device to run a Host Information report. Left-click an interface to run an Interface Information report. Right-click an any item in the tree for a menu of reports that you can run on that item.

Use the View box in the navigation panel to select the interface-oriented view of the network you wish to investigate. There are three default views:

- WAN - shows optimized and non-optimized WAN interfaces
- Deployment - shows all other devices and interfaces known to the NetProfiler appliance
- VXLAN - shows VTEPs (virtual tunnel endpoints) and virtual gateways and their physical interfaces

You can define your own views of the network based on attributes that are useful, such as geographic locations or business units. You can define views and interface groups within views on the Definitions > Interface Groups page.

Browse Preferred Interfaces page

Device interfaces that are sending traffic information to NetProfiler can be designated “preferred.” Traffic statistics for preferred interfaces are precomputed and cached for quick access.

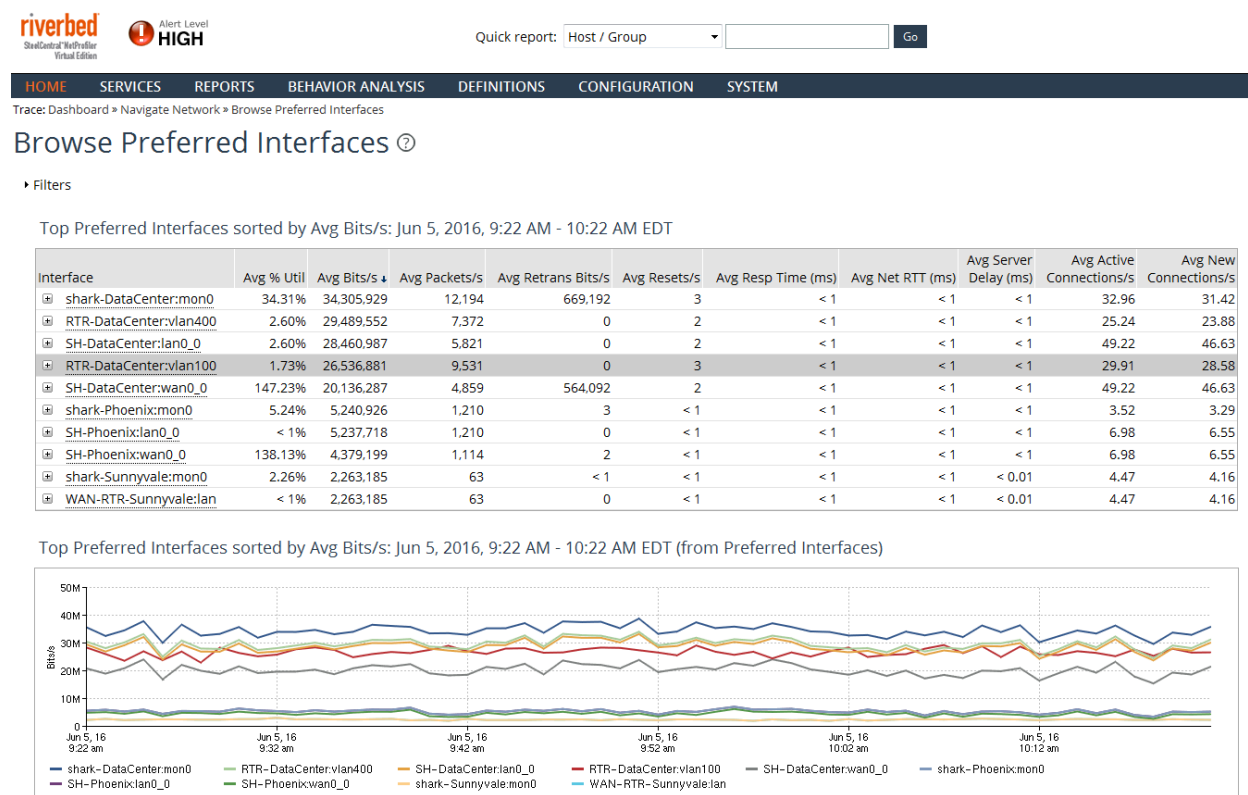
The Home > Browse Preferred Interfaces page displays statistics for the top 10 busiest preferred interfaces in order of traffic volume. It displays only preferred interfaces, and no other interfaces on the monitored network.

Preferred interfaces are listed in a table and also graphed. Each entry in the table can be expanded to display statistics for the following categories of information seen on the preferred interface:

- Applications with Ports
- Host Pairs with Ports
- DSCP values

Each of these categories can be expanded to display the top 10 members of the category. Click “+” to expand an entry and “-” to collapse it. Left-click any entry to run a traffic report on that entry. Right-click any entry to display a menu of reports available to be run for the entry.

Figure 1-4. Home > Browse Preferred Interfaces page



The graph displays the values for the entry selected in the table. Left-click a plot on the graph to run a traffic report on it. Right-click it to display a menu of reports available to be run for the selection. Use the graph menu to edit the display settings or to export the data to a file in CSV format.

Filtering

Expand the Filters section of the page to limit the displays to a particular time frame or selected preferred interface. The Filters section enables you to:

- Enter the DNS name or IP address of a device and the name of a preferred interface on that device. Enter the first letters of the name or first numbers of the address in the Preferred Interface box, and a drop-down list displays auto-complete options.
- Browse for a preferred interface. Click Browse to open the Look Up Interface tool. Enter the first few letters of the device name or IP address in the “Search for” box and click Search to find preferred interfaces that start with those letters or numbers. Alternatively, select the “Search all” or “Search within” options and click Search. Select a preferred interface from the search results and click OK.
- Report inbound statistics and outbound statistics separately by selecting the Split Inbound/Outbound check box.
- Show total values or average values of the metrics for the specified time frame.

Click Apply in the lower right corner of the Filters section to filter the table and graph displays.

Controlling which interfaces are preferred interfaces

The first time NetProfiler is started after being installed, it treats each interface it receives data from as a preferred interface, up to the limit for which its platform can reserve system resources. Interfaces are designated as preferred in the order in which they are discovered; first-come, first-served. It then displays statistics for the preferred interfaces carrying the top 10 traffic volumes.

This is a one-time operation. The initial selections remain in effect until you change them.

You can change the selections to any interfaces you want to have displayed on the Browse Preferred Interfaces page. Go to the System > Devices/Interfaces page Preferred Interfaces (List) tab to change the selection of preferred interfaces.

Other GUI pages

The Dashboard is the main page for monitoring the network. Typically, users start on the Dashboard page; go to other pages as necessary to run reports, investigate events, change settings, or check status; and then return to the Dashboard for routine monitoring.

The other GUI pages are described throughout the remainder of this guide. The controls, parameter fields and usage procedures for all GUI pages that are accessible from the navigation bar are described in the online help system.

Some features are available only if the security analytics module enabled, as noted in the setup section.

In summary, the GUI includes the following main pages:

- Home pages - Dashboard and Navigate Network pages
- Services - pages for defining services, running service reports, and managing service policies.
- Reports - pages for creating, saving, and viewing reports and templates for reports.
 - Shortcuts - shortcuts to reports for viewing summaries of network activity.
 - Traffic - provides tabs oriented towards generating reports on hosts, interfaces, and applications. Also includes an advanced tab for more specific reporting on combinations of categories.
 - WAN Optimization - supports reporting on WAN optimization benefits and opportunities.
 - Top Talkers - generates reports of monitored categories of traffic (hosts, interfaces, applications, etc.) for a specified time span.
 - Events - lists events and provides links to Event Detail reports.
 - SteelHead QoS Shaping - indicate the performance of SteelHead QoS shaping policies.
 - Active Directory Users - generates reports on user names and last login dates of users accessing the monitored network. (This page is not displayed when user identity information is unavailable.)
 - Saved Reports - lists saved reports and report templates.
- Behavior Analysis - pages for setting up event detection policies, alerting rules, and alert notifications.
 - Policies - sets parameters for service, application, performance, security, and user-defined policies and the values controlling when events produce alert messages.
 - Notifications - specifies the destination addresses for email and SNMP notifications of alerts.
 - Events - lists event Detail reports.
- Definitions - places hosts or ports into groups for simpler monitoring.
 - Applications - define custom applications by either fingerprints or mappings.
 - Host Groups - manages the grouping of hosts into named groups for ease of monitoring.

- Interface Groups - allows aggregating interface statistics into groups for reporting and alerting.
- Port Names - assigns names to ports for ease of tracking.
- DSCP - defines Differentiated Services Code Point markings.
- Sensors/NetSharks & SteelHeads - identifies sources of information.
- WAN - defines the WAN by identifying its interfaces.
- Configuration - after the appliance has been installed, use these pages to prepare for operational use.
 - UI Preferences - controls the conventions used for displaying names, addresses, units of traffic measurement, date and time formats, and protocol/port sorting.
 - Account Management - enables Administrators to create and modify user accounts; configures the appliance for remote authentication and authorization of users who do not have accounts set up on the appliance.
 - Change Password - changes your password. (This page is not displayed for Administrators, who edit passwords on the Accounts page.)
 - Integration - pages for integration the appliance with other network devices. This includes:
 - SteelHead QoS Shaping - reports the QoS shaping configurations that are set on the SteelHead appliances that are sending information to the NetProfiler or NetExpress.
 - Vulnerability Scanning - configures vulnerability scanning to be performed automatically or manually.
 - External Links - configures the appliance for contacting other network devices for additional information about a host or user of interest.
 - Switch Port Discovery - identifies switches so that the appliance can determine which switch port a host is using.
 - API Access - specifies accounts that can access the appliance via the API.
 - Identity Sources - allows you to disable or delete the use of identity information from selected sources.
 - Load Balancers - enables you to manage a list of load balancers that are used when defining services.
 - Mitigation - configures the appliance to use network devices to mitigate attack traffic. This includes:
 - Plans and Actions - manage mitigation plans and actions.
 - Trusted Hosts - identify hosts whose traffic is not to be blocked.
 - Switching Setup - identify switches that can be used for blocking attack traffic.
 - Routing Setup - identify routers that can be used for blocking attack traffic.
 - Flow Log - balances or reallocates disk storage space for optimum storage of flow information. Specifies the reporting time frames at which the appliance automatically switches from using one data resolution to using another data resolution.
 - SSL Decryption - (NetExpress only) enables SteelCentral Packet Analyzer users to view metrics for encrypted traffic when using NetExpress as a probe.
 - Packet Capture - (NetExpress only) capture packet information and export trace files.
 - Port Synchronization - (NetExpress only) select which ports are used to validate network performance metrics.
 - NetProfiler Export - (NetExpress only) identifies NetProfiler appliances to which the NetExpress can send traffic information
 - Flow Forwarding - (NetExpress only) forwards flow data to up to five other destinations

- Security Profiles - defines the days and times for which the appliance develops profiles for the security analytics.
- Licenses - manages feature and capacity licenses.
- General Settings - sets parameters necessary for the appliance to connect over the network with users, Sensors, DNS servers and email servers. Also sets parameters for sending to trap receivers and receiving flow data. Identifies addresses and address ranges to be tracked individually and what version of MIB browsing to support.
- System - provides status information about the appliance, its data sources, and its users.
 - Information - displays the status of this appliance.
 - Devices/Interfaces - provides several views of information about network devices and device interfaces. In the tree view, you can view detailed information by rolling over an item with your mouse. In the Interface List and Device List views, you can review details about all devices known to the appliance. You can also label device interfaces for easier recognition in reports. On the NetExpress, a Synchronization tab is provided for synchronizing with NetShark and SteelHead appliances. (Does not apply to CAX360 models.) The Preferred Interfaces tab controls which interfaces are preferred interfaces.
 - Audit Trail - provides an audit trail of the appliance usage.
 - Shutdown/Reboot - allows Administrators to reboot or shut down the appliance.
 - Upgrade - assists with upgrading to future versions.

Getting help

This remainder of this guide describes the appliance primarily at the conceptual level. For detailed information about controls, parameter fields formats, procedures, or technical considerations, refer to the online help system. This is available from the Help menu near the upper right-hand corner of all top-level GUI pages.

Additionally, all top-level GUI pages have links to the help system. All top-level pages are described under their names or functions in the help system. Refer to the help system table of contents, index, and search features.

CHAPTER 2 Configuration

This chapter describes configuring the SteelCentral™ NetProfiler and SteelCentral™ NetExpress to be accessible on the network to authorized users. It includes the following sections:

- [“Accessing the user interface,” next](#)
- [“User interface preferences” on page 24](#)
- [“Selecting preferred interfaces” on page 26](#)
- [“Account management” on page 27](#)
- [“Integration” on page 37](#)
- [“Mitigation” on page 37](#)
- [“Flow log” on page 38](#)
- [“Packet capture \(NetExpress only\)” on page 40](#)
- [“SSL decryption \(NetExpress only\)” on page 47](#)
- [“Port synchronization \(NetExpress only\)” on page 50](#)
- [“NetProfiler export \(NetExpress only\)” on page 52](#)
- [“Flow data forwarding \(NetExpress only\)” on page 54](#)
- [“Licenses \(hardware-based models only\)” on page 55](#)
- [“Licenses \(virtual editions only\)” on page 56](#)
- [“General settings” on page 57](#)

The appliance configuration tasks are assumed to be the responsibility of those with Administrator accounts. However, users with Operator accounts can perform all the tasks described in this section except for managing user accounts.

Accessing the user interface

The appliance can be accessed using a web browser from anywhere on the network that has access to its address.

To log in to the user interface

1. Ensure that your computer has network access to the management interface of the appliance.
2. Enter the IP address or DNS name of the appliance in your web browser using https.
3. Log in using the account name and password that were set up for you during the product installation.

If a user attempts to log in using incorrect passwords too many consecutive times, the appliance disables logins to the account for specified time. This lockout is canceled if someone with an Administrator account assigns a new password to the account.

Logging out differs from simply closing the browser window in that it returns you to the log-in page. You can log out as one user and log back in as another user without having to reestablish a browser session.

To log out of the user interface

- Click the Logout button at the upper right side of the header. This terminates your current user session and returns to the log in page.

User interface preferences

The Configuration > UI Preferences page controls the display conventions that apply generally throughout the user interface for a specific user. The page includes four sections: Data, Autocomplete, Date and Time Formatting, and Miscellaneous.

Data section

- **Host/Device Name Resolution** – chooses one, both, or neither of the following options. Based on your knowledge of your environment (for example, host names changing as a result of a recent equipment redeployment, your DHCP server not yet integrated with the NetProfiler, etc.), you can choose the options that work the best for your reporting needs.
 - **Resolve host and device names** – This option is available only if DNS, DHCP or SNMP name resolution has been enabled on the Configuration > General Settings page.
 - **Suppress DHCP/DNS/SNMP search domains () from resolved host and device names** – This suppresses the display of the domain names for hosts in the search domain. If no search domain is specified in the Name Resolution section of the Configuration > General Settings page, then all resolved hosts are displayed by their fully qualified names.
- **Host group** – which type of host group is to be displayed in event reports and traffic reports when the reports are set to display host group membership.
- **Protocol/Port Sort Options** – which sorting order for protocols and ports to use on reports.
- **Traffic Data Units** – units in which statistics are displayed wherever traffic volume or throughput is displayed.
- **Percentage Displays on Reports** – when to display percent-of-total numbers on reports.

Figure 2-1. Configuration > UI Preferences page

UI Preferences ?

Data

Host/Device Name Resolution

☒ Resolve host and device names.

☒ Suppress DHCP/DNS/SNMP search domains (lab.nbttech.com,nbttech.com) from resolved host/device names.

Example: hostname

Host Group

When displaying, show: ByLocation

Protocol/Port Sort Options

☒ Sort by port, then by protocol ☐ Sort by protocol, then by port

Traffic Data Units

When displaying Volume (Totals), by default show: ☒ Bytes ☐ Bits

When displaying Throughput (Averages), by default show: ☐ Bytes/s ☒ Bits/s

Percentage Displays on Reports

Display percentage-of-total in report columns:

☒ Always ☐ Never ☐ On the sorted column only

Autocomplete

Clear autocomplete cache: Clear

Turn On/Off autocomplete entries in input fields:

☒ Hosts/Host Groups

☒ Ports/Protocols

☒ Devices/Interfaces/Interface Groups

☒ Applications

☐ Steelheads

☐ Shaping Policy Paths

☐ BGP AS

☒ Auto Recognized Applications

Apply Preferences

Date and Time Formatting

Date Style

☒ Jan 10, 2000 ☐ 1/10/2000 ☐ 10-Jan-2000 ☐ 2000-1-10

Time Style

☒ 12-hour ☐ 24-hour

Time Zone

My time zone is: America/New_York ?

When displaying time zone, show as: ☒ EST ☐ -05:00

Example: Jan 14, 2017 11:39 AM EST

Miscellaneous

Non-interactive Connection Graph

☐ Show non-interactive Connection Graph

Color Palette

☐ Use alternate color scheme for graphs

Refresh Rate

Refresh page every: 1 minute(s).

Print/Email

Include a maximum of 200 rows in printed and emailed tables (HTML, PDF).

Packets Export from Sensor

Maximum size of tcpdump file (MB): 10

Autocomplete section

In this section you can enable or disable automatic completion of entries in input fields by category. Categories include:

- Hosts/Host Groups
- Ports/Protocols
- Devices/Interfaces/Device and Interface Groups
- Applications
- BGP Autonomous Systems
- SteelHead appliances
- SteelHead Shaping Policy Paths

You can also clear the autocomplete cache.

Date and Time Formatting section

- **Date Style** - convention for displaying days, months, and years.
- **Time Style** - 12-hour or 24-hour time display.
- **Time Zone** - the default time zone for your user account. This time zone is used for all time displays and time inputs except on pages:
 - where it is overridden. You can specify a different time zone when scheduling a report, specifying a user-defined policy, or creating a new user account.
 - where system time of the appliance is used. System time is used on the Configuration > Security Profiles page and the Configuration > Flow Log Storage page.

Note: You can select a time zone using the Continent/City convention, the Country/Zone convention, or the time zone abbreviation. However, to ensure that the selected time zone is automatically adjusted for summer and winter time changes, it is preferable to select it using the Continent/City convention instead of the Country/Zone convention or its abbreviation.

You can display the time zone either by its name or as an offset from UTC. This time zone selection applies to only your user account. The appliance has its own system time zone setting.

Miscellaneous section

- **Non-interactive Connection Graph** - selects whether connection graphs and service maps allow users to rearrange the layout by dragging and dropping elements of the display.
- **Color Palette** - selects an alternate color scheme for graphs.
- **Refresh Rate** - specifies the rate at which to refresh the data on the GUI pages. One to ten minutes. The default is once per minute, which is the lowest rate.
- **Print/Email** - maximum number of rows for printed and emailed tables.
- **Packet Export from Sensor** - the maximum size of the file used to export a tcpdump-style file for a packet analysis report from the Sensor.

Selecting preferred interfaces

Device interfaces that are sending traffic information to NetProfiler can be designated “preferred.” Traffic statistics for preferred interfaces are precomputed and cached for quick access and display on the Home > Browse Preferred Interfaces page.

The System > Devices/Interfaces page Preferred Interfaces (List) tab controls the selection of preferred interfaces.

The Interfaces table lists all interfaces that are sending information to NetProfiler. For each interface, it lists the IP address and DNS name of the device and the index of the interface. If the interface has a name and description that NetProfiler can retrieve, the table lists those also.

The first time NetProfiler is started after being installed, it marks the first interfaces it receives data from as preferred interfaces, up to the limit for which its platform can reserve system resources. This is a one-time operation. The initial selections remain in effect until you change them.

You can select or deselect these markings in the Preferred column of the table. Select the interfaces whose statistics you want to be pre-computed and cached, and choose Apply.

If you have just updated from a version earlier than version 9.0, or if the appliance is receiving traffic information but no interfaces are listed on the Browse Preferred Interfaces page, ensure that storage space for Preferred Interfaces data has been specified on the Configuration > Flow Log page Disk Allocation tab.

Figure 2-2. System > Devices/Interfaces page - Preferred Interfaces tab

Devices/Interfaces ?

Devices & Interfaces (Tree) Interfaces (List) Devices (List) Synchronization (List) Preferred Interfaces (List)

Search by Device Address: Search

Interfaces 1 - 10 of 118 Select All: ☐

Device Address	Device Hostname	Index	Name (ifDescr)	Description (ifAlias)	Preferred
10.100.220.20	SW-DCCluster2	5	swport5	Access port for ESX Host, DCCluster2-EH5	<input checked="" type="checkbox"/>
10.100.220.20	SW-DCCluster2	2	swport2	Access port for ESX Host, DCCluster2-EH2	<input checked="" type="checkbox"/>
10.100.220.20	SW-DCCluster2	3	swport3	Access port for ESX Host, DCCluster2-EH3	<input checked="" type="checkbox"/>
10.100.220.20	SW-DCCluster2	4	swport4	Access port for ESX Host, DCCluster2-EH4	<input checked="" type="checkbox"/>
10.100.220.20	SW-DCCluster2	100	uplink0	Uplink to RTR-DataCenter	<input checked="" type="checkbox"/>
10.100.220.20	SW-DCCluster2	1	swport1	Access port for ESX Host, DCCluster2-EH1	<input checked="" type="checkbox"/>
10.100.220.10	SW-DCCluster1	100	uplink0	Uplink to RTR-DataCenter	<input type="checkbox"/>
10.100.220.10	SW-DCCluster1	2	swport2	Access port for ESX Host, DCCluster1-EH2	<input type="checkbox"/>
10.100.220.10	SW-DCCluster1	1	swport1	Access port for ESX Host, DCCluster1-EH1	<input type="checkbox"/>
10.100.220.10	SW-DCCluster1	4	swport4	Access port for ESX Host, DCCluster1-EH4	<input type="checkbox"/>

Account management

The Configuration > Account Management submenu options include:

- User Accounts
- Remote Authentication
- ODBC DB Access

User accounts

The Configuration > Account Management > User Accounts page allows those with Administrator privilege to add, audit, edit, enable, disable, delete and unlock user accounts and specify global settings affecting password requirements and login actions. This page does not list users who can log in to the appliance by having an account on a remote authentication server, instead of by having an account on the appliance.

Account role permissions

To protect the security of the appliance, Administrators should provide users with accounts having the permissions appropriate to their task responsibilities. NetProfiler and NetExpress provide five user accounts roles:

Figure 2-3. Configuration > Account Management > User Accounts page

User Accounts ?

Accounts New... Settings...

Username	Account Role	First Name	Last Name	Authentication	Authorization	Last Access	Timeout	Enabled	Actions
★ admin	Administrator			Local	Local	Jun 5, 2016 11:10:25 AM		Yes	Run Audit Trail report Edit Copy
demo	Administrator			Local	Local			Yes	Run Audit Trail report Edit Copy Delete Disable

1 go to page Show: 10 entries per page

- **Administrator** - Administrators set up the appliance on the network, set up user accounts, monitor the appliance status and usage, and perform backup operations. A user with an Administrator account can access all appliance functionality. Only those with Administrator accounts can specify mitigation actions, view the user activities log, grant users the ability to run user reports, specify global account settings, manage user accounts, and set passwords other than their own.
- **Operator** - Operators are responsible for the operational configuration of the appliance. This includes managing groups, alerting thresholds, event detection tuning, traffic reporting and event reporting. Operators can also modify the appliance network settings, allocate disk storage space for logs, and run vulnerability scans. However, they cannot specify mitigation actions, view the audit trail page, specify global account settings, or modify user accounts or other people's passwords.
- **Monitor** - Monitors check the Dashboard page for new events or unexpected activity. They can run traffic reports and view all Reports pages. They can also view the appliance status page. The only settings pages that Monitors can change are UI Preferences and Change Password. Typically, a user with a Monitor account is in a network operations center.
- **Dashboard Viewer** - Dashboard viewers can log in and view the displays on the Dashboard page. They cannot navigate away from the Dashboard page except to go to the UI Preferences and Change Password pages. Additionally, right-click menus and reporting links are not active for Dashboard Viewer accounts.
- **Event Viewer** - Event Viewers can use their log name and password to view an Event Detail report whose URL they have obtained from a network management system. They cannot take any actions on the event or navigate away from the Event Detail report.

Global account settings

User accounts are managed both globally and by user. Global account settings control password requirements and log in actions that apply to all users (except where they can be exempted on individual accounts).

On the Configuration > Account Management > User Accounts page, a user logged into an Administrator account can click **Settings** to display the Global Account Settings page. This page has three sections:

- **Password Requirements** – specifies password length, case usage, and requirement for non-alphabetic characters. Specifies the number (from 1 to 16) of previous passwords the appliance should save and test to ensure that the user is not recycling a small set of passwords. Also specifies the lifespan of a password. When a password expires, the user is forced to change it upon their next login.
- **Login Settings** – allows you to:
 - Limit the number of user sessions to one per name/password combination.
 - Require users of new accounts to change their password on their first log in.
 - Specify the number of consecutive failed login attempts the appliance allows before disabling logins for an account.
 - Specify how long logins are disabled on an account after the allowed number of failed login attempts has been exceeded. If a user needs access before the lockout period has expired, the Administrator can edit the account profile to specify a new password for the account.

Figure 2-4. Configuration > Manage Accounts > User Accounts > Settings page

Global Account Settings

Password Requirements

Minimum number of characters:	<input type="text" value="6"/>
<input type="checkbox"/> Require mixed case	
<input type="checkbox"/> Require non-alphanumeric characters	
Number of passwords to remember to prevent repeats:	<input type="text" value="1"/>
<input type="checkbox"/> Enable password aging	
Number of days before password expiration:	<input type="text" value="90"/>

Log-in Settings

<input type="checkbox"/> Allow only one log-in per user name/password combination	
<input type="checkbox"/> Force password change on first log-in	
Number of log-in attempts before account is locked:	<input type="text" value="3"/>
Number of minutes to keep an account locked:	<input type="text" value="30"/>
<input type="checkbox"/> Prevent user 'admin' from being locked out via DoS attack.	
Log-in splash screen display:	<input type="text" value="No splash screen"/>
Upload new log-in splash screen:	<input type="button" value="Browse..."/> No file selected.
Add login text:	<div style="border: 1px solid #ccc; height: 40px;"></div>

Inactivity Timeout

<input type="checkbox"/> Enable maximum inactivity timeout:	<input type="text" value="15"/> minute(s)
<input checked="" type="checkbox"/> Override timeout for auto-refreshing pages (status/dashboards).	

Changes will apply to all future account log-ins.
Currently logged-in accounts will need to log out before these changes apply.

OK

Cancel

- Exempt the admin account from being locked out by repeated unsuccessful login attempts. The “Prevent user 'admin' from being locked out via a DoS attack.” feature applies to only the factory-created admin account. It does not affect any user-created admin accounts.
- Specify if the splash screen is dismissed automatically after 5 seconds, is displayed until the user clicks **Acknowledge**, or is not displayed.
- Specify the path to a splash screen graphic file, such as a company banner in a gif, jpg, png or tiff file. NetProfiler uploads the file and saves it until it is overwritten by a subsequent splash screen file upload. The file can be up to 1 Megabyte in size. Additional file formats are also supported: aiff, jb2, jp2, jpc, jpf, pad, swc, swf, wbmp and xbm.
- Add text to be displayed to a user before they log in, such as an appropriate use statement.
- **Inactivity Timeout** – specifies how long an account can remain inactive before being automatically logged off.
 - This global setting can be overridden by a shorter time set for an individual user account, but not by a longer time.
 - When the appliance is in the Strict Security mode, this setting is automatically limited to no more than 10 minutes.

- The timeout can be overridden when the appliance is displaying the main pages used for monitoring the network.

Settings made on this page are linked to the settings made on the Configuration > Appliance Security > Password Security page.

Some of the settings on this page cannot be modified when the appliance is in the Strict Security mode.

New accounts

Administrators create new accounts by clicking New on the Configuration > Accounts page. The New User NetProfiler page has sections for specifying the user name, role, time zone and authentication method (local or remote). It also controls password characteristics. On this page you can exempt the user account from the strict password requirements that are defined on the Global Settings page. Additionally, you can grant the account permission to view user information where it appears in reports.

Figure 2-5. Configuration > Manage Accounts > User Accounts > New User Profile page

New User Profile

General

Username:	<input type="text"/>
Account Role:	Administrator ?
First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Time Zone:	America/New_York

Security

Authentication:	<input checked="" type="radio"/> Local <input type="radio"/> Remote
<input checked="" type="checkbox"/> Exempt from password requirements	
New password:	<input type="password"/>
Confirm password:	<input type="password"/>
<input type="checkbox"/> Force password change at next login	
<input type="checkbox"/> Enable inactivity timeout:	15 minute(s)

User Reporting

<input type="checkbox"/> Allow to view active directory user information in reports

OK Cancel

Security considerations

Administrators should consider the following when configuring the global account settings and creating user accounts:

- Create an account having only the permission level appropriate to the user's responsibilities.
- Follow your organization's guidelines for password composition and aging.
- Use the lowest inactivity timeout value practical for the user role.
- Require the user to change the password upon the first login.
- Do not enable database access unless the user requires external access to the appliance traffic information database.
- Do not enable User Reporting unless the user needs to identify other users by user name.

Remote authentication and authorization

The Configuration > Account Management > Remote Authentication page specifies the sequence in which NetProfiler and NetExpress check authentication sources when a user logs in. It also provides tabs for setting up RADIUS authentication and TACACS+ authentication.

Types of authentication and authorization

NetProfiler and NetExpress authenticate and authorize user logins in three ways:

- **Authenticated and authorized by NetProfiler or NetExpress** - The user has an account on NetProfiler or NetExpress. This account specifies their login credentials and their user role. If NetProfiler or NetExpress can authenticate their login credentials in its local user database, it logs them in and authorizes permissions based on the user role assigned to their account.
- **Authenticated remotely, authorized by NetProfiler or NetExpress** - The user has an account on NetProfiler or NetExpress. This account specifies their user role, but not their login credentials. It specifies that their credentials are to be authenticated remotely. If NetProfiler or NetExpress can authenticate their login credentials using a remote authentication server, it logs them in and authorizes permissions based on the user role assigned to their account.
- **Authenticated and authorized remotely** - The user does not have an account on NetProfiler or NetExpress. When the user attempts to log in, NetProfiler or NetExpress uses a remote authentication server to both authenticate their login credentials and authorize permissions based on their user role.

NetProfiler and NetExpress can use RADIUS and TACACS+ authentication servers.

Authentication sequence

NetProfiler and NetExpress always check their local database first to authenticate a user's login credentials. If they cannot authenticate the user locally, they attempt to authenticate the credentials using the protocol specified in the Authentication Sequence section of the page.

You can specify that NetProfiler or NetExpress are to check RADIUS servers or TACACS+ servers, or first one and then the other, or neither (that is, use only local authentication).

The appliance attempts to contact the first authentication server in its list. If that server is unreachable, it checks the next authentication server in the list. It continues until it succeeds in connecting to an authentication server.

When searching for RADIUS authentication, the appliance contacts RADIUS servers in the order in which they are listed on the RADIUS tab. When searching for TACACS+ authentication, the appliance contacts TACACS+ servers in the order in which they are listed on the TACACS+ tab.

When it succeeds in connecting and receives a valid message back from an authentication server, NetProfiler or NetExpress stops searching for authentication servers, regardless of whether the message is a pass/success or a “user not found” or other failure message. If authentication and authorization succeed, the appliance logs the user in. If either authentication or authorization fail, the appliance displays an error message and records an unsuccessful login attempt in the audit logs.

RADIUS authentication

RADIUS authentication is configured on the RADIUS tab of the Configuration > Account Management > Remote Authentication page. Configuring NetProfiler or NetExpress to use RADIUS involves:

- **Global Settings** - Click Settings and specify the global RADIUS settings. These apply to all RADIUS servers that NetProfiler or NetExpress connects to.
- **Specifying RADIUS servers** - Specify the IP address, port number, authentication protocol and shared secret of each RADIUS server that NetProfiler or NetExpress is to use for authenticating users.

- Mapping roles to authorization attributes - For users who have no account on the appliance, map the NetProfiler or NetExpress user roles to RADIUS authorization attributes.

Global settings

On the RADIUS tab of the Configuration > Account Management > Remote Authentication page, click **Settings** to open the Global RADIUS Settings page.

Figure 2-6. Global RADIUS Settings page

Global RADIUS Settings

Authentication

Select NAS-Identifier and/or NAS-IP-Address to be sent to RADIUS Servers

☒ Send NAS-Identifier as part of Authentication Request

☐ Use custom NAS-Identifier:

☒ Use the hostname of the SteelCentral NetProfiler Virtual Edition as a NAS-Identifier

☐ Send NAS-IP-Address as part of Authentication Request

Connection

Connection timeout: seconds

Max number of tries:

OK

Cancel

A RADIUS server sees the NetProfiler or NetExpress as being a Network Access Server (NAS). You can specify that the appliance is to send a NAS-Identifier or NAS-IP-Address with the authentication request.

You can also specify the number of seconds that the appliance waits for a connection attempt to succeed and the number of times it tries to connect to the RADIUS server before moving on to the next server in the list.

Specifying RADIUS servers

You can specify multiple RADIUS servers. NetProfiler or NetExpress tries to connect to each RADIUS server in the order in which it is listed. It sends an authentication request to the first RADIUS server it is able to connect to. Authentication requests include the information specified in the global RADIUS settings.

To specify a RADIUS server:

1. Go to the Configured Servers section of the RADIUS tab of the Configuration > Account Management > Remote Authentication page.
2. Enter the server information. (The shared secret is provided by the RADIUS server administrator.)
3. Select **Enabled** for the NetProfiler or NetExpress to use the server.
4. Click **Add**. This adds the server to the list.
5. Click the **Test** link in the Actions column for the entry to verify that NetProfiler or NetExpress can connect to the server. A message box reports the results of the connection attempt.

Server entries can be enabled, disabled, edited, deleted, and tested.

Figure 2-7. Configuration > Account Management > Remote Authentication > RADIUS tab

Remote Authentication ?

Authentication Sequence

The order of primary and fallback authentication methods: Local, RADIUS, TACACS+

Edit

RADIUS
TACACS+

Configured Servers

Settings...

Order	Address	Port	Authentication Protocol	Shared Secret	Enabled	Actions
		1812	PAP		<input type="checkbox"/>	Add

Roles-Attributes Mapping

Edit

Test User

Local Role/Permission	Type	RADIUS Attribute/Value
Administrator	role	
Operator	role	
Monitor	role	
Event Viewer	role	
Dashboard Viewer	role	
Allow to view active directory user information	permission	

Mapping roles to authorization attributes

Users who do not have a NetProfiler or NetExpress account must have both their authentication information (login name, password) and their authorization information (user role indicated by the value of the Class attribute or the Cascade-User-Role attribute) specified on the RADIUS server. The values of the RADIUS authorization attributes must be mapped to their corresponding user roles on NetProfiler or NetExpress.

Ensure that you know which authorization attributes the RADIUS administrator is using and what values may be assigned to them. The values on the RADIUS server and the values on NetProfiler or NetExpress must match for the user to be logged on.

To map the NetProfiler or NetExpress user roles to RADIUS authorization attributes:

1. Click **Edit** in the Roles-Attributes Mapping section of the RADIUS tab of the Configuration > Account Management > Remote Authentication page.
2. For the first user role, click **Add new attribute** to display an edit box.
3. Select the RADIUS authorization attribute (Class or Cascade-User-Role).
4. Enter the value of the attribute that is required for a RADIUS-authorized user to be logged on in this user role.
5. If applicable, click **Add new attribute** to add another mapping.
6. Continue with the next user role that is to be authorized by RADIUS.
7. When the RADIUS authorization attributes have been mapped to their corresponding NetProfiler user roles, click **Save**.
8. If desired, click **Test User** to open a page on which you can specify a user name and password to be tested. When you click **Run** on this page, NetProfiler attempts to log the user in using RADIUS authentication and reports the test results.

A user who does not have a NetProfiler or NetExpress account logs in by entering the login name and password that are specified on the RADIUS server. NetProfiler or NetExpress sends this information to the RADIUS server in an authentication and authorization request.

If the RADIUS server can authenticate the user's login name and password, it sends a "request accepted" code back to NetProfiler or NetExpress, along with the authorization attribute value. The authorization attribute value is a string that the RADIUS administrator assigns to the RADIUS Class attribute or to the Cascade-User-Role attribute for the user.

The NetProfiler or NetExpress administrator must also assign this same value to the corresponding attribute definition in the Configuration > Account Management > Remote Authentication page RADIUS tab Role-Attribute Mapping section.

When NetProfiler or NetExpress finds a match between the RADIUS definition of the authorization attribute and its own definition of the attribute, it logs the user on to the appliance and authorizes the matching user role. If no match is found, then the login attempt fails.

When NetProfiler or NetExpress logs the user on, it automatically creates an account for the user. However, subsequent logins by the RADIUS user do not create multiple NetProfiler or NetExpress accounts for the user.

Vendor-specific RADIUS attributes

Riverbed provides a RADIUS dictionary file containing the definitions of vendor-specific attributes for use with Riverbed appliances. This definition is identified to the RADIUS server by the vendor name RBT and the vendor number 17163. The definition identifies the vendor-specific attributes as Cascade-User-Role and Local-User. The Cascade-User-Role attribute is for use with Riverbed NetProfiler products. The Local-User attribute is for use with Riverbed SteelHead appliances. The product does not support mapping the Local-User attribute value to NetProfiler user roles.

Depending on which RADIUS server you are using, you can either enter these attribute definitions on a GUI page or else copy and paste them from the dictionary.rbt file, which you can download from the downloads page of the on line help system.

TACACS+ authentication

TACACS+ authentication is configured on the TACACS+ tab of the Configuration > Account Management > Remote Authentication page. Configuring NetProfiler or NetExpress to use TACACS+ involves:

1. Global settings - Click **Settings** and specify the global TACACS+ settings. These apply to all TACACS+ servers that the appliance connects to.
2. Specifying TACACS+ servers - Specify the IP address, port number, authentication protocol, shared secret and client port of each TACACS+ server that NetProfiler or NetExpress is to use for authenticating users.
3. Mapping roles to authorization attributes - For users who have no account on NetProfiler or NetExpress, map the appliance user roles to TACACS+ authorization attributes.

Global settings

On the TACACS+ tab of the Configuration > Account Management > Remote Authentication page, click **Settings** to open the Global TACACS+ Settings page.

Specify the TACACS+ service under which authorization roles/flags will be found on the TACACS+ server. The service must be configured on the TACACS+ server for TACACS+ authorization to work. Check with the TACACS+ server administrator if you need a service defined exclusively for NetProfiler or NetExpress users.

You can also specify the number of seconds that NetProfiler or NetExpress waits for a connection attempt to succeed before moving on to the next server in the list.

Figure 2-8. Global TACACS+ Settings page

Global TACACS+ Settings

Authorization

Service under which authorization roles/flags will be found:

Connection

Connection timeout: 5 seconds

OK Cancel

Specifying TACACS+ servers

You can specify multiple TACACS+ servers. NetProfiler or NetExpress tries to connect to each TACACS+ server in the order in which it is listed. It sends an authentication request to the first TACACS+ server it is able to connect to. The first TACACS+ server to provide a valid pass/fail response ends the search. Authentication requests include the information specified in the global TACACS+ settings.

Figure 2-9. Configuration > Account Management > Remote Authentication > TACACS+ tab

Remote Authentication

Authentication Sequence

The order of primary and fallback authentication methods: Local, RADIUS, TACACS+ Edit

RADIUS **TACACS+**

Configured Servers Settings...

Order	Address	Port	Authentication Protocol	Shared Secret	Client Port	Enabled	Actions
		49	PAP			<input type="checkbox"/>	Add

Roles-Attributes Mapping Edit Test User

Local Role/Permission	Type	TACACS+ Attribute/Value
Administrator	role	
Operator	role	
Monitor	role	
Event Viewer	role	
Dashboard Viewer	role	
Allow to view active directory user information	permission	

To specify a TACACS+ server:

1. Go to the Configured Servers section of the TACACS+ tab of the Configuration > Account Management > Remote Authentication page.
2. Enter the server information. This is normally provided by the TACACS+ server administrator.
The Client Port field specifies the TACACS+ protocol client port used on the Network Access Server (NAS). Leave this field empty unless the TACACS+ server administrator asks you to specify a port.
3. Select **Enabled** for the NetProfiler or NetExpress to use the server.

4. Click **Add**. This adds the server to the list.
5. Click the **Test** link in the Actions column for the entry to verify that the NetProfiler or NetExpress can connect to the TACACS+ server. A message box reports the results of the connection attempt.

Server entries can be enabled, disabled, edited, deleted, and tested.

Mapping roles to authorization attributes

Users who do not have a NetProfiler or NetExpress account must have both their authentication information (login name, password) and their authorization information specified on the TACACS+ server. The values of the TACACS+ authorization attributes must be mapped to their corresponding user roles on NetProfiler or NetExpress.

Ensure that you know which authorization attributes the TACACS+ administrator is using and what values may be assigned to them. The values on the TACACS+ server and the values on NetProfiler or NetExpress must match for the user to be logged on.

To map the NetProfiler or NetExpress user roles to TACACS+ authorization attributes:

1. Click **Edit** in the Roles-Attributes Mapping section of the TACACS+ tab of the Configuration > Account Management > Remote Authentication page.
2. For the first NetProfiler or NetExpress user role, click **Add new attribute** to display an edit box.
3. Enter the TACACS+ authorization attribute.
4. Enter the value that is required for a TACACS+ authorized user to be logged on in this user role. This attribute/value pair must be defined on the TACACS+ server under the service that is specified on the NetProfiler Global TACACS+ Settings page.
5. If applicable, click **Add new attribute** to add another mapping.
6. Continue with the next NetProfiler or NetExpress user role that is to be authorized by TACACS+.
7. When the TACACS+ authorization attributes and values have been mapped to their corresponding NetProfiler or NetExpress user roles, click **Save**.
8. If desired, click **Test User** to open a page on which you can specify a user name and password to be tested. When you click **Run** on this page, NetProfiler attempts to log the user in using TACACS+ authentication and reports the test results.

A user who does not have a NetProfiler or NetExpress account logs in by entering the login name and password that are specified on the TACACS+ server. NetProfiler or NetExpress sends this information to the TACACS+ server in an authentication and authorization request.

If the TACACS+ server can authenticate the user's login name and password, it sends a "request accepted" code back to NetProfiler or NetExpress, along with the authorization attribute value.

This value must be specified in the Configuration > Account Management > Remote Authentication page TACACS+ tab Role-Attribute Mapping section.

When NetProfiler or NetExpress finds a match between the TACACS+ definition of the authorization attribute and the NetProfiler or NetExpress definition of the attribute, it logs the user on to the appliance and authorizes the matching user role. If no match is found, then the login attempt fails.

When NetProfiler or NetExpress logs the user on, it automatically creates an account for the user. However, subsequent logins by the TACACS+ user do not create multiple NetProfiler or NetExpress accounts for the user.

ODBC DB Access

The Configuration > Account Management > ODBC DB Access page lists user accounts that have been created for accessing the internal database. These accounts are typically used by scripts or programs that other systems use to retrieve information from the internal NetProfiler or NetExpress database.

Use this page to delete an existing database user account or to add a new one.

When the NetProfiler or NetExpress is in the Strict Security mode, database access is disabled and this page is not displayed.

Figure 2-10. Configuration > Account Management > ODBC DB Access page

OAuth Access

OAuth Access Codes						Generate new
Username	Issued 	Client IP	Expires	Last Access	Description	Actions
No Data Available.						

Passwords

All users except Event Viewers and Administrators can change their own passwords on the Configuration > Change Password page. Administrators can replace the password on any account by using the Configuration > Account Management > User Accounts > Edit feature. Therefore, the Change Password page is not displayed on Administrator accounts.

Figure 2-11. Configuration > Change Password page

Change password for mon

Current password:	<input type="password"/>
New password:	<input type="password"/>
Re-type new password:	<input type="password"/>
	<input type="button" value="Change"/> <input type="button" value="Cancel"/>

Integration

The integration features are accessed from the Configuration > Integration menu. Integration is described in [Chapter 5, “Enterprise Integration.”](#)

Mitigation

The mitigation features are accessed from the Configuration > Mitigation menu. Mitigation is described in [Chapter 14, “Mitigation.”](#)

Flow log

The Configuration > Flow Log pages include two tabs:

- **Disk Allocation** - specifies how the appliance uses disk space to store traffic flow data at various data resolutions. You can reallocate disk space usage. This tab also indicates when the storage space allocated to flow logs for a particular data resolution can be rebalanced to retain the information for a longer period of time.
- **Reporting** - specifies the reporting time frames at which the appliance automatically switches from using one data resolution to using another data resolution.

Flow log disk space allocation

The Configuration > Flow Log page Disk Allocation tab displays how NetProfiler disk storage is being used to store traffic flow information. The flow logs make it possible to quickly report on historical traffic flows with data resolutions of 1 minute, 5 minutes, 15 minutes, 1 hour, 6 hours, and 1 day. When viewing historical trends, you can use a lower data resolution to view a longer time span conveniently. When investigating specific behavior, you can use higher resolution for a higher degree of accuracy.

Figure 2-12. Configuration > Flow Log page Disk Allocation tab

Flow Log

Disk Allocation

Reporting

The table below shows the current disk allocation and estimated retention period for each log resolution. The log start and end times show the actual time range available, which may be less than the full retention period for newly installed systems.

Current system time: **Sunday, June 5, 2016 12:02 PM EDT (America/New_York)**.

Current Flow Log Status

Rebalance...

Reallocate...

Resolution	Disk Allocation	% of Total	Retention	% Used	Log Start Time	Log End Time	Status
Flow	83.0 GB	40.00%	1 month 2 weeks	20.1%	May 26, 2016 8:56 AM	Jun 5, 2016 11:58 AM	OK
1 minute	41.5 GB	20.00%	3 days 15 hours	81.5%	Jun 1, 2016 8:42 PM	Jun 5, 2016 11:57 AM	Rebalance to achieve 1 week 3 hours
5 minutes	20.7 GB	10.00%	2 days 15 hours	76.7%	Jun 2, 2016 6:45 PM	Jun 5, 2016 11:55 AM	Rebalance to achieve 5 days 18 hours
15 minutes	2.6 GB	1.25%	11 hours 1 minute	84.7%	Jun 4, 2016 11:30 PM	Jun 5, 2016 11:45 AM	Rebalance to achieve 1 day 1 minute
1 hour	10.4 GB	5.00%	3 days 23 hours	64.0%	Jun 1, 2016 11:00 AM	Jun 5, 2016 11:00 AM	Rebalance to achieve 1 week 1 day
6 hours	5.2 GB	2.50%	4 days 6 hours	64.5%	Jun 1, 2016 12:00 AM	Jun 5, 2016 6:00 AM	Rebalance to achieve 1 week 1 day
1 day	2.6 GB	1.25%	5 days 17 minutes	57.2%	May 31, 2016 12:00 AM	Jun 5, 2016 12:00 AM	Rebalance to achieve 1 week 2 days
Preferred Interfaces	41.5 GB	20.00%	1 month 2 weeks	22.5%	May 26, 2016 8:00 AM	Jun 5, 2016 11:58 AM	OK
Total	207.5 GB	100%	1 month 2 weeks	43.10%	May 26, 2016 8:00 AM	Jun 5, 2016 11:58 AM	

Rebalancing is recommended when the log for a given resolution is not efficiently using the disk space allocated for it. The operation of rebalancing temporarily stops flow logging, thus should be performed during scheduled down times.

The tab displays the percent of total disk storage capacity that is allocated to the various flow logs. It also shows how long a period of time the flow data for each data resolution can be retained, using the current allocation, before being overwritten with newer data. By default, NetProfiler allocates approximately half its disk storage space to the highest resolution flow logs. It allocates the remaining disk space among the flow logs for the other data resolutions and to storing pre-computed data for Preferred Interfaces reporting.

You can modify the allocations. For example, if you do not anticipate wanting to run reports for time spans of more than 6 months, then you might want to reduce the allocation for the flow logs with 1-day data resolution and reallocate that space to the logs for 15-minute data resolution. This would allow NetProfiler to store a longer history of data with a 15-minute resolution.

The amount of space allocated for Preferred Interfaces data along with the number of interfaces selected as “Preferred” determines the amount of historic pre-computed data that can be retained.

Caution on allocating zero disk space

If you set the disk space allocation for a data resolution interval to 0 GB or less than 0.1%, that data resolution will no longer be available for selection on the Report Criteria section of traffic reports. This is not user-reversible. It will require assistance from Riverbed Support to restore the log for that data resolution interval.

Additionally, if you set the disk space allocation for a 1-minute data resolution interval to less than 0.1%, it triggers a system restart, which may take the system down for tens of minutes, as well as require assistance from Riverbed Support to restore.

These considerations do not apply to the Preferred Interfaces data storage allocation. Changing the Preferred Interfaces allocation from a non-zero number to zero causes all pre-computed Preferred Interfaces data to be deleted and stops storing any new Preferred Interfaces data. However, you can subsequently allocate storage space for pre-computed Preferred Interfaces data and the data will start being stored again, without requiring assistance from Riverbed Support.

Flow log disk space balancing

The flow log for each data resolution contains information about all network behavior that the appliance tracks. For example, the flow log for reporting with 15-minute data resolution contains traffic statistics for each host pair, interface, etc. during each 15-minute interval that the log covers. It also contains information about each application, port, and protocol in use during each 15-minute interval it covers.

Depending on the characteristics of your network, the appliance may need more storage space for one attribute of network behavior, such as host pair traffic, than for another attribute, such as interfaces.

The length of time that a flow log can cover is limited to the disk space required for storing the attribute that requires the most space. So the retention times displayed on the Disk Allocation tab depend on the balance among the many types of information the flow logs are storing.

The appliance monitors how well the space allocated to each flow log is being utilized. When it finds that some types of information are consuming much less or much more disk space than other types, it notifies you that it can increase the retention time of the log by rebalancing how the log's disk space allocation is being used.

Rebalancing a flow log does not affect the amount of disk space allocated to the log. It just optimizes the use of the allocated space based on the behavior of your network. This allows you to get a longer retention time out of the same amount of disk space.

If the balance of activities on your network changes over time, the appliance detects this and notifies you that flow logs should be rebalanced.

Reporting time frames

The Configuration > Flow Log page Reporting tab allows you to customize the automatic data resolution feature.

When you specify a traffic report, the “Data resolution” box in the Report Criteria section of the report page has a drop-down list box that lists all the data resolution intervals that are available. It also has a choice for automatic data resolution. When you choose automatic, the appliance uses the data resolution that corresponds to the time frame of the report. This correspondence is specified on the Configuration > Flow Log page Reporting tab.

Figure 2-13. Configuration > Flow Log page Reporting tab

Flow Log ?

Disk Allocation | **Reporting**

When you select 'automatic' for data resolution ? in a report, a resolution will automatically be selected based on time frame of the report. The table below allows customizing which resolutions are selected based on the time frame of the report.

For example, if you set the minimum timeframe for the 15 minute resolution to be 10 hours and the 1 hour resolution to be 3 days, this means that a report that covers less than 10 hours, but less than 3 days, will show data grouped in 15 minute intervals.

Please note that these timeframes are only 'hints' to NetProfiler. If NetProfiler determines that the timeframe for your report is better covered by another resolution, it may use that instead.

Configure timeframes for 'automatic' data resolution

Resolution	Minimum Timeframe
1 minute	1 Minutes
5 minutes	20 Minutes
15 minutes	2 Hours
1 hour	8 Hours
6 hours	2 Days
1 day	2 Weeks

Apply Timeframes

Specify the report time frame at which you want the NetProfiler to start using a particular data resolution and click **Apply Time Frames**. NetProfiler applies your new specifications and displays a confirmation message.

The default settings for the minimum reporting time frame for each data resolution are:

Data Resolution	Time Frame
1 minute	1 minute
5 minute	20 minutes
15 minutes	2 hours
1 hour	8 hours
6 hours	2 days
1 day	2 weeks

Packet capture (NetExpress only)

The NetExpress includes packet capture and packet export features. You can define capture jobs and export packet capture (pcap) files just as you would on a NetShark appliance. The packet capture files can be analyzed by Wireshark or Packet Analyzer software. Additionally, the Packet Analyzer can connect to the NetExpress just as it would connect to a NetShark. It cannot access the NetExpress web user interface and define capture jobs. But otherwise, the NetExpress performs the same capture functions as the NetShark. This feature is not available on CAX360 models.

Use the Configuration > Packet Capture page to add, edit, start, stop, view, clear and remove capture jobs and to export packet capture (pcap) files for analysis.

Figure 2-14. Configuration > Packet Capture page

Packet Capture

Capture Job Summary

Job Name	Interface	Status	Size	Actions
Sagar_Test	mon0_0	RUNNING	4.33 MB	View Stop

Add A New Job

Adding a capture job

To add a capture job,

1. Go to the Configuration > Packet Capture page and click **Add New Job**.

Figure 2-15. Configuration > Packet Capture > Add Capture Job page

Add New Job

Capture Settings

Name:

Status: **Stopped**

Interface:

mon0_0

(NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

☒ Enable Indexing

☐ Enable DPI

☒ Start new job immediately

Retention Settings

Data Retention
Start / Stop Settings

Packet Data (Packet Storage Total Space: 3.63 TB, Unallocated Space: 2.54 TB)

Packet Retention Size: TB % Of Disk

Additional Retention Criteria:
☐ Packets

☐ Seconds

Microflow Index (User Data Storage Total Space: 445.24 GB, Unallocated Space: 434.07 GB)

Retain Index On Disk Up To: GB % Of Disk

Additional Retention Criteria:
☐ Days

☐ Synchronize With Packet Recording

Note: Packets are stored in specially formatted packet storage. Indexes are stored in the conventional User Data Storage.

Save Cancel

2. On the Add New Job page, enter a name for the capture job.
3. Select the network interface that is seeing the traffic that the job is to capture. The Interface list box identifies all interfaces that are available. See the note below for an explanation of network monitoring interface naming.

4. If desired, specify a BPF filter. A BPF filter can select a subset of network traffic for capturing. For example, the filter `src host 192.168.43.17` captures only packets with a source address of 192.168.43.17. Leave this box empty to capture all packets. You can find more information on BPF filters at <http://wiki.wireshark.org/CaptureFilters>.

A filter specified in this section applies to only the capture job. It does not filter the traffic that the NetExpress reports on the reporting pages.

5. Specify the maximum number of bytes of each packet to capture. Specify 65535 to capture the entire packet.
6. Select the **Start new job immediately** option to place the job into the Running state as soon as you click **Save** at the bottom of the page. Deselect this option if you want to start the job manually.

The status of a new capture job is shown as Stopped until the job is started. Once you start it, its status is Running. You can delay the start of a capture job by specifying a start time on the Start/Stop tab.

7. Click **Save** to accept the default data retention and start/stop settings and start the capture job. Alternatively, adjust the settings and then click **Save**. See the notes below about Data Retention and Start/Stop settings.

Monitoring network interface naming

NetExpress

The names and positions of the monitoring interface connectors are indicated on a sticker on the top of the chassis. The four built-in copper interfaces are named `mon0_0`, `mon0_1`, `mon0_2` and `mon0_3`.

If your NetExpress has a 2-port 10G fiber network interface card installed in traffic monitoring Slot 1, its interfaces are named `mon1_0` and `mon1_1`. If it is installed in traffic monitoring Slot 2, its interfaces are named `mon2_0` and `mon2_1`.

A virtual interface named `mon_tcap` is also available. This provides an aggregation of all physical interface traffic, including the built-in interfaces and, if present, the optional interface card traffic.

The `mon_tcap` virtual interface and all the monitoring interfaces are listed on the Interfaces drop-down list in the Capture Settings section of the page. You can define a capture job to use any interface in the list.

NetExpress virtual edition

The Configuration > Packet Capture page of the NetExpress virtual edition works the same as that of the NetExpress, except that the monitoring interfaces are labeled `Mon0`, `Mon1`, `Mon2` and `Mon3` and the `mon_tcap` aggregation interface is not present on the virtual edition. The interfaces are listed on the Interfaces drop-down list in the Capture Settings section of the page. You can define a capture job to use any interface in the list.

Data Retention tab

The Packet Data section of the Data Retention tab specifies the limits of captured packet storage in terms of size, percent of disk space, number of packets, and seconds of data. When the most constraining limit is met, the oldest data is discarded to make space for the newest data. Changing the packet capture storage settings on this page has no effect on the settings for flow data storage specified on the Configuration > Flow Log page.

The Microflow Indexing section of the tab specifies limits for the storage of Microflow indexes. Microflow Indexing captures summary information about conversations between devices on the network. This information is all that is needed by the Packet Analyzer software to calculate many of the View metrics that describe the traffic stream. Because it is already in summary form, processing of Microflow Indexing data for View metrics is very fast.

If you will be connecting to the NetExpress from Packet Analyzer, enable Microflow indexing. If you will be using the NetExpress packet capture feature only to export pcap files, disable Microflow indexing to reduce the processing load on the system.

Enabling Microflow indexing on the Data Retention tab disables the Start/Stop tab. Refer to the Packet Analyzer documentation for more information about Microflow indexing.

Start/Stop tab

The Start/Stop tab specifies the starting time and stop time of the capture job using the MM/DD/YYYY HH:MM:SS format to specify times that are local for your web browser session. You can also specify stop criteria in terms of the Microflow index file size, the percent of disk space consumed, the number of packets saved to packet storage, or the number of seconds of packet data that have been saved. The capture job stops when the stop time or any of the stop rule criteria are met.

Managing capture jobs

Once a capture job has been created, it can be started, stopped, viewed, edited, cleared and removed on the Configuration > Packet Capture page. Which operations are available on the Packet Capture page depends on whether the job is running or stopped.

Figure 2-16. Configuration > Packet Capture page

Packet Capture

Capture Job Summary				
Job Name	Interface	Status	Size	Actions
New Job 1	mon0	STOPPED	140.62 GB	Edit Start Clear Remove
New Job 2	mon0	STOPPED	0 B	Edit Start Clear Remove
Add A New Job				

Operations on a Running capture job

The status of a capture job can be Running or Stopped. A job that is running can be viewed or stopped, but not edited, cleared or removed. To view a running job, click either the name of the job or the **View** button. This opens the Job Details page.

The Job Details page displays the capture settings and also the statistics for the capture job at the time you opened the page. The statistics include:

- Start and end time of the job (Start Packets and End Packets respectively)
- Current size of the capture job on the disk
- Current size of the Microflow Index file on the disk (if enabled)
- Number of packets captured in the last second, last minute and last hour
- Number of packets dropped if the NetExpress could not capture all of them

The Job Details page for a running job cannot be edited. Only the Packet Export tab is active.

Figure 2-17. Configuration > Packet Capture > View - Running Job Details page

Job Details: Sagar_Test*Note: Settings on running jobs may not be modified.*

Capture Settings

Name:

Status: **RUNNING**

Interface: (NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

☒ Enable Indexing

☒ Enable DPI

Statistics

Start Packets: 6/1/2016 17:07:08 (-0400)

End Packets: 6/6/2016 15:49:22 (-0400)

Packet Capture Size: 4.34 MB

Microflow Index Size: 2.87 MB

Packets	Last Second	Last Minute	Last Hour
Written:	0	8	480
Dropped:	0	0	0

Retention Settings

Data Retention

Start / Stop Settings

Packet Export

Start Export: ☒ From Beginning Of Job

☐ From Start Time:

Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0400.

End Export: ☒ At End Of Job

☐ At End Time:

Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0400.

☐ When export file size is bytes

☐ When export file contains packets

Export File Format & Timestamp Resolution: ☒ pcap (microsecond)

☐ pcap (nanosecond)

☐ pcap-ng (microsecond)

☐ pcap-ng (nanosecond)

Limit Each Packet To: ☒ No Limit

☐ Bytes

Operations on a Stopped capture job

A job that is stopped can be started, edited, cleared or removed. To edit a stopped job, click either the name of the job or the **Edit** button. This opens the Job Details page.

Figure 2-18. Configuration > Packet Capture > Edit - Stopped Job Details page

Job Details: New Job 1

Capture Settings

Name:

Status: **STOPPED**

Interface:
(NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

☒ Enable Indexing

☒ Enable DPI

Statistics

Start Packets: 5/26/2015 11:13:49 (-0400)

End Packets: 9/17/2015 12:34:40 (-0400)

Packet Capture Size: 140.62 GB

Microflow Index Size: 0 B

Packets	Last Second	Last Minute	Last Hour
Written:	0	0	0
Dropped:	0	0	0

Retention Settings

Data Retention

Start / Stop Settings

Packet Export

Packet Data (Packet Storage Total Space: 3.63 TB, Unallocated Space: 1.45 TB)

Packet Retention Size: TB % Of Disk

Additional Retention Criteria: ☐ Packets
☐ Seconds

Microflow Index (User Data Storage Total Space: 292.83 GB, Unallocated Space: 270.49 GB)

Retain Index On Disk Up To: GB % Of Disk

Additional Retention Criteria: ☐ Days
☐ Synchronize With Packet Recording

Note: Packets are stored in specially formatted packet storage. Indexes are stored in the conventional User Data Storage.

The Job Details page displays the capture settings and also the statistics for the capture job at the time you opened the page. All the fields are active, so you can edit the capture settings, retention settings and start/stop settings. You can also export the packet capture to a pcap file.

A stopped job can be cleared or removed by clicking the **Clear** or **Remove** button on the Configuration > Packet Capture page. The Clear operation deletes all the capture data, but leaves the capture job available in the job list to be started again. The **Remove** operation deletes the capture data and also deletes the definition of the capture job. The job is deleted from the job list and no longer available.

Exporting a packet capture file

Data from a capture job can be exported to a pcap file from the Job Details page of either a running job or a stopped job.

Packet data can also be exported from a report by using the right-click menu. Refer to [“Analyzing packet information with Packet Analyzer”](#) in [Chapter 13, “Reporting”](#) for information about exporting data about specific traffic flows to pcap files.

Figure 2-19. Exporting Packet Capture files

The screenshot shows the 'Packet Export' configuration tab. It includes the following sections and options:

- Start Export:**
 - ☒ From Beginning Of Job
 - ☐ From Start Time: 5/26/2015 11:13:49
 - Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0400.*
- End Export:**
 - ☒ At End Of Job
 - ☐ At End Time: 9/17/2015 12:34:40
 - Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0400.*
 - ☐ When export file size is 134217728 bytes
 - ☐ When export file contains 1000000 packets
- Export File Format & Timestamp Resolution:**
 - ☒ pcap (microsecond)
 - ☐ pcap (nanosecond)
 - ☐ pcap-ng (microsecond)
 - ☐ pcap-ng (nanosecond)
- Limit Each Packet To:**
 - ☒ No Limit
 - ☐ 65535 Bytes

At the bottom, there are two buttons: 'Prepare Export URL' and 'Download Packets Now'.

To export capture job data to a pcap file,

1. Go to the Configuration > Packet Capture page and select the capture job.
2. Select the **Packet Export** tab.
3. Specify the start and end of the export. See the notes below.
4. Specify the export file format and time stamp resolution. See the notes below.
5. Click either **Prepare Export URL** or **Download Packets Now**. See the notes below.

Start Export

From Beginning of Job - The export starts with the earliest data available in the capture job.

From Start Time - Specify a time that is local to the web browser session you are using to access the page. The note under this field displays the offset from UTC time.

End Export

End of Job - If the job is stopped, then the export ends with the last data available when the job was stopped. If the job is still running, then the export ends at the present time.

At End time - Specify a time that is local to the web browser session you are using to access the page. The note under this field displays the offset from UTC time.

After - The export includes only enough data to reach the specified byte or packet count.

Export File Format and Timestamp Resolution

If you will analyze the file with Packet Analyzer or Wireshark, select the format you want to export. If you will analyze the file with other software, use the default setting of **pcap (microsecond)**.

Prepare Export URL

Click this button to display a URL from which the pcap file can be downloaded.

Download Packets Now

Click this button to download the pcap file to your local machine.

SSL decryption (NetExpress only)

The NetExpress SSL decryption feature enables SteelCentral™ Packet Analyzer users to view metrics for encrypted traffic. When a Packet Analyzer uses NetExpress as a probe, the feature decrypts the traffic that is encrypted in one or more TCP connections established between one or more web clients and a web server.

If a user is interested in analyzing the encrypted traffic between a web server and its clients, the user copies the RSA private key used by the web server along with any necessary decryption of the key, installs it in NetExpress, and associates it with the IP address and TCP port that the web server is using. When the Packet Analyzer user applies a web view, NetExpress attempts to match the IP address and port number specified in the view with an IP address and port number that NetExpress has associated with an encryption key. If it finds a match, it uses the key to decrypt the specified traffic. Then it derives the traffic metrics for the view and sends them to the Packet Analyzer.

Access to the NetExpress decryption feature can be limited to Packet Analyzer users who have an Administrator account on NetExpress or it can also be granted to those with an Operator account.

For each link that is to be decrypted, the Configuration > SSL Decryption page must specify:

- IP address and TCP port of the HTTPS server
- Private key in PEM format (associated certificate is optional)
- Password, if the private key is encrypted
- Type of account on NetExpress (Operator or Administrator) that a Packet Analyzer user must have in order to use NetExpress as a probe for the encrypted link
- Description; a short string for identifying the key in the list

Requirements

- SSL/TLS versions:
 - SSL v2
 - SSL v3
 - TLS 1.0
 - TLS 1.1
 - TLS 1.2 (limited to AES CBC cyphers)

- Private Keys:
 - Type: RSA
 - Format: PEM
 - PKCS#1
 - PKCS#8
 - Plain text or password encrypted
 - Supported key lengths (bits): 128, 256, 512, 1k, 2k, 4k, 8k
 - Maximum length: 8192 bits
 - Maximum number of keys: 512
- NetExpress must see the full initial RSA handshake. Only the RSA handshake is supported. Diffie Hellman and Elliptical Curves are not supported.
- One key can be associated with multiple server IP address/port pairs. However, NetExpress does not support more than one key associated with the same server IP address/port pair.

Security considerations

HTTPS packets are decrypted, parsed, and temporarily stored in memory. Decrypted packets are never stored on disk or sent outside NetExpress. If packet captures of encrypted data are sent to Packet Analyzer, Wireshark, SteelCentral™ AppResponse or a file, the packets are not decrypted.

When importing a password-protected key, the key is decrypted and saved unprotected in the vault. Once added to the system, the key is not displayed. The password is not saved.

When “Sharing Views Containing Decrypted Information” is enabled on the SSL Decryption page, Packet Analyzer users who have accessed NetExpress as a probe can share views of decrypted data with other Packet Analyzer users who do not have NetExpress accounts.

When NetExpress is in FIPS mode:

- Cyphers based on MD5 are not accepted.
- PKCS#1 encrypted keys are not accepted.
- SSL 2.0 and 3.0 traffic is not decrypted.

The keys and key assignments are deleted if NetExpress is reinstalled. Updating NetExpress does not remove the keys or key assignments.

Configuring SSL decryption

The Configuration > SSL Decryption page has a section controlling sharing and a section specifying decryption keys.

Sharing views

The sharing section applies to Packet Analyzer users who use NetExpress as a probe. When sharing is enabled, Packet Analyzer users can share views that include metrics for traffic that NetExpress decrypts. This allows Packet Analyzer users who do not have an account on NetExpress to view information that they would not otherwise be able to view.

When the Enabled check box is changed, the Apply button becomes active. Packet Analyzer users should close or stop sharing any shared views containing decrypted data before clearing the Enabled check box.

Figure 2-20. NetExpress Configuration > SSL Decryption page

SSL Decryption

Sharing Views Containing Decrypted Information

Allow users to share views that include decrypted data

Enabled

Protocol

☒ HTTP

Apply

Decryption Keys

<input type="checkbox"/>	Server IP	Server Port	Description	Groups	Fingerprint
No Keys Defined					

Add New

Edit Selected

Remove Selected

Specifying decryption keys

A NetExpress Administrator account is required for adding, removing or editing decryption entries. To add a decryption key, first obtain the private key and, if applicable, the certificate and password from the administrator of the server that is encrypting the data. If the private key requires a password, obtain that also. If there is a certificate associated with the key, it can be included in the PEM format as follows:

```
-----BEGIN ... PRIVATE KEY-----
...
-----END ... PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

Then use the Configuration > SSL Decryption page to add a decryption key as follows:

1. Click **Add New** to open the Add New SSL Decryption Key page.

Figure 2-21. Add New SSL Decryption Key page

Add New SSL Decryption Key

Server IP:

Server Port:

Description:

PEM:

Password:

Groups:

Administrator

Operator

Add

Cancel

2. Enter the IP address and TCP port number of the server.
3. Optionally, enter the description as you want it to appear on the SSL Decryption page.
4. Paste the private key or the private key and certificate into the PEM box.
5. If key is encrypted, enter the password.

6. In the Groups section, select the type of NetExpress user account that the Packet Analyzer user must have to use the NetExpress as a probe: Operator or Administrator. Multi-select both types to allow Packet Analyzer users with either type of account to use NetExpress as a probe.
7. Click **Add**.
8. When the SSL Decryption page is displayed, check the results.

If a certificate was included with the RSA private key, the certificate SHA1 fingerprint is displayed. The decryption key itself is never displayed after it has been added to NetExpress.

Users with an Administrator account can view decryption key assignments for which access has been given to both Operators and Administrators. Additionally, they can edit the description and account types for an entry and delete an entry.

Users with an Operator account can view decryption key assignments for which access has been given to Operators. They cannot view entries for only Administrator accounts and they cannot edit or delete entries.

Port synchronization (NetExpress only)

The Configuration > Port Synchronization page enables you to specify which ports are used for calculating Service Response Time (SRT) metrics. Calculating performance metrics consumes system resources, so the default settings on this page are for NetExpress to perform SRT calculations on only the ports that are most typically used by request/response application layer protocols. However, you can select or deselect ports as appropriate for your network as follows:

1. In the Service Response Time column, select the check boxes beside the ports you want to use.
2. Click **Apply**.

To revert to the last-applied settings, click **Cancel** instead of **Apply**.

Figure 2-22. NetExpress Configuration > Port Synchronization page

Port Synchronization ?

Name	Port	Protocol	Service Response Time	Delete
tcpmux	1	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
compressnet	2	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
compressnet	3	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
rje	5	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
echo	7	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
discard	9	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
systat	11	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
daytime	13	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
netstat	15	tcp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
qotd	17	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
msh	18	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
chargen	19	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ftp-data	20	tcp/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ftp	21	tcp/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	22	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
telnet	23	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
smtp	25	tcp/udp	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
nsw-fe	27	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
msg-lcp	29	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>
msg-auth	31	tcp/udp	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Notes:

- Selecting the Service Response Time check box does not affect existing connections. If a connection was already established at the time the check box is selected, NetExpress does not calculate SRT metrics for that connection.
- If the NetExpress is reporting to a NetProfiler, Service Response Time metrics for the selected ports are included in the information sent to the NetProfiler.
- Changing the settings of the Service Response Time check boxes on this page has no effect on the corresponding settings on a NetShark that is synchronized to the NetExpress.
- If a connection is silent for more than five minutes, SRT metrics are no longer available for that connection.
- SRT metrics are not available for optimized connections.

Service Response Time (SRT) metrics

NetExpress calculates Round Trip Time (RTT) for all connections on which it sees a TCP 3-way handshake. When the Service Response Time check box is selected, NetExpress calculates the following additional metrics for TCP connections carrying request/response application layer protocols:

- Request Transfer Time
- Response Transfer Time
- Request Retransmission Delay
- Response Retransmission Delay
- Server Response Time

Web, Email, and SSH are examples of TCP connections with request/response application layer protocols. Application layer protocols carried by TCP that do not support these metrics include:

- Pipelining, for example, HTTP pipelining or CIFS
- Two-way communication, for example, H.323, Citrix, or chat applications

Default SRT settings

The following ports have the Service Response Time box selected by default.

Port Name	TCP Port	Port Name	TCP Port
ftp-data	20	ldaps	636
ftp	21	rsync	873
smtp	25	ftps-data	989
tftp	69	ftps	990
http	80	imaps	993
pop3	110	pop3s	995
sftp	115	ms-sql-s	1433
nntp	119	ms-sql-m	1434
epmap	135	ncube-lm	1521
netbios-ns	137	pdap-np	1526

Port Name	TCP Port	Port Name	TCP Port
netbios-dgm	138	sms-rcinfo	2701
imap	143	sms-xfer	2702
ldap	389	sms-chat	2703
https	443	sms-remctrl	2704
urd	465	mysql	3306
ibm-db2	523	postgresql	5432
Imap4-ssl-deprecated	585	http-alt	8080
submission	587	bacula-dir	9101
ipp	631	bacula-fd	9102

NetProfiler export (NetExpress only)

The Configuration > NetProfiler Export page has a NetProfilers tab an Exported Interfaces tab, except for CAX360 models, which do not have an Exported Interfaces tab.

NetProfilers tab

The NetProfilers tab lists NetProfiler or NetExpress appliances to which the NetExpress you are logged into can send information. It can send information to two other NetProfiler or NetExpress appliances. It sends only information that it has developed from inputs it has received. It does not pass through any unprocessed information.

The NetExpress can receive:

- Processed traffic information from Cascade Sensor and NetShark appliances
- Network traffic from taps or mirror ports
- Processed flow data from Flow Gateway appliances
- SteelFlow Net data from SteelHead appliances
- Flow data from routers and switches

In addition to monitoring and reporting this data to its users, the NetExpress can also send certain types of data to NetExpress or NetProfiler appliances that are identified on the NetProfiler Export page. It can send them traffic statistics that it develops from:

- Monitoring the network from taps or mirror ports
- Receiving flow information from routers and switches

The NetExpress does not forward raw, unprocessed flow data (such as NetFlow and SteelFlow Net) to other destinations. Also, it does not forward processed information that it receives from other devices, such as Sensor, Flow Gateway and NetShark appliances. To have another NetExpress or NetProfiler receive information from Sensor, Flow Gateway or NetShark appliances, configure those appliances to send their information directly to the destination NetProfiler or NetExpress.

Figure 2-23. NetExpress Configuration > NetProfiler Export page NetProfilers tab

NetProfiler Export ?

The screenshot shows the 'NetProfilers' tab in the 'NetProfiler Export' configuration page. It includes a description of the page's purpose, an 'Add New Entry' button, a text input for 'NetProfiler IP Address' with the value '10.38.130.44', a 'Delete' button, and a 'Configure Now' button. A detailed instruction explains how to specify the target NetProfiler by entering the IP address of the management interface for a NetExpress or Standard NetProfiler, or the address of the Analysis Module for an Enterprise NetProfiler.

Exported Interfaces tab

The Configuration > NetProfiler Export page has an Exported Interfaces tab. You can select which of the appliance's network monitoring interfaces you want to use. You can limit the traffic that is processed by specifying BPF filters for the monitoring interfaces. You can also enable or disable the computation of VoIP metrics and the processing of Deep Packet Inspection (DPI) data for the traffic seen on each monitoring interface. Select DPI Enabled to enable the processing of Layer 7 application identification information.

These selections apply to both the traffic that the NetExpress itself monitors, analyzes and reports, and to the traffic that it exports to the NetProfiler or NetExpress appliances listed on the Configuration > NetProfiler Export page NetProfilers tab.

Figure 2-24. NetExpress Configuration > NetProfiler Export page Exported Interfaces tab

NetProfiler Export ?

The screenshot shows the 'Exported Interfaces' tab in the 'NetProfiler Export' configuration page. It features a checkbox for 'Enable Flow Export' which is checked. Below this is a table for 'Exported Interfaces' with columns for 'Enabled', 'Interface', 'BPF Filter', 'VoIP Enabled', and 'DPI Enabled'. Four interfaces are listed: mon0_0, mon0_1, mon0_2, and mon0_3. Each interface has a checked 'Enabled' checkbox, an empty 'BPF Filter' text box, and checked 'VoIP Enabled' and 'DPI Enabled' checkboxes. An 'Apply' button is located at the bottom left.

Enabled	Interface	BPF Filter	VoIP Enabled	DPI Enabled
<input checked="" type="checkbox"/>	mon0_0		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	mon0_1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	mon0_2		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	mon0_3		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Flow data forwarding (NetExpress only)

NetExpress can forward flow data to up to five other destinations in the format in which it was received.

If you are using a flow collector with limited capacity for sending flow data to monitoring devices, you can conserve that capacity by sending the data to NetExpress instead of to the original destination. NetExpress can then transparently forward the data to the original destination.

Additionally, you can use the **Overwrite Source** option to make the forwarded data appear to be coming from NetExpress. This may be necessary to prevent packets from appearing to be spoofed. This option does not apply to the forwarding of NetFlow version 9 or IPFIX packets.

Figure 2-25. Configuration > Flow Forwarding page

Flow Forwarding ?

The NetExpress can be configured to forward incoming traffic information from multiple sources to multiple other devices. This page specifies which flow sources are forwarded to which target devices. Use the Add New Entry button to create an empty target entry, if necessary, and fill in the information. Then click Configure Now to activate the configuration.

Add New Entry

Destination IP Address	Port	Flow Type *	Overwrite Source	Flow Sources
<input type="text" value="10.38.130.47"/>	<input type="text" value="2055"/>	<input type="text" value="NetFlow"/>	<input type="checkbox"/>	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>
<div style="display: flex; justify-content: space-between; align-items: center;"> Delete Browse... </div>				

Specify the target IP Address, Port, and Flow Type of an individual device that is configured to receive the data.

Check the Overwrite Source box to make the NetExpress overwrite the source addresses of forwarded packets with its own address. This may be necessary to prevent packets from appearing to be spoofed. This option does not apply to the forwarding of Netflow version 9 or IPFIX packets.

Enter a list of device IP addresses whose traffic is to be forwarded to the destination address. Leave the Flow Sources field empty if the NetExpress is to send all flow data to the target destination.

*Note: sFlow and Packeteer are not currently enabled. They can be enabled on the Configuration > General Settings page.

Configure Now

To specify flow data forwarding destinations

1. Go to the Configuration > Flow Forwarding page.
2. Click **Add New Entry** to open a blank entry for specifying a destination.
3. Enter the destination IP address, port number, and data type for each destination that is configured to receive the data. For IPFIX data, select NetFlow.
4. If you need to have the data identified as coming from NetExpress, select **Overwrite Source** to use the NetExpress address as the source address in the forwarded data packets. This option does not apply to the forwarding of NetFlow version 9 or IPFIX packets.
5. In the Flow Sources box, either:
 - Leave the box blank to forward all flow data to the specified device, or

- Enter a comma-separated list of the IP addresses of flow source devices whose traffic is to be sent to the specified destination device.

You can enter IP addresses by clicking **Browse** and searching for the flow source device by name, address, or subnet.

6. Click **Configure Now** at the bottom of the page to apply the settings.


NetExpress begins forwarding flow data to the destination devices within 5 minutes after you click **Configure Now**.

All flow data that is available for forwarding to other devices is also processed by NetExpress. Data from sources specified in the Excluded Sources box in the Data Sources section of the Configuration > General Settings page cannot be forwarded to other devices.

Licenses (hardware-based models only)

The NetProfiler and NetExpress require feature licenses and capacity licenses. Licenses for basic features are included with the software. Other licenses must be downloaded from the Riverbed licensing web site. All downloaded licenses are listed on the Configuration > Licenses page.


Figure 2-26. Configuration > Licenses page

Licenses 





License Updates

Updates successfully retrieved last time on Jun 5, 2016 3:37 PM [Fetch Updates now](#)

☒ Enable Automatic License Download from Riverbed

[How to generate license keys](#) 

Licenses [Add license\(s\)](#) [Delete selected](#)

<input type="checkbox"/> License key 	Description	Device serial number	Installed date	Status
<input type="checkbox"/> LK1-MSPECSCNE470FLOW5-0000	NetExpress 470 Flow Limit (120K flows)	LE1VT0404A42C	May 31, 2016	
<input type="checkbox"/> LK1-CPEL-0000-000	Packet Analyzer Concurrent License (1 pack)	LE1VT0404A42C	May 31, 2016	
Included				

Pilot Concurrent Licenses

Total: 1 | Available: 1 | In use: 0

For each license, the Configuration > Licenses page lists the license key, license description, installation date and status. A status of red indicates that the license is not valid. Yellow indicates that the license will expire within 10 days. Hover the mouse pointer over the status indicator to see the expiration date.

The **Enable automatic license download from Riverbed** option allows the appliance to automatically connect to the Riverbed licensing web site and download the licenses that are assigned to it. It downloads licenses at the time it is installed and then checks for any new licenses once per day thereafter while this option is enabled.

The **Fetch Updates Now** button causes the appliance to immediately connect to the Riverbed licensing web site and download any new licenses that you have purchased.

If the appliance does not have Internet connectivity, then you must log in to the Riverbed licensing web site, generate the license keys, and manually enter them into the list of licenses. The **Add License(s)** button is for manually entering license keys that you get from the Riverbed licensing web site.

If you purchase and download a license for a higher capacity than a current license, the appliance uses the license with the higher capacity.

To delete an obsolete or invalid license, select the check box for the entry and click **Delete Selected**. This does not affect the status of the license on the licensing web site.

The licensing web site provides the flexibility to assign different feature and capacity licenses to different appliances. You can ship appliances to remote locations without concern for which appliance is to have which license. When you have the serial numbers and know where the appliances are deployed in the network, you can make the license assignments on the Riverbed licensing web site.

When all the appliances are to be licensed for the same features and capacities, the licensing web site handles this automatically. The appliances can automatically download their licenses without your needing to visit the licensing web site.

For instructions for generating and downloading license keys, refer to the on line help system or to the *NetProfiler*, *NetExpress* and *Flow Gateway Installation Guide*.

Packet Analyzer licensing

In addition to purchasing licenses for features and capacities on the NetProfiler, you can purchase a license pack for multiple Packet Analyzer software instances. This is activated from the Riverbed licensing web site just as the NetProfiler licenses. Once it is added to the NetProfiler, you can license Packet Analyzer software by adding the address of the NetProfiler to the Packet Analyzer.

This is useful for situations where you have operators on different shifts who may all be using Packet Analyzer software at different times. Instead of buying enough licenses for each person to have their own, you might prefer to purchase only enough licenses to cover the largest number of concurrent Packet Analyzer users you anticipate. These serve as a license pool that users can draw from as needed.

Packet Analyzer licenses expire 48 to 72 hours after they are issued. The expiration time is based on UTC and therefore the actual number of hours depends on the time zones of the Packet Analyzer and NetProfiler. They are automatically renewed if the Packet Analyzer is connected to a NetProfiler that has Packet Analyzer licenses available.

When you install a license for multiple Packet Analyzer instances, the Configuration > Licenses page expands to include a Packet Analyzer Concurrent Licenses section at the bottom. This section lists the total number of Packet Analyzer licenses available and the number currently in use.

If at least one Packet Analyzer is connected, a View link is displayed. Click the View link in the Packet Analyzer Concurrent Licenses section to see the licenses that are currently in use.

Figure 2-27. Configuration > Licenses page - Viewing concurrent Packet Analyzer licenses

Pilot Concurrent Licenses

Packet Analyzer Concurrent Licenses				
Activation Code	Host	User	Generation Date	Expiration Date
LK1-CPEL-4242-4244	BRDUBOIS-VM2-W7.nbttech.com	brdubois	Jun 10, 2016 9:12 AM	Jun 12, 2016 7:59 PM

Page 1 of 1

Displaying 1 - 1 of 1

Licenses (virtual editions only)

Virtual editions require feature licenses and capacity licenses. Licenses for basic features are included with the software. Other licenses must be downloaded from the Riverbed licensing web site. All downloaded licenses are listed on the Configuration > Licenses page.

Figure 2-28. Configuration > Licenses page

Licenses ?

License Updates
 Updates have not been retrieved yet. [Fetch Updates now](#)
☐ Enable Automatic License Download from Riverbed

License Request
 License request token: [Request key](#)

[How to generate license keys ?](#)

Licenses		Add license(s)	Delete selected
<input type="checkbox"/> License key +	Description	Device serial number	Installed date Status
<input type="checkbox"/> LK1-MSPECSCNEV470FLOW5-0000-0000	NetExpress 470 Flow Limit (120K flows)	N/A	May 31, 2016 ●
<input type="checkbox"/> LK1-CPEL-0000-0000		N/A	May 31, 2016 ●
<input type="checkbox"/> LK1-CPEL#2+00000000-0000-0000	Packet Analyzer Concurrent License (2 pack)	N/A	Jun 1, 2016 ●

Pilot Concurrent Licenses
 Total: 2 | Available: 2 | In use: 0

To activate a license, you enter a token that you receive when you purchase the license. The product generates a license activation code. You enter this code on the Riverbed licensing website and it generates a license key. You enter the license key on this page to activate the license. For detailed licensing instructions, refer to the on line help system or the installation guide.

For each license, the Configuration > Licenses page lists the license key, license description, installation date and status. A status of red indicates that the license is not valid. Yellow indicates that the license will expire within 10 days. Hover the mouse pointer over the status indicator to see the expiration date.

If you purchase and download a license for a higher capacity than a current license, the appliance uses the license with the higher capacity.

To delete an obsolete or invalid license, select the check box for the entry and click **Delete Selected**. This does not affect the status of the license on the licensing web site.

General settings

The Configuration > General Settings page includes controls for setting up:

- Management Interface Configuration
- Name Resolution
- Aux Interface Configuration (NetExpress only)
- Static Routes (NetExpress only)
- Monitor Interface Configuration (NetExpress only)
- Packet Deduplication (NetExpress only)
- Time Configuration
- Module Addresses (Enterprise NetProfiler only)

- Data Sources (NetExpress only)
- SNMP MIB Configuration
- Outgoing Mail Server (for alerts and reports sent by the appliance)
- Inside Address Configuration
- Security Module Configuration
- Report Data Management
- Baseboard Management Controller Settings
- Service Management

Changing the Network page requires an Administrator or Operator account. Changes you make on the Configuration > General Settings page take effect when you click **Configure now** at the bottom of the page.

Note: If someone were to misconfigure the management interface settings, the appliance would become unreachable and it would be necessary to reinstall the software in order to access it. If other parameters were misconfigured, the appliance might not monitor traffic and send alerts correctly. It is important to the operation of the appliance for the settings on the General Settings page to be correct.

Note: If you deploy a Sensor on the same subnetwork as the appliance, and if an intruder can place an unauthorized device on that subnetwork, then a security risk may exist. Refer to [Appendix C, “Securing the Environment.”](#) for a description of securing the appliance against this type of risk.

Management Interface Configuration

The management interface configuration specifies the name and address of the NetProfiler or NetExpress appliance. (For the Enterprise NetProfiler, this is the address of the User Interface Module.) You can specify the speed, duplex mode, or auto-negotiate mode. When you click **Configure Now**, these values are set into the management interface. Additionally, the current status of management link is displayed.

Figure 2-29. Management Interface Configuration section of the Configuration > General Settings page

Management Interface Configuration

*Hostname:	<input type="text" value="cascade-profiler-VE"/>	Specify the hostname and other management interface information for the NetProfiler. Use this information to log in to the NetProfiler after it is fully configured.
*IP address:	<input type="text" value="10.38.129.70"/>	
*Netmask:	<input type="text" value="255.255.192.0"/>	
*Default gateway:	<input type="text" value="10.38.128.1"/>	
Management settings: <input type="button" value="Auto Negotiate"/>		Current status: 10000, Full, Off, Link detected, Twisted pair

Name Resolution

This section determines how host names and network device names are resolved when **Resolve host and device names** is enabled in the Data section of the Configuration > UI Preferences page.

Figure 2-30. Name Resolution section of the Configuration > General Settings page

Name Resolution

Search domains: For resolution of unqualified names, enter the suffix to append for DHCP/DNS searches. You can enter multiple domains as a comma-separated list.

☒ Enable DNS name resolution. [Edit /etc/hosts...](#)

Primary DNS IP address: Specify the DNS server that the NetProfiler uses to look up hostnames.

Secondary DNS IP address:

Hosts name resolution:

☒ Enable DNS name resolution for hosts.

Resolve host names for only the first hosts in any one table or graph.

Send no more than DNS lookup requests at a time.

☒ Enable DHCP name resolution for hosts managed by DHCP. Available with DHCP integration.

☒ IPv4 take precedence over IPv6 ☐ IPv6 take precedence over IPv4

Network devices name resolution:

☒ Enable SNMP name resolution for network devices. Available with SNMP integration. [Global SNMP Settings...](#)

☒ Enable DNS name resolution for network devices.

Refresh data every Week(s) [Clear device DNS cache](#)

☐ SNMP names take precedence over DNS ☒ DNS names take precedence over SNMP

Search domains

When the NetProfiler or NetExpress appliance looks up the address of a host name that does not include a domain name, it appends a specified domain name to the host name in order to construct a fully qualified domain name and perform the search. You can specify multiple search domains as a comma-separated list. The NetProfiler tries to resolve the host name using each domain in the search list in the order in which it appears in the list. For example, assume that you specified a comma-separated list of domain names, such as:

newcompany.com,emea.newcompany.com,oldcompany.com

Also, assume that you specified “finance_1” in a report criteria field that accepts host names. The appliance would append the first search domain in the list and use *finance_1.newcompany.com* in a lookup. Then it would append the second domain in the list to the host name and use *finance_1.emea.newcompany.com* in another lookup, and so on. It would attempt to find the address by looking up the host name and a fully qualified domain name based on each domain in the search list.

If a host name is registered in more than one domain, the appliance uses the first IP address it obtains. Therefore, it is best to enter the list of search domains with the most preferred domain first.

DNS servers

Specify the addresses of the DNS servers that the NetProfiler or NetExpress appliance accesses to look up the host name associated with an IP address or the IP address associated with a host name. Leaving the primary and secondary DNS server address fields blank disables the use of DNS.

This section enables DNS name resolution in general. Name resolution can be enabled or disabled for hosts and network devices separately in their respective sections.

Edit /etc/hosts - opens an editor for modifying the hosts file. This file includes address-name assignments required by the appliance, which are not editable, and address-name assignments that are user-defined. Assignments that you define in the */etc/hosts/* file take precedence over DNS lookups. They are not affected by configuration changes. DNS name resolution must be enabled for this feature to be available.

Host name resolution

Enable DNS name resolution for hosts - Enables DNS name resolution for hosts and sets limits to protect your DNS server from excessive traffic loads. You can limit the number of host lookups that the NetProfiler appliance requests at one time. For example, if you specify that the NetProfiler is to resolve no more than 1000 hosts at a time, then it will send 1000 DNS lookup requests and wait for all 1000 to be answered or timed out before sending the next thousand.

You can also limit the number of lookups for any one table, graph or list on a report. If the number of hosts in any one table, graph or list exceeds the specified limit, then all hosts beyond the limit are reported by their addresses instead of by their host names. This setting applies to Reports pages and the Host Groups page.

Enable DHCP name resolution for hosts managed by DHCP - Enables name resolution for hosts managed by DHCP. When this option is selected, the appliance looks for the name assignment in its local DHCP data records. This requires DHCP integration to have been configured.

If both the DNS and DHCP options are selected, then the NetProfiler first looks in its DHCP data records before performing a DNS lookup.

When it finds the name of the host, it displays the host name on GUI pages that list hosts. It also displays the domain to which the host belongs, unless you have selected the Suppress DHCP/DNS search domains option in the Data section of the Configuration > UI Preferences page.

Network device name resolution

Enable SNMP name resolution for devices - Allows the NetProfiler or NetExpress appliance to use SNMP to obtain the names of network devices that are sending traffic information to it. This requires SNMP polling to be configured.

Enable DNS name resolution for devices

Specifies how often the cache containing the DNS names for network devices is refreshed. Additionally, the following conditions cause the cache to be cleared and rebuilt:

- Enabling or disabling DNS name resolution globally in the Host name resolution section.
- Modifying the search domains setting.
- Modifying the primary or secondary DNS server addresses.
- Using the Edit /etc/hosts button to edit the /etc/hosts file.
- Clicking the Clear device DNS cache button.

Precedence - If both SNMP and DNS name resolution for network devices are enabled, you can select which takes precedence over the other.

Aux Interface Configuration (NetExpress only)

The Configuration > General Settings page Aux interface configuration section allows the NetExpress to use both the Management and Aux interfaces for processing traffic flow information (NetFlow, SteelFlow Net, sFlow, Packeteer FDR, etc.) and control information (user sessions, network services and communication with other SteelCentral™ products).

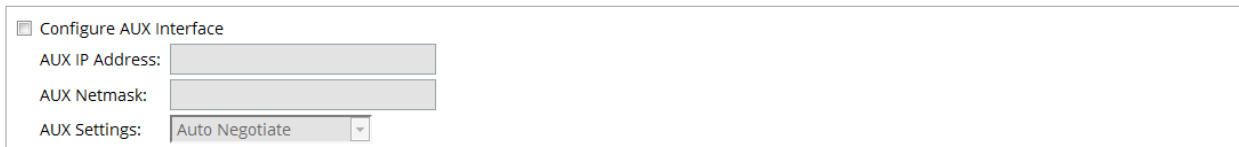
The processing of traffic flow information on these two interfaces can be limited by the Data Sources section of the page. The Data Sources section can be set to allow or not allow flow data protocols on the Aux interface or the Management interface or both interfaces. The option to block flow data from being processed on the management interface enables the NetExpress appliance to support configurations that require network data and network management functions to be handled by separate subnets for security purposes.

When the Aux interface is enabled, it uses the same incoming connection security requirements as the management interface, except for protocols used for flow information (NetFlow, SteelFlow Net, sFlow, Packeteer FDR, etc.).

If the flow data forwarding feature is used when the Aux interface and Management interface are configured on separate subnets, the default behavior is to forward flow data using the interface that is on the same subnet as the destination address. If the destination address is not on either subnet, the flow data packets are sent to the default gateway. This default configuration can be overridden by specifying static routes.

Figure 2-31. Aux Interface Configuration section of the Configuration > General Settings page

AUX Interface Configuration



☒ Configure AUX Interface

AUX IP Address:

AUX Netmask:

AUX Settings: Auto Negotiate

Configuring interfaces for separate data and control networks

The procedure for setting up separate network data and network control interfaces on the NetExpress appliance assumes that:

- There are two separate networks with non-overlapping IP addresses.
- The NetExpress appliance management interface is already connected and the web GUI is accessible.

The general procedure is to:

1. Connect the network for the flow information (NetFlow, SteelFlow Net, sFlow, Packeteer FDR, etc.) to the Aux port of the NetExpress chassis.
2. Go to the Configuration > General Settings page Aux interface configuration section. Enable the Configure AUX Interface option and set the IP address, netmask, and interface speed, as required.
3. In the Data Sources section of the page, allow receiving flow protocol traffic on the Aux interface and not on the Management interface, and enable the flow protocols you want the NetExpress appliance to receive.
4. If you need to override the default configuration, go to the Static Routes section of the page and configure any necessary static routes.
5. Configure the flow exporting devices to send flow data to the Aux interface address instead of the Management interface address.

Configuring a single interface for data and control

If the Management and Aux interfaces are already set up and working for split operation and you want to switch to having both network data and network control traffic on the same subnet, the general procedure is as follows:

1. Go to the Configuration > General Settings page Aux interface configuration section and deselect the Configure AUX Interface option. This disables the Aux interface.
2. In the Data Sources section of the page, set the Allow on interface selection to allow receiving flow protocols on the Management interface.
3. If any static routes were added for the configuration that used separate networks for data and control, remove them in the Static Routes section of the page.

4. Configure flow exporting devices to send flow data to the Management interface address instead of the Aux interface address.

Static Routes (NetExpress only)

If there are multiple subnets on the Aux interface network, or if you need to use a gateway router other than the default gateway, it may be necessary to define static routes. Use the Static Routes section of the Configuration > General Settings page to specify static routes as necessary.

Figure 2-32. Static Routes section of the Configuration > General Settings page

Static Routes

Network	Netmask	Gateway
No Data Available.		
Edit Static Routes...		

Monitor Interface Configuration (NetExpress only)

If your NetExpress is not a flow-monitoring-only model, then the network monitoring ports must be configured for the speed of the tap or mirror ports they use on the monitored network.

Figure 2-33. Monitor Interface Configuration section of the Configuration > General Settings page

Monitor Interface Configuration

mon0_0 settings:	Auto Negotiate	Current status: 100, Half, On, Link detected, Twisted pair
mon0_1 settings:	Auto Negotiate	Current status: speed?, duplex?, On, No link, Twisted pair
mon0_2 settings:	Auto Negotiate	Current status: speed?, duplex?, On, No link, Twisted pair
mon0_3 settings:	Auto Negotiate	Current status: 1000, Full, On, Link detected, Twisted pair

Packet Deduplication (NetExpress only)

If the NetExpress is receiving traffic from more than one source in the same network, it may see some of the same packets more than one time. This can impact the accuracy of reports. For example, duplicated packets can cause over-counting, and duplicated packets that contain TCP SYNs can interfere with the measurement of performance metrics, such as RTT.

There can be many causes of packet duplication in a network, and there can be several effects on the accuracy of reporting by the NetExpress. If you believe that your network configuration might cause the NetExpress to see duplicated packets, you should enable packet deduplication.

Packet deduplication consumes NetExpress resources and can impact its performance on a busy network. So if your network configuration does not artificially introduce duplicated packets, it may be desirable to deselect the packet deduplication option.

Figure 2-34. Packet Deduplication section of the Configuration > General Settings page

Packet Deduplication

<input checked="" type="checkbox"/> Enable packet deduplication.	Enable packet deduplication if your network configuration might cause the SteelCentral appliance to see duplicated packets.
--	---

Time Configuration

The Time Configuration section of the Configuration > General Settings page sets the time zone and specifies the time reference used for timekeeping in the appliance.

- **Time Zone** – sets the time zone in which the appliance itself is operating.
- **Synchronize to an external NTP server** – specifies NTP servers the appliance should use as timing sources. If the first server specified is unreachable, the appliance attempts to use the second one.

The connection to the NTP server can use SHA1 or MD5 encryption or no encryption. For an encrypted connection to the NTP server, obtain the encryption key and index from the person who is responsible for controlling the domain's authoritative time server.

If the appliance is to be operated in the FIPS 140-2 Compatible Cryptography mode, the NTP server connection must use SHA1 encryption.

Note: When the appliance is switched to the FIPS 140-2 Compatible Cryptography mode, any NTP servers that are currently configured to use MD5 encryption will be disconnected without notification to the user.

- **Use local clock** – selects the internal clock as the time reference for timekeeping in the appliance. To use the local clock, click **Set System Time** and edit the time and date as necessary.

The time configuration is not applied until you click **Configure Now** at the bottom of the page.

Figure 2-35. Time Configuration section of the Configuration > General Settings page

Time Configuration

Time Zone: America/New_York ?

☐ Synchronize to an external NTP server

IP Address	Encryption	Key	Index	Action
Add new NTP server				

☒ Use local clock: Jun 5, 2016 1:19:57 PM Set System Time

You can either configure the NetProfiler to synchronize with an external NTP server (recommended) or use the NetProfiler's local clock. If you would like to use the local clock, you can set the system time now.

Note: There is no notification when switching to the FIPS 140-2 Compatible Cryptography mode disconnects NTP connections using MD5 encryption.

Module Addresses (Enterprise NetProfiler only)

The Enterprise NetProfiler Module Addresses section lists all modules that are present in the system. It specifies the IP address, connection mode and connection status of each module.

If the Enterprise NetProfiler includes a Dispatcher Module that is connected to a switch configured for link aggregation (channel bonding), an information icon is displayed behind the Dispatcher listing. Click the icon to display channel bonding status.

Figure 2-36. Enterprise NetProfiler Module Addresses section of the Configuration > General Settings page

Enterprise NetProfiler Module Addresses

Riverbed NetProfiler requires an IP address for each module. These should be in the same subnet as the Management module. Riverbed Sensors and third-party data sources send data to the IP address of Analysis Module.

*Management Module:	10.38.134.65		1000, Full, On, Link detected, Twisted pair
*Dispatcher Module:	10.38.133.241	1000 Mbs, Full Duplex	1000, Full, Off, Link detected, Other
*Expansion Module:	10.38.133.243	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.133.246	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.133.248	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.133.251	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Analysis Module:	10.38.134.78	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.134.0	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.134.6	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.134.10	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.134.12	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Expansion Module:	10.38.134.14	Auto Negotiate	1000, Full, On, Link detected, Twisted pair
*Database Module:	10.38.134.55	Auto Negotiate	1000, Full, On, Link detected, Twisted pair

Figure 2-37. Enterprise NetProfiler Bonded Addresses

Bonded interfaces

Interface name	Link detected	Auto Negotiate	Port	Duplex	Speed
eth0_0	no	on	twisted pair		
eth0_1	no	on	twisted pair		
pri	yes	on	twisted pair	full	1000 Mbs

Data Sources (NetExpress only)

The NetProfiler can be configured to receive traffic flow information from devices using NetFlow (versions 1, 5, 7 and 9), SteelFlow Net, IPFIX, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). You can specify one or more ports in a comma-separated list for each type of flow data, up to a combined total of 50 ports.

You can also exclude data sources. NetProfiler ignores data sent to it from addresses listed in the Excluded Sources box. For example, it drops NetFlow data sent to it from a router whose address is listed in the Excluded Sources box. Excluded data is not processed and is not available for forwarding to other devices.

When the NetExpress is configured to use the Aux and Management interfaces on separate networks, use the **Allow on interface** option to control which interface is to receive traffic flow data.

Figure 2-38. Data Sources section of the Configuration > General Settings page

Data Sources

<input checked="" type="checkbox"/> Use NetFlow/IPFIX	Port: <input type="text" value="2003, 2055"/>	<p>The NetExpress can be configured to receive traffic flow information from NetFlow (versions 1, 5, 7 and 9), IPFIX, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). Specify one or more ports in a comma-separated list for each type of flow data, up to a combined total of 50 ports. Do not assign a port to receive more than one type of flow data. That is, each port can be listed only once. The combined capacity of these data sources is 90,000 flows/minute. The common default ports for NetFlow are 2055, 9555, 9995 and 9996.</p>
<input checked="" type="checkbox"/> Use sFlow	Port: <input type="text" value="6343"/>	
<input checked="" type="checkbox"/> Use Packeteer	Port: <input type="text" value="9800"/>	
Allowed on interface:	<input checked="" type="checkbox"/> Management <input type="checkbox"/> AUX	
Excluded Sources:	<input type="text"/> ?	

SNMP MIB Configuration

The appliance MIB can be browsed by external applications and devices. NetExpress supports browsing by Version 1, 2c and 3 clients but can support only one type of client at a time. To limit support to SNMP V1 clients, fill out the Location, Description, Contact, and Community fields. To support SNMP V3 clients, fill out the authentication and optional privacy information fields instead of the Community field.

Figure 2-39. SNMP MIB Configuration section of the Configuration > General Settings page

SNMP MIB Configuration

Location:	<input type="text"/>	<p>The NetProfiler MIB can be browsed by external applications and devices. The NetProfiler supports V1, V2C and V3 clients but can only be configured to support one type of client at a time. To limit support to SNMP V1 and V2C clients, fill out the Community String, Location, Description, and Contact fields. To support SNMP V3 clients also fill out the authentication and optional privacy information.</p>
Description:	<input type="text"/>	
Contact:	<input type="text"/>	
SNMP version:	<input checked="" type="radio"/> V1 <input type="radio"/> V2C <input type="radio"/> V3 <input type="radio"/> Off	
Community:	<input type="text" value="....."/>	
Username:	<input type="text"/>	
Security level:	<input type="text" value="No Authentication/No Privacy"/>	
Authentication passphrase:	<input type="text"/>	
Authentication protocol:	<input type="text"/>	
Privacy passphrase:	<input type="text"/>	
Privacy protocol:	<input type="text"/>	
Maximum length of lists attached to traps: <input type="text" value="10"/>		

Authentication and Privacy Fields

- **Username** - SNMP security name that the application attempting to browse the appliance MIB must use.
- **Authentication passphrase** - String that the application attempting to browse the appliance MIB must use to authenticate itself to the appliance.
- **Authentication protocol** - Algorithm that the appliance must use to decipher the authentication passphrase used by the application attempting to browse the appliance MIB. This can be MD5 or SHA.
- **Privacy passphrase** - String that the application attempting to browse the appliance MIB must use.
- **Privacy protocol** - Algorithm that the appliance must use to decipher the privacy passphrase used by the application attempting to browse the appliance MIB. The appliance uses DES at this time.

Outgoing Mail Server (SMTP) Settings

This section specifies the IP address or name and port number of the mail server that the appliance uses when it sends email with alert notifications or reports. You can also specify a “from” address to ensure that the email is allowed through a firewall.

The appliance supports mail server authentication. To use this, click **Use name and password**. Then enter the user name and password that the appliance is to use to gain access to the mail server.

Figure 2-40. Outgoing Mail Server (SMTP) Settings section of the Configuration > General Settings page

Outgoing Mail Server (SMTP) Settings

Server:	<input type="text"/>	The NetProfiler can be configured to send emails to indicate alert conditions and to deliver traffic reports. Specify the server and the from email address for outgoing messages.
Port:	<input type="text"/>	
From address:	<input type="text"/>	
<input type="checkbox"/> Use name and password		
*User name:	<input type="text"/>	
*Password:	<input type="password"/>	

Inside Address Configuration

The inside address specification is used by the security analytics. The security analytics compare current network behavior to profiles of typical network behavior. Because the security analytics focus on what is happening inside your network, internal addresses are tracked individually in the internal security database. However, external addresses are by default tracked in blocks of /8 within the internal security database to conserve system resources.

The inside address specification provides for tracking hosts individually within the security profile. It has no effect on address tracking and reporting for Performance and Availability analytics. All hosts seen or reported to the NetProfiler or NetExpress are tracked individually and stored in flow logs for real time and historical reporting, regardless of the inside address specification. The inside address specification affects only which hosts are tracked individually in the internal security database.

Figure 2-41. Inside Address Configuration section of the Configuration > General Settings page

Inside Address Configuration

Inside addresses:	<input type="text" value="10/8, 172.16/12, 192.168/16"/>	The Inside Address Configuration allows you to specify the "inside" of your network. Please configure all ranges of addresses (from /32 to /0) that belong inside your network including your public IP Address space and all reserved address space. Addresses that are not included in this definition will not be grouped within Host Groupings and won't be considered by the security module (if enabled) for security policies.
	(e.g., "10/8, 172.16/12, 192.168/16")	

Security Module Configuration

The General Settings page includes the Security Module Configuration section for enabling and disabling the security analytics module.

Figure 2-42. Security Module Configuration section of the Configuration > General Settings page

Security Module Configuration

<input checked="" type="checkbox"/> Enable the Security Module for the NetProfiler.	The NetProfiler is capable of a wide range of security-focused tasks and abilities. These include creating expected traffic profiles of the inside network, running security heuristics on data collected, doing automatic attack mitigation and much more. Please note that turning the security module on or off will force all current NetProfiler users to log in again.
---	---

When the security analytics module is disabled or not installed, the following security-related features are not displayed:

- Network Security Dashboard
- Behavior Analysis > Policies page Security tab
- Reports > Shortcuts page Built-in tab Executive Event Summary
- Reports > Traffic page Advanced tab “Typical behavior” option in the Report Format section
- Reports > Events page “Security” check box in the Triggering policies section
- Configuration > Mitigation
- Configuration > Security Profiles
- Configuration > Integration > Vulnerability Scanning

Report Data Management

Select a check box in this section if you expect to be adding statistics to reports after you run them. Otherwise, leave the check box deselected for faster reporting.

Figure 2-43. Report Data Management section of the Configuration > General Settings page

Report Data Management

Collect *all* traffic statistics that can be displayed when running:

- ☐ User-initiated reports
- ☐ Scheduled/Run in background reports

Select these features if you want all statistics that can be displayed to be collected at the time the report is run. This allows you to change what the report displays without needing to refresh the report. Deselect these features for faster reporting. When the feature is deselected, the report collects only the information required by the report template. You must refresh the report if you modify the settings to display additional information.

When these check boxes are not selected

When you run a report, the appliance collects just the data necessary to display the statistics specified in the template for the report. This includes the data for the statistics that are displayed and also any data needed to derive those statistics.

You can modify the report to include additional statistics, such as by using the Column Chooser tool to add a column to a table. If the statistic that you add is one of those that was already collected for use in deriving a statistic that is displayed, then it will be displayed immediately. If it is not, then you must refresh the report for the appliance to collect more data and display the new statistic.

When a check box is selected

When you run a report, the appliance collects data for every statistic that can be displayed on the report. This consumes more system resources and requires more time for the report display initially. But if you make modifications to the report, it enables you to see the results of your modifications more quickly.

Baseboard Management Controller Settings (Models xx70 only)

The hardware platform includes a web user interface to the Baseboard Management Controller (BMC). This BMC web user interface is separate from the NetProfiler or NetExpress web user interface.

The BMC monitors system and network watchdogs, error logs and sensors. The sensors measure internal temperature, power settings, fan speeds and other chassis health conditions. Using a web browser, you can remotely start, restart and power down the chassis. You can monitor hardware operating parameters and configure alerts for conditions outside specified limits.

For descriptions of these features, log in to the BMC web user interface and open the online help system or refer to Appendix B of the Upgrade and Maintenance Guide for series xx70 SteelCentral products.

Remote access to BMC functionality is disabled by default. To enable the BMC web user interface, you must use the NetProfiler or NetExpress web user interface to:

- Specify an IP address on the network for the BMC. This can be done by either enabling DHCP or specifying a static address.
- Assign a log name and password for logging into the BMC web user interface.

The BMC web user interface has a default user account named “root” and the default password “superuser.” The root account cannot be renamed. However, you can assign a different password to the root account.

In the NetProfiler or NetExpress web user interface you can assign a second account name if you enter anything other than “root.” For example, you could change the password on the root account to something more secure than the default password for one group of users and then create a second account name and password for another group of users.

Use the NetProfiler or NetExpress web user interface to assign login credentials to the BMC web user interface. Do not change the user name or password from within the BMC web user interface.

If your security practices require you to disable remote access to the BMC web user interface, use the Edit feature to set the IP address, subnet and gateway address all to 0.0.0.0.

1. On an Enterprise NetProfiler system, specifying the login credentials in the NetProfiler web user interface automatically sets them for all modules. Changing login credentials in the BMC web user interface does not. If you add or replace a module in an Enterprise NetProfiler system, re-specify the login credentials in the NetProfiler web user interface to bring the new module into synchronization with the other modules.

Figure 2-44. Baseboard Management Controller Settings section of the Configuration > General Settings page

Baseboard Management Controller Settings

Host	Host Label	IP Address	Netmask	Gateway	DHCP	Action	Specify the address and login credentials for remote access to the Baseboard Management Controller (BMC).
cascade-express	uihost	10.38.135.216	255.255.192.0	10.38.128.1		Edit	

[Set Up BMC access credentials ...](#)

To configure the BMC settings

1. On the Configuration > General Settings page, go to the Baseboard Management Controller Settings section and click **Set up BMC access credentials**.
2. In the “BMC access credentials” window, enter a user name and a password and click **Save**.
3. In the Action column, click the **Edit** link.
4. Either select **Enable DHCP** or else enter the IP address, netmask and gateway to be used for accessing the BMC.
5. Click **Save**.
6. For the Enterprise NetProfiler, repeat Steps 3 through 5 for each module. (The login credentials are automatically distributed to all modules.)

Service Management

The end-user component of a service is tracked and reported by location. This enables you to examine performance metrics by location and isolate a problem to a location. In order to perform by-location tracking and reporting, the NetProfiler or NetExpress must know the location of each member of the end-user component of the service. It determines the location of an end user by checking the end user's IP address against the IP addresses defined for the groups in the group type that is selected in the Service Management section of the Configuration > General Settings page.

Figure 2-45. Service Management section of the Configuration > General Settings page

Service Management

<p>The location-based group type to use for your services:</p> <p>ByLocation ▼</p>	<p>The locations in this group type will be used to organize end user systems on dashboards and in reports, allowing you to track performance metrics on a per location basis. This group type will be applied to all service definitions. See the documentation for details on best practices for choosing an appropriate group type and for consequences of switching group types once services are defined.</p>
--	--

The default selection is the ByLocation group type. If you want to use the ByLocation group type for determining how end user components are tracked and reported, then ensure that the groups of that group type associate IP addresses with the locations you want to track.

If you have a large network, it may be desirable to track and report end users by region, rather than by individual location. In this case, you may prefer to create a ByRegion group type for managing services. In this new group type you might define regional groups instead of using smaller geographical locations.

The group type selection you make on the Configuration > General Settings page is applied to all service definitions. It determines how end-user service components are grouped on dashboards and reports. You should choose this group type carefully because historical data for services will be lost if you must change the group type later.

CHAPTER 3 Monitoring Services

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress service monitoring features. It includes the following sections:

- [“Overview,”](#) next
- [“Service dashboard”](#) on page 71
- [“Managing services”](#) on page 89

Overview

The SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliances define a service as all clients, servers, applications and ports involved in the end-to-end delivery of a network service. A service is composed of one or more service segments that can be monitored, reported and alerted on individually.

Each service segment comprises a client component, a server component, and the applications and ports in use between them. The components are groups of user or server machines. The applications and ports in use between components are treated as connections.

Information about services can be displayed on the dashboard or in the service reports. As part of defining a service, you can select performance metrics to be monitored for the service. This automatically creates policies that can detect and alert on excessive changes in the values of the monitored metrics.

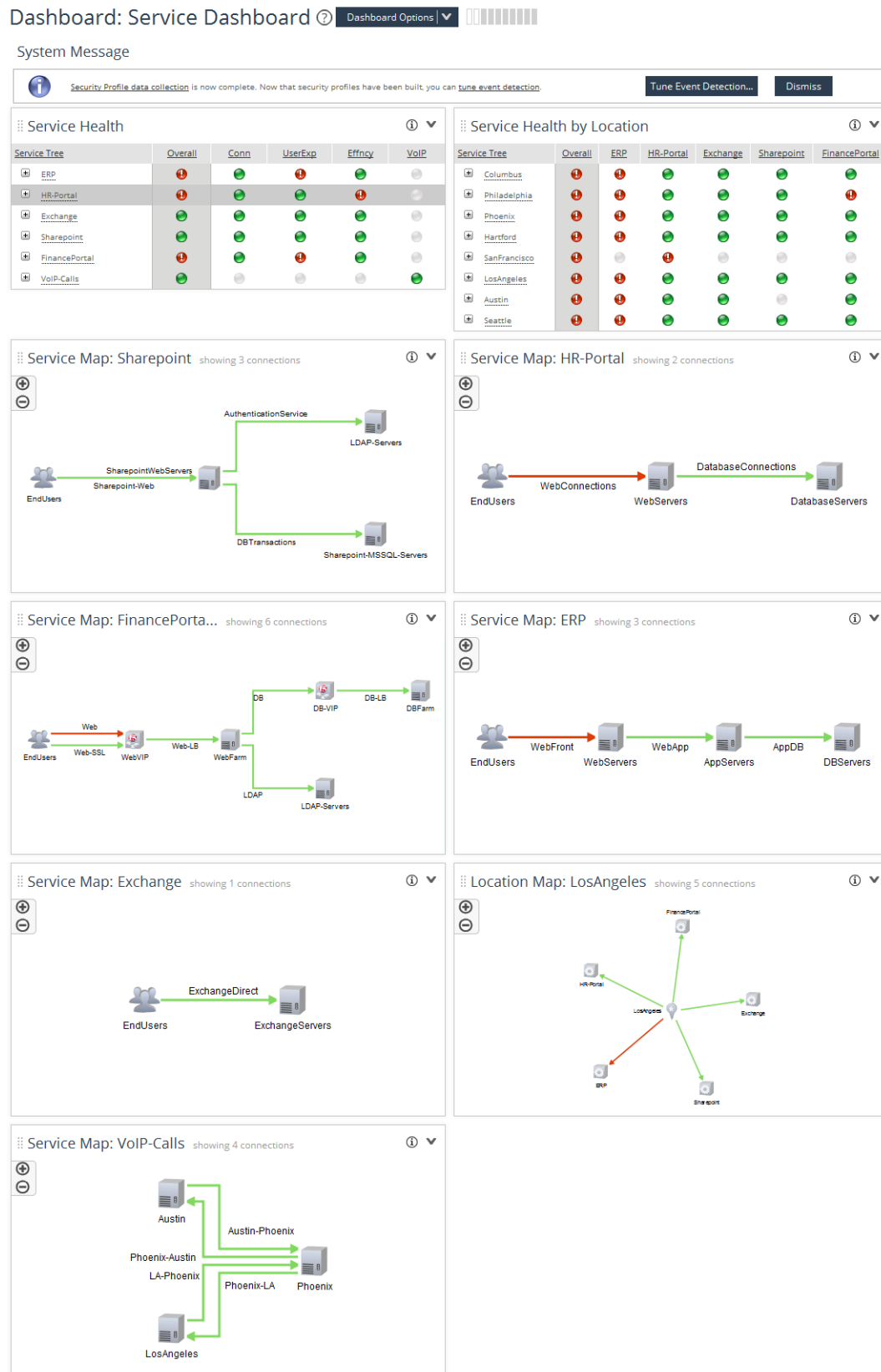
Alerts are displayed on the service dashboard and in service reports. Service reports also indicate trends and provide comparisons and summaries.

Service dashboard

The appliance includes a default Service dashboard with widgets for displaying the health of services. However, you must define the services your network provides before their performance metrics can be monitored and displayed on the dashboard.

After your services are defined, you can monitor their performance on a default or custom dashboard. Service health is displayed in four types of dashboard widgets:

- **Location Map** - locations of service components and their status
- **Service Health** - service health by metric category

Figure 3-1. Service Dashboard

- **Service Health by Location** - service health by user location
- **Service Map** - service components and the applications and ports in use between them

The dashboard widgets display information as soon as at least one service has been defined and set to monitor at least one service metric. The Service Health and Service Health by Location widgets display the status of the service. After a service is selected, the Service Map widget displays the relationships among service components of a service.

Service Health widget

The Service Health widget displays the health of each of the following categories of metrics for each service:

- **Connect** - Connectivity
- **UserExp** - User Experience
- **Effncy** - Efficiency
- **VoIP** - Voice over IP

Each metric category represents the state of the metrics that it comprises. When you define a service, you select which of these metrics are to be monitored for the service. You might monitor only a few, or you might monitor all of them.

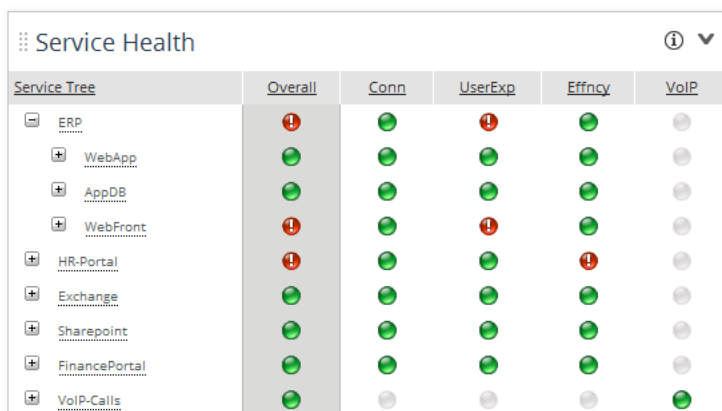
When you create a Service Health widget (Dashboard Options > Add Widget), you can limit the display to selected services and/or locations. If the widget is not displaying all services for all locations, then a funnel icon is displayed on the title bar. You can hover the mouse over this to see a list of which services for which service locations are being displayed.

The health of the metric category (green, red) indicates the health of the least healthy metric in the category. So a green (normal) indication for a metric category means that all the metrics in that category that are being monitored for the service are in normal health. If any one of those metrics were in an alert state (red), then the metric category indicator would also display that condition.

Similarly, the Overall indicator displays the health status of the least healthy metric category. So if any one metric in any one of the metric categories is in an alert condition, this is displayed by the Overall indicator. Note that the Overall column indicates the overall health of just the services that are shown in the widget. If the definition of the widget filters out services or locations, these are not included in the status indicated by the Overall indicator.

Each service shown on the service tree can be expanded to show the status of each of its service segments. The service segment that includes the end users of the service can be further expanded to show the status of each service location group.

Figure 3-2. Service Health widget



Service Tree	Overall	Conn	UserExp	Effncy	VoIP
ERP	🔴	🟢	🔴	🟢	🟡
WebApp	🟢	🟢	🟢	🟢	🟡
AppDB	🟢	🟢	🟢	🟢	🟡
WebFront	🔴	🟢	🔴	🟢	🟡
HR-Portal	🔴	🟢	🟢	🔴	🟡
Exchange	🟢	🟢	🟢	🟢	🟡
Sharepoint	🟢	🟢	🟢	🟢	🟡
FinancePortal	🟢	🟢	🟢	🟢	🟡
VoIP-Calls	🟢	🟡	🟡	🟡	🟢

Service Health by Location widget

The Service Health by Location widget provides a view of the health of services by location-based group. Part of defining a service is specifying the IP addresses or CIDR blocks of addresses of the end users of the service. All user addresses are specified as end user components of the front end service segments.

This same set of end user IP addresses must also be broken into location-based host groups, using the Definitions > Host Groups pages. If there are more than 30 location groups, the display includes an overall health indicator, which represents to aggregation of all location-based groups.

By default, the Service Health by Location widget reports location groups of the ByLocation group type. However, you can create a new group type (such as “ByRegion”) and populate it with location groups. Remember to ensure that this group type is selected in the Service Management section of the Configuration > General Settings page.

The Service Health by Location widget displays the location-based groups that you have defined. For each location group, it displays health status indicators for each service that has end users in that location. It also displays and Overall indicator.

When you create a Service Health by Location widget (Dashboard Options > Add Widget), you can limit the display to selected services and/or locations. If the widget is not displaying all services for all locations, then a funnel icon is displayed on the title bar. You can hover the mouse over this to see a list of which services for which service locations are being displayed.

Each location group can be expanded to display the Connectivity, User Experience and Efficiency metric categories. When you define a service, you select which of these metrics are to be monitored for the service. You might monitor only a few, or you might monitor all of them.

The health of the metric category (green, red) indicates the health of the least healthy metric in the category. So a green (normal) indication for a metric category for a particular service means that all the metrics in that category that are being monitored for the service are in normal health. If any one of those metrics were in an alert state (red), then the indicator for the metric category for that service would also display that condition.

Similarly, the Overall indicator displays the health status of the least healthy service. So if any one service in one of the service locations is in an alert condition, this is displayed by the Overall indicator. Note that the Overall column indicates the overall health of just the services that are shown in the widget. If the definition of the widget filters out services or locations, these are not included in the status indicated by the Overall indicator.

Figure 3-3. Service Health by Location widget



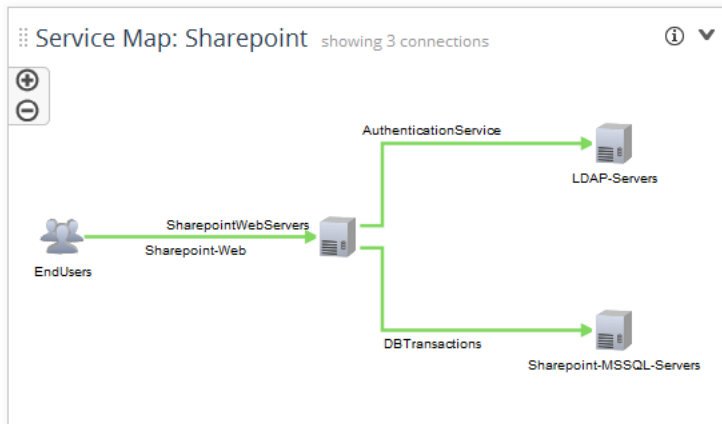
Service Tree		Overall	ERP	HR-Portal	Exchange	Sharepoint	FinancePortal
[-] Columbus		🔴	🔴	🟢	🟢	🟢	🟢
Connectivity		🟢	🟢	🟢	🟢	🟢	🟢
User Experience		🔴	🔴	🟢	🟢	🟢	🟢
Efficiency		🟢	🟢	🟢	🟢	🟢	🟢
[+] Philadelphia		🔴	🔴	🟢	🟢	🟢	🟢
[+] Phoenix		🔴	🔴	🟢	🟢	🟢	🟢
[+] Hartford		🔴	🔴	🟢	🟢	🟢	🟢
[+] SanFrancisco		🔴	🔴	🔴	🔴	🔴	🔴
[+] LosAngeles		🔴	🔴	🟢	🟢	🟢	🟢
[+] Austin		🔴	🔴	🟢	🟢	🔴	🟢
[+] Seattle		🔴	🔴	🟢	🟢	🟢	🟢

Service Map widget

A service map illustrates the relationships between the components of the network that are delivering the service and the connections between them. Services are monitored in terms of service segments, which are used for monitoring, reporting and alerting. A service segment is defined by a client component, a server component, and the applications and ports in use between them.

Service segments are displayed on a service map. Each segment is displayed with a label that identifies it. You can right-click a component or an application/port connection between two components for a menu of reporting options.

Figure 3-4. Service Map



The line representing the applications and ports in use between two components can be displayed in color. Lines are green to indicate normal traffic between components. They are red to indicate an alert condition.

All lines are gray until enough data has been collected to determine their health status. If health monitoring is not configured, and on reports that do not include health status, the lines are black. You can display the service map in several layout formats and adjust the layout by dragging and dropping components.

Service maps are available on the Dashboard page and in service reports. When you save, print or email a report that contains a service map, the display includes any zooming, panning, scaling, or layout modifications that you have made. The display can be either embedded in the email or attached as a PDF file. The display remains scaled and retains your layout modifications.

Service reports

Service reports provide high-level and detailed views of the performance of network services. The following service reports can be run from the Services > Reports menu or from the Reports > Shortcuts page:

- **Overall Performance Report** - presents a high-level view of how well all monitored services are performing.
- **Service Performance Report** - reports how well a service or a sub-component of a service has performed. This shows the current trends of the service and provides historical information about how the service performed over a specified time such as a week, month, quarter or year.
- **Service Incident Report** - shows the performance of a service or sub-component of a service over a short duration of time. This is useful for quickly determining why a dashboard health indicator is green or red.
- **Location Performance Report** - shows the health of a location, the health of services that include the location, and the health of front end segments for these services. This report provides quick indications of why a traffic indicator is green or red, when problems occurred, and for which components.

- **Location Incident Report** - indicates how well a location has performed across all services over a specific time range. This report shows current trends in the location as well as performance over time. This is useful for a high-level view, such as for end-of-quarter reports.

Overall Performance Report

The Overall Performance Report displays comparisons, trends, and summaries by alert conditions by service for the current or previous week, month, quarter or year. It has four sections:

- **Report Criteria** - Expand the Report Criteria section to choose a time frame for the report and to specify if the report format is to include breakdowns for all services.
- **Summary** - The Overall Service Health section indicates the percent of the time frame of the report that the services spent in normal and alert conditions. The Service Health by <time> section displays this information by smaller units of time than the time frame of the report for which data is available. For example, the report for a week displays the performance for each day.
- **Trends** - The Trends section display and lists the percent of the time frame of the report that each service has been in normal or alert conditions. It lists the five best-performing services and the five worst-performing services. For a report on a service listed in the table, right-click the name of the service and choose which report to run. For additional detail, you can add columns to the table from a column chooser tool.
- **Service Breakdown** - If this section is enabled in the Report Criteria section, it displays the performance for all services. If you have many services, you can limit the length of the table by choosing Change Number of Rows from the menu for this section. For additional detail, you can add columns to the table from a column chooser tool.

Figure 3-5. Overall Performance Report

Overall Performance Report ?



Service Performance Report

The Service Performance Report indicates how well a service or a sub-component of a service has performed. This shows the current trends of the service and provides historical information about how the service performed over a specified time such as a week, month, quarter or year.

The Service Performance Report has three sections:

- Report Criteria
- Summary
- Service Breakdown

All sections have menus for actions that can be performed on the section.

Report Criteria

The Report Criteria section allows you to select a service, service segment, location, metric category, or metric to report on. You can also limit the report to a time frame and location or metric. The section includes the following subsections:

- **Select Service Policy** - an expandable and collapsible tree diagram of service, service segment, location, metric category, and metric policies.
- **Report on** - sets the time frame of the report.
- **Additional Traffic Criteria** - provides lists for limiting the report to a selected location and a selected metric category.
- **Report Format** - determines whether the report includes a Service Breakdown section.

Figure 3-6. Service Performance Report - Report Criteria section

Service Performance Report ?

The screenshot shows the 'Report Criteria (default)' section of the Service Performance Report interface. It includes a tree view for 'Select Policy' with nodes for Exchange, ExchangeDirect, Austin, Columbus, Hartford, LosAngeles, Connectivity, Efficiency, User Experience, and Response Time. The 'Report on' dropdown is set to 'this week'. The 'Additional Criteria' section has dropdowns for 'Location' and 'Metric'. The 'Report Format' section has a checkbox for 'Show Detailed Service breakdown' which is checked. At the bottom are buttons for 'Run now' and 'Run in background...'. A 'Templates' dropdown is visible in the top right corner.

Summary of Events

The Summary of Events section of the report includes:

- **Service Summary** - this table show the following values for the time frame of the report:
 - Percent of time the system is available, which is defined as Normal health status.
 - Number of events that occurred.
 - Average duration of the events.
 - Duration of the worst event.
 - Element of the service that caused the most events.
- **Service Map** - a graphical representation of the service.
- **Service Health Breakdown** - percentage of time that the service was in normal and alert conditions.
- **Service Health Breakdown by <time>** - percentage of time that the service was in normal or alert conditions, broken out by smaller units of time than the time frame of the report. For example, the report for a week displays the performance for each day for which data is available.
- **Number of Events per <time>** - number of events that occurred, broken out by smaller units of time than the time frame of the report. For example, the report for a week displays the performance for each day for which data is available.
- **Average Event Duration by <time>** - the average duration of events broken out by smaller units of time than the time frame of the report.

Service Breakdown

If this section is enabled in the Report Criteria section, it displays the performance of the service, service segment, location, metric category, and metric in an expandable and collapsible tree table, as selected in the diagram in the Report Criteria section.

For additional detail, choose Add/Remove Columns from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table.

The columns in the table are sortable. Additionally, you can right-click the name of a service and run a service report on it.

Figure 3-7. Service Performance Report - Results

Service Performance Report ?



Service Incident Report

The Service Incident Report shows the performance of a service or sub-component of a service over a short duration of time. This is useful for quickly determining why a dashboard health indicator is green or red.

The Service Incident Report page has three sections:

- Report Criteria
- Event Summary
- Event List
- Service Breakdown

All sections have menus for actions that can be performed on the section.

Report Criteria

The Report Criteria section allows you to select a service, service segment, location, metric category, or metric to report on. You can also limit the report to a time frame and location or metric. The section includes the following subsections:

- **Select Policy** - an expandable and collapsible tree diagram of service, service segment, location, metric category, and metric policies.
- **Time frame** - specifies a length of time ending at the present time, or else a To/From time span.
- **Additional Criteria** - provides lists for limiting the report to a selected location and a selected metric category.
- **Report Format** - determines whether the report includes a Service Breakdown section.

Figure 3-8. Service Incident Report - Report Criteria section

Service Incident Report ?

Report Criteria (default) Templates ▾

Select Policy:

- ERP
 - Exchange
 - ExchangeDirect
 - Austin
 - Connectivity
 - Efficiency
 - User Experience
 - Response Time
 - Columbus
 - Hartford

Time frame:

☒ Previous Minute(s) ▾

☐ From:

To:

Additional Criteria

Location:

Metric:

Report Format

☒ Show Detailed Service breakdown

Figure 3-9. Service Incident report - Results

Service Incident Report ⓘ



Event Summary

The Event Summary section of the report includes:

- **Summary** - this table show the following values for the time frame of the report:
 - Number of events that occurred.
 - Duration of the worst event.
 - Health of the service element you are reporting on. Right-click the health indicator for a list of reports that you can run for this service.
- **Service Map** - a graphical representation of the service.
- **Segment Health** - displays the health of each segment of the reported service for each metric category. Click any segment name or health indicator (red, green) for a menu of reports that are available for it.
- **Location Health** - displays the health of each location of the reported service for each metric category. Click any location name or health indicator for a menu of reports that are available for it.

Event List

The Event List section presents the events that occurred within the time frame of the report in both graphical and tabular formats.

Active Events

The graph displays the number of events over time. Left-click and drag over a time period to zoom the graph to that period. The graph extends beyond the report time frame in order to provide more context for understanding the events.

Event List

The table lists all events that were active during the time frame of the report. By default, the table includes:

- **Event ID** - identifies the event that caused the alert condition. Click this to run an Event Details report.
- **Policy** - provides the full identification of the metric policy that triggered the alert.
- **Alert Level** - Low or High
- **Metric** - the name of the metric that the policy is monitoring.
- **Start time**
- **Duration**
- **Location**
- **Policy Actions** - the Tune link opens the Policy Tuning page for the policy. The Report link runs a Service Level Objective report for the location.

Many of the columns are sortable. For additional detail, choose Add/Remove Columns from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table.

For convenience in viewing, you can limit the length of the table by choosing Change Number of Rows from the menu for this section. The table can also be filtered.

Service Breakdown

This section displays an expandable breakdown of the selected service or service component. The Performance column displays the percentage of time that each component has been normal (green) and in an alert condition (red). You can use the section-level menu to add columns for additional metrics to the table.

Location Performance Report

The Location Performance Report can be run from the Services > Reports menu or from the Reports > Shortcuts page. It reports how well services and their sub-components at a location have performed. This shows the current trends of the service and provides historical information about how the service performed over a specified time such as a week, month, quarter or year.

The Location Performance Report page has three sections:

- Report Criteria
- Summary
- Service Breakdown

All sections have menus for actions that can be performed on the section.

Report Criteria

The **Report Criteria** section allows you to select a location, metric category, or metric to report on.

The section includes the following subsections:

- **Select Policy** - an expandable and collapsible tree diagram of location, metric category and metric policies.
- **Report on** - sets the time frame of the report.
- **Additional Criteria** - provides lists for limiting the report to a selected metric category.
- **Report Format** - determines whether the report includes a detailed location breakdown section.

Figure 3-10. Location Performance Report - Report Criteria section

Location Performance Report ?

Report Criteria (default) Templates ▼

Select Policy: Report on: this week ▼

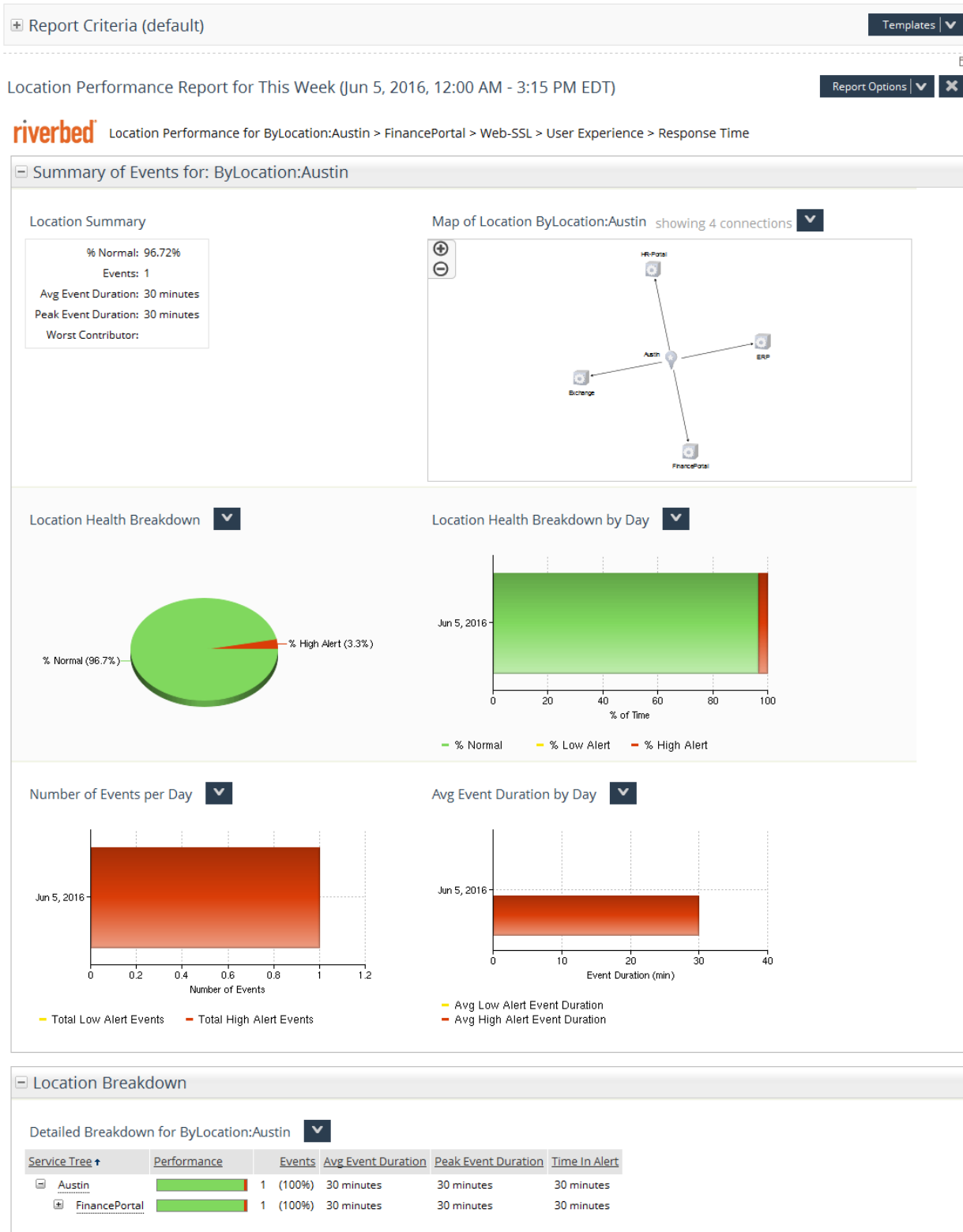
- Austin
 - ERP
 - Exchange
 - FinancePortal
 - Web
 - Web-SSL
 - Connectivity
 - Efficiency
 - User Experience
 - Response Time

▶ Additional Criteria
 ▶ Report Format

Run now Run in background...

Figure 3-11. Location Performance report - Results

Location Performance Report ?



Summary of Events

The Summary of Events section of the report includes:

- **Location Summary** - this table show the following values for the time frame of the report:
 - Percent of time the system is available, which is defined as Normal health status.
 - Number of events that occurred.
 - Average duration of the events.
 - Duration of the worst event.
 - Element of the service that caused the most events.
- **Location Map** - a graphical representation of the service by location.
- **Location Health Breakdown** - percentage of time that the service for the location was in normal and alert conditions.
- **Location Health Breakdown by <time>** - percentage of time that the service for the location was in normal or alert conditions, broken out by smaller units of time than the time frame of the report. For example, the report for a week displays the performance for each day for which data is available.
- **Number of Events per <time>** - number of events that occurred, broken out by smaller units of time than the time frame of the report. For example, the report for a week displays the performance for each day for which data is available.
- **Average Event Duration by <time>** - the average duration of events broken out by smaller units of time than the time frame of the report.

Location Breakdown

If this section is enabled in the **Report Criteria** section, it displays the performance of the metric category and metric for the location in an expandable and collapsible tree table, as selected in the diagram in the **Report Criteria** section.

For additional detail, choose **Add/Remove Columns** from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table. The columns in the table are sortable. Additionally, you can right-click the name of a service and run a service report on it.

Location Incident Report

The Location Incident Report can be run from the Services > Reports menu or from the Reports > Shortcuts page. It reports the health of services and their sub-components at a location. This is useful for quickly determining why a dashboard health indicator is green or red.

The Location Incident Report page has four sections:

- Report Criteria
- Event Summary
- Event List
- Location Breakdown

All sections have menus for actions that can be performed on the section.

Report Criteria

The **Report Criteria** section allows you to select a service, service segment, location, metric category, or metric to report on. You can also limit the report to a time frame and location or metric. The section includes the following subsections:

- **Select Policy** - an expandable and collapsible tree diagram of service, service segment, location, metric category, and metric policies.
- **Time frame** - specifies a length of time ending at the present time, or else a To/From time span.
- **Additional Criteria** - provides lists for limiting the report to a selected location and a selected metric category.
- **Report Format** - determines whether the report includes a Service Breakdown section.

Figure 3-12. Location Incident Report - Report Criteria section

Location Incident Report ?

Report Criteria (default) Templates | ▼

Select Policy:

- Austin
 - ERP
 - Exchange
 - ExchangeDirect
 - Connectivity
 - Efficiency
 - User Experience
 - Response Time
 - FinancePortal

Time frame:

☒ Previous Minute(s) ▼

☐ From: Jun 5, 2016 3:39 PM

To: Jun 5, 2016 3:40 PM

Additional Criteria

Metric: ▼

Report Format

☒ Show Detailed Location breakdown

Run now Run in background...

Event Summary

The **Event Summary** section of the report includes:

- **Summary** - this table show the following values for the time frame of the report:
 - Number of events that occurred.
 - Duration of the worst event.
 - Health of the service element for the location you are reporting on. Right-click the health indicator for a list of reports that you can run for this service.
- **Service Map** - a graphical representation of the service.
- **Location Health** - displays the health of each segment of the reported location for each metric category. Click any segment name or health indicator (red, green) for a menu of reports that are available for it.
- **Location Health** - displays the health of each location of the reported service for each metric category. Click any location name or health indicator for a menu of reports that are available for it.

Figure 3-13. Location Incident report - Results

Location Incident Report ⓘ



Event List

The **Event List** section presents the events that occurred within the time frame of the report in both graphical and tabular formats.

Active Events

The graph displays the number of events over time. Left-click and drag over a time period to zoom the graph to that period. The graph extends beyond the report time frame in order to provide more context for understanding the events.

Event List

The table lists all events that were active during the time frame of the report. By default, the table includes:

- **Event ID** - identifies the event that caused the alert condition. Click this to run an Event Details report.
- **Policy** - provides the full identification of the metric policy that triggered the alert.
- **Alert Level** - Low or High
- **Metric** - the name of the metric that the policy is monitoring.
- **Start time**
- **Duration**
- **Location**
- **Policy Actions** - the Tune link opens the Policy Tuning page for the policy. The Report link runs a Service Level Objective report for the location.

Many of the columns are sortable. For additional detail, choose **Add/Remove Columns** from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table. For convenience in viewing, you can limit the length of the table by choosing **Change Number of Rows** from the menu for this section. The table can also be filtered.

Location Breakdown

This section displays an expandable breakdown of service or service components for a selected location. The Performance column displays the percentage of time that each location or component has been normal (green) and in an alert condition (red). You can use the section-level menu to add columns for additional metrics to the table.

Managing services

The NetProfiler and NetExpress enable you to monitor the performance of services that your network provides to end users. A service might be a specific application, such as Exchange, Oracle or SAP, or it might be a combination of applications integrated through custom software. The appliance monitors the entire application delivery path of each service.

For services provided by multi-tiered applications, you can identify a series of service segments along the application delivery paths. This allows you to monitor performance and identify problems with greater resolution. You can receive an alert and run a report on any segment of the service to isolate a problem to a particular application, server, or link.

The NetProfiler and NetExpress define a *service* as all servers, clients, applications and ports involved in the end-to-end delivery of a network service. A service is composed of one or more *service segments* that can be monitored, reported and alerted on individually.

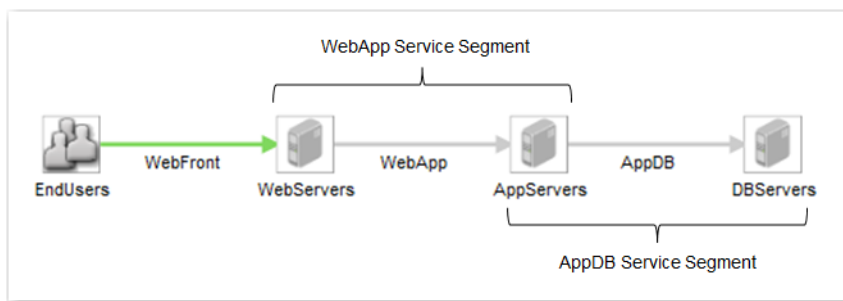
A *service segment* is composed of two components and the applications and ports in use between them. Each *component* is a group of hosts. Once defined, a component can be acting in the role of client in one service segment, but in the role of server in another service segment.

For example, in [Figure 3-14](#) the AppServers host group is the server component of the WebApp Service Segment and also the client component of the AppDB Service Segment. This indicates that hosts in the AppServers component are connecting to both the web servers and the database servers.

Each service segment comprises:

- Client component - a group of hosts that connect in the role of client
- Server component - a group of hosts that connect in the role of server
- Applications and ports in use between the client component and the server component

Figure 3-14. Service segments



Service segments can be defined by manually specifying the client and server components and manually specifying the applications and ports in use between them. Alternatively, you can use the service definition wizard to automatically discover hosts, applications, and ports involved in the service.

The service definition wizard provides many opportunities for manual intervention in adding, deleting, and editing the various elements comprising the service. You can use the **New Component** and **New Segment** buttons to add components and segments to a defined service manually. However, if you were to define a new service using the most simple and straightforward path through the wizard, it could proceed as follows:

First you assign a name for the new service. Then you assign a name for the front end server component of the service and provide the names or IP addresses of the front end servers making up that component.

Next you use the wizard to discover all the applications and ports that the end users use to connect to the server hosts in the front end component.

Some of the applications and ports the wizard discovers may not be involved in providing the service you want to monitor. The wizard enables you to review the applications and ports in use, look at the percentage of traffic that they account for, and decide whether or not they should be tracked as part of the service.

You identify the service segments (that is, the client-application/port-server combinations) that should be monitored as part of the service and add them to the service. You may be able to merge multiple applications and ports into the same segment where practical. For example, you might merge all client-server traffic for tcp/80, udp/80, and tcp/443 into one segment named “Web.” Conversely, you can drop or delete those client-application/port-server combinations that are not related to the delivery of the service.

Using this process of adding service-related traffic definitions and excluding information that should not be tracked as part of the service, you build up definitions of one or more front end segments.

The front end segments of the service are the starting point for defining additional segments, such as additional back-end applications/ports and components. The wizard helps you discover, organize, and label the additional pieces of the service.

Once you have identified all the segments of the service, you can specify which performance metrics are to be monitored for each segment.

When all the segments of the service are named and defined and the monitoring is specified, you commit the new service. As part of this process, the wizard automatically creates all the service policies necessary for monitoring the performance of each segment.

For step by step directions for defining a new service, refer to the online video tutorials or the online help system.

CHAPTER 4 Definitions

This chapter describes how to define applications, groups, port names and DSCP markings so that they can be tracked, reported, and alerted on. It includes the following sections:

- [“Applications,”](#) next
- [“Host groups”](#) on page 102
- [“Interface groups”](#) on page 108
- [“Port names”](#) on page 109
- [“DSCP”](#) on page 110
- [“Sensors/NetSharks and SteelHeads”](#) on page 111

Applications

NetProfiler and NetExpress identify applications that are communicating over the monitored network by matching traffic attributes against application definitions. If the traffic attributes match an application definition, then the traffic is included in the statistics for the application.

NetProfiler and NetExpress are shipped with definitions for common applications. When another supported device sends application identification information to NetProfiler and NetExpress, that information is added to the set of definitions.

Applications that NetProfiler and NetExpress recognize based on libraries of application definitions received from other sources are referred to as Auto-Recognized applications. Additionally, you can create custom application definitions by mapping traffic attributes to an application name.

Application definitions are managed on the Definitions > Applications page. This page has three tabs:

- General - for creating custom application definitions based on hosts, host groups, protocols, ports or Auto-Recognized applications.
- URL - for creating custom application definitions based on one or more URLs.
- Auto-recognized - for viewing a listing of all Auto-recognized applications.

The Definitions > Applications page includes a tab for each of these types of application definitions.

NetProfiler and NetExpress can track up to 2000 custom applications. This total could be:

- 2000 General application mappings and 0 URL application mappings

- 0 General application mappings and 2000 URL application mappings
- Any combination in between that totals 2000

General applications

General application mapping allows traffic between specified hosts and ports to be tracked and reported as application traffic. You can define a custom application by associating an application name with connections to a specific server host or group of server hosts using a specific port or group of ports. NetProfiler can then report on that application traffic.

Alternatively, you can assign a custom application name to an automatically-recognized application. You can make separate assignments of the same custom application name to multiple automatically-recognized applications and to applications defined by hosts and ports. This enables you to track and report on the group under a single custom application name.

The General tab of the Definitions > Applications page has two sections. The first section is for specifying search criteria for locating existing application mappings. The second section enables you to:

- Define a new custom application mapping.
- Edit an existing mapping.
- Change the priority of a mapping.
- Copy a custom mapping to use as the basis for defining a new one.
- Enable or disable mapping-based tracking of a custom application.
- Specify how the mapping should override automatically-recognized application definitions.

Searching and displaying the General application list

To locate an application definition by name, hosts or ports, enter or select the values in the General Applications section of the tab. This limits the list of application definitions to just those that match the criteria you specify.

Figure 4-1. Definitions > Applications page General tab

Applications ?

General URL Auto-Recognized (read-only)

General Applications

Application name:

Hosts or groups:

Ports:

Show known protocols/ports ☐ Apply

Application Mappings New...

Application	Host Definitions	Port Definitions	Priority	Override Policy	Enabled	Actions
No Data Available.						

Show: 20 entries per page

Selecting the “Show known protocols/ports” check box includes two types of system-defined applications in the list:

- **Known protocols** - If traffic uses a protocol known to the system but does not match any application mapping, it is tracked as belonging to a system-defined application for that protocol. The system-defined application is given the name of the protocol itself. If the protocol is not recognized, the system tracks it under one of the following application names: TCP_Unknown, UDP_Unknown, or IP_Proto_Unknown.
- **Known ports** - If a name is defined for a protocol/port combination on the Definitions > Port Names page, and if the “Generate App Mapping” check box is selected in that definition, then the system creates an application using that name and maps it to that protocol/port combination.

The system-defined application mappings cannot be edited on the Definitions > Applications page. Therefore, they are not listed unless you select the “Show known protocols/ports” check box.

When you click **Apply**, the application definitions that match your search criteria are listed in the Applications Mapping section of the tab. Each application has options in the Actions column. Choose a link in the Actions column to view, edit, delete or copy an application mapping.

Choose **Disable** to stop NetProfiler from tracking and reporting traffic for an application. Choose **Enable** to resume tracking and reporting.

If you do not specify any matching criteria in the General Applications section, the Application Mappings section displays all application mappings. This includes system-defined applications for legacy port groups.

NetProfiler and NetExpress Versions prior to 10.9.5 supported defining port groups. When the product is updated to version 10.9.5, port group definitions are automatically converted to General application definitions of the same name and given the “_portgroup” suffix. For example, a legacy port group named “web” is automatically converted to an application named “web_portgroup.” These new system-created definitions are listed with the General applications.

The update edits the dashboard widgets and scheduled reports that monitor port groups to reflect the changes. This enables you to continue to track and report on traffic previously defined for the port group.

Application definitions that the system creates from legacy port group definitions are listed with the other General application definitions and are fully editable.

Additionally, any Layer 4 application definitions you created before updating to version 10.9.5 or later are preserved “as is” and listed as General applications. They are also fully editable.

Creating a General application definition

There are two ways to create a new application definition on the Definitions > Applications page General tab:

- Choose the **New** button at the top of the Application Mappings list. This opens a section above the list for defining a new application.
- Choose **Copy** in the entry for an existing application. This opens a section above the list for defining a new application based in the existing application. The section is pre-populated with the definition of the mapping you copied. You can change the name and modify the definition as necessary to create the new application.

An application is defined by one or more mappings. You can create a mapping based on hosts or ports, or a mapping based on Auto-Recognized applications, but not both in the same mapping. To track traffic based on both hosts or ports and Auto-Recognized applications, create two separate definitions, both using the same application name. Map the hosts and ports to the custom application name in one definition. Map the Auto-Recognized applications to the custom application name in another definition.

A General application definition remains in effect until it is deleted or modified. It affects only new flows that begin after the mapping is created. A change to the definition affects only flows that begin after the change is made. On-going flows and historical flows continue to be reported as belonging to applications based on the definitions at the time they began.

Figure 4-2. Definitions > Applications page General tab - New Application Mapping**New Application Mapping**

Application mapping allows flows between specified hosts and server ports to be identified as application traffic without signature matching. (?)

Application name: <input type="text"/> Browse...	Hosts: <input type="text" value="Comma-separated list of IP addresses, CIDR blocks, or host groups."/> Browse...	Ports: <input type="text" value="Comma-separated list of ports."/> Browse...	Auto-Recognized Applications: <input type="text" value="Comma-separated list of auto recognized applications."/> Browse...
---	---	---	---

☒ Enabled

Override: ☒ Always - Unconditionally overwrite any existing layer 7 application mapping..
☐ Unknown - Apply to flows that did not match any Auto-Recognized applications or General Rules.

To create a mapping based on hosts and ports

- Go to the Definitions > Application page General tab.
- In the title bar of the Application Mappings section of the page, click **New**. This expands the page to display a section for defining a new application mapping.
 - Application name:** Enter the name for the new application as you want it to appear on reports and in the applications list. This can be up to 25 alphanumeric characters, periods and underscores. Alternatively, browse for an existing application name.
 - Hosts (optional):** Define the application in terms of a comma-separated list of the server hosts or server host groups that it uses:
 - hosts** – Enter as the names or IP addresses of hosts acting as servers, or enter the IP address ranges in prefix length notation of hosts acting as servers.
 - host groups** – Enter manually in the `server_host_group_type:host_group_name` format or else enter by browsing lists of server host group types and server host group names using the lookup tool.
 If this field is left empty, the mapping matches all hosts that use the ports specified in the Ports field.
 - Ports:** Define the application in terms of a comma-separated list of the ports that it uses:
 - tcp or udp ports** – Enter using protoport format, e.g., `tcp/80`
 - protocols other than tcp or udp** – Enter the protocol name. You can browse for ports and protocols using the lookup tool.
 - port number** – A port number is assumed to be a tcp or udp port. It is automatically translated into protoport format for display on reports. For example, “80” is interpreted as meaning `tcp/80` and `udp/80`.
 - port name** – browse for port name using the lookup tool.
- Select or deselect Enabled to enable or disable mapping-based tracking and reporting of the application.
- Specify in which cases, if any, the General definition of an application should override a Auto-Recognized definition:
 - Always** - Ignore any Auto-Recognized definition of the application and always use this definition.
 - Unknown** - Use this definition for classifying flows that do not match any Auto-Recognized application.

5. Click **OK** to add the definition to the Application Mappings list.

A custom application can be defined by more than one mapping. For each mapping, traffic on *any* host or host group in the hosts field is classified as belonging to the application if it uses *any* port specified in the ports field.

You can also define an application as traffic that involves *only* a particular host or host group that uses *only* a particular port. To do this, create multiple mappings for the same application name. For example,

```
My_app 172.16.0.100 tcp/40430
```

```
My_app 172.16.0.120 tcp/40440
```

This definition specifies the host and port combinations.

To create a mapping based on Auto-Recognized applications

1. Go to the Definitions > Application page General tab.
2. In the title bar of the Application Mappings section of the page, click **New**. This expands the page to display a section for defining a new application mapping.
3. In the Auto-Recognized Applications box, enter the name of one or more applications that the product recognizes automatically. Alternatively, choose Browse and use the search tool to locate the applications.
4. Select or deselect Enabled to enable or disable mapping-based tracking and reporting of the application.
5. For the Override policy, select **Always**. Because the mapping is applied to only flows that have been tagged with an Auto-Recognized application, setting this to **Unknown** will never result in a match.
6. Click **OK** to add the definition to the Application Mappings list.

Overlapping application definitions

NetProfiler and NetExpress can use a system of prioritizing application definitions to prevent traffic being reported multiple times when the same traffic attributes appear in more than one application definition. However, the priority assignments cannot be exported to NetShark or AppResponse 11 when those products are synchronized with NetProfiler or NetExpress. So if traffic matches more than one application definition, the total traffic for all elements of a display on NetShark or AppResponse 11 could be greater than the actual total traffic.

Application definition priorities

Each application mapping is assigned a priority. This allows you to use overlapping definitions. For example, assume that you have a group of servers in an address range and all but one of them is used for Application A. One of them will be used for Application B, but you don't know which one yet.

You can start by defining Application A as:

```
Application_A 172.16.0.0/12
```

At some later time, you can add the definition:

```
Application_B 172.16.0.100
```

You can then set the priority of the Application B definition to be higher than the priority of the Application A definition. NetProfiler looks at the highest priority definition first. So traffic to and from host 172.16.0.100 is classified as belonging to Application B. All traffic in the 172.16.0.0/12 range *except* for 172.16.0.100 is classified as belonging to Application A.

Application mappings are automatically assigned priorities at the time they are created. The first mapping you create is assigned Priority 1 (the highest priority). The second mapping you create is assigned Priority 2, and so forth.

NetProfiler or NetExpress looks for traffic that meets Priority 1 mapping first. If it finds traffic that matches the first priority mapping, it designates the traffic as belonging to that application. If the traffic does not match the first priority mapping, then NetProfiler checks it against the Priority 2 mapping.

NetProfiler or NetExpress continues to successively check traffic information against mappings. Therefore, it is recommended that you assign first priority to the application with the highest volume of traffic.

If you change a priority or delete an application mapping, all priority levels are automatically adjusted so that there are no gaps in the sequence of priorities.

System-generated mappings (known protocols and known ports) are automatically a lower priority than any user-created application mapping. The priority of system-generated mappings cannot be changed.

To change an application mapping priority

1. Go to the Definitions > Application page General tab.
2. Locate the application in the Application Mapping section.
3. In the Priority column, choose the priority number. This opens a window in which you can specify the priority.
4. Enter the new priority for the application mapping.

URL applications

NetProfiler and NetExpress can track and report traffic based on URLs. On the Definitions > Applications page URL tab you can define a custom application as traffic using any of up to ten URLs.

The URL tab of the Definitions > Applications page enables you to:

- Search and display the list of applications defined by one or more URLs.
- Add a new URL-based application definition.
- View or Edit a URL-based application definition.
- Copy a URL-based application definition to use as the basis for defining a new one.
- Enable or disable tracking of traffic matching a URL-based application definition.

Figure 4-3. Definitions > Applications page URL tab

The screenshot shows the 'Applications' page with the 'URL' tab selected. At the top, there are three tabs: 'General', 'URL', and 'Auto-Recognized (read-only)'. Below the tabs, there is a section for adding a new application with a text input for 'Application name' and an 'Apply' button. Below this is a section titled 'Url Applications' with a 'New...' button. A table lists existing applications with columns for 'Application name', 'Description', and 'Actions'. The table contains one entry: 'soak_appL72'. The 'Actions' column for this entry includes links for 'View', 'Edit', 'Delete', 'Copy', and 'Disable'. At the bottom, there is a pagination control showing 'go to page 1' and 'Show: 20 entries per page'.

Application name	Description	Actions
soak_appL72		View Edit Delete Copy Disable

Versions prior to 10.9.5 supported the use of URLs to define custom Layer 7 applications. When the product is updated to version 10.9.5 or later, previous URL-based Layer 7 definitions are listed on the URL tab.

Searching for a URL-based application definition

URL-based application definitions are listed in the URL Applications section of the Definitions > Application page URL tab.

To search for a URL-based application definition

1. Go to the Definitions > Application page URL tab.
2. In the URL Applications section, enter the name of the application you want to search for.
3. Choose **Apply**. If the application is recognized, it will be listed in the URL Applications section.
4. In the Actions column of the URL Applications section, choose the action you want to perform.

Creating a new URL-based application definition

There are two ways to open the “New URL Application” section of the Definitions > Application page URL tab:

- Choose **New** in the URL Applications section.
- Locate an existing definition that is similar to the one you want to create. In the entry for the similar definition, choose **Copy** in the Actions column. This opens the “New URL Application” section with the fields already containing the values of the definition you copied. You can change the name and modify the definition to create a new definition.

Figure 4-4. Definitions > Applications page URL tab New URL Application Section

New Url Application

Custom url application can be created by specifying a URL. (?)

Name:	Signature(s)
<input type="text"/>	<div> <div>URL</div> <div><input type="text"/></div> <div>remove</div> </div>
	Add new signature

☒ Enabled

OK Cancel

To create a new URL-based application definition

1. Go to the Definitions > Application page URL tab.
2. In the title bar of the URL Applications section, click **New**. This expands the page to display a section for specifying a new definition.
3. Enter the name for the new application as you want it to appear on reports and in the applications list. This can be up to 25 alphanumeric characters, periods and underscores.
4. Enter a URL in http format, such as <http://www.riverbed.com> or <http://www.riverbed.com/solutions>. You can use an asterisk as a wildcard at the beginning or end of a URL. For example,

- `http://*.foo.com/`
 - `http://www.foo.com/bar*`
 - `http://*.foo.com/bar*`
5. If you want to define more than one URL for the application, choose the “Add new signature” link display additional fields for specifying URLs. One application definition can include up to 10 URLs.
 6. Select or deselect **Enabled** to enable or disable URL-based tracking and reporting of the application.
 7. Click OK to add the definition to the applications list.

If you specify multiple URLs, the traffic needs to match only one. The relationship among the definitions is OR (and not AND).

If more than one URL matches, the most specific URL that matches is used. For example, assume you define:

`http://intranet.domain.com`

`http://intranet.domain.com/app1`

The second definition is more specific than the first and therefore it takes precedence over the first.

Notes on monitoring social media usage

If you are monitoring or alerting on the usage of social media web sites, then additional considerations apply.

There are several ways in which traffic from sites such as Facebook, Twitter and YouTube can be associated with specific users:

- User login to service – If a user logs in to one of these applications, you can track their usage.
- Embedded content – Many web sites pull content from YouTube, Facebook, Twitter and other sites and display a small amount for visitors to see. If a user visits a web site that has embedded content from one of these applications, NetProfiler can detect the packets that the web site automatically obtains for displaying. Even though the user did not visit the social media site, the packets retrieved for the embedded content will be associated with the user’s IP address.
- User login credentials – Some services, such as AOL instant messenger, allow a user to log in using their Facebook or Twitter login credentials. When a user does this, NetProfiler can detect the application packets involved in the login process. So even though the user has not logged in to Facebook or Twitter, there will be a small number of packets from those applications associated with the user’s IP address.

If you do not want to track social media traffic generated by embedded content on web sites or by users logging in to other services with their social media credentials, you can create a user-defined policy that alerts on only traffic flows of more than the small amount required for these other actions.

Auto-recognized applications

SteelCentral Flow Gateway receives flow information from a variety of sources and sends it to NetProfiler. NetExpress receives flow information from a variety of sources and also from monitoring network traffic. Many of the flow collectors that provide this information also recognize the applications that are producing the flows they are monitoring. NetProfiler and NetExpress obtain application identification information from the following sources:

- Sensor - information provided by a Cascade Sensor.
- AppResponse 11 - information provided by an AppResponse 11.
- SteelConnect Manager - information provided by a SteelConnect Manager

- Palo Alto Networks - information provided by a Palo Alto Networks product.
- AppFlow - information provided by a Citrix product that supports AppFlow.
- NBAR - requires a Cisco device to be sending Network-Based Application Recognition data to NetProfiler.
- Packeteer - requires a compatible Packeteer device to be sending Flow Detail Records to NetProfiler.
- NetShark - information provided by a NetShark.
- SteelHead - requires the SteelHead to be sending SteelFlow Net information to NetProfiler.

Application names from each of these sources are displayed on the Definitions > Applications page Auto-Recognized tab. On this tab you can:

- Search for an application by name. To search for an application, enter the application name, select the applicable “Show sources” criteria, and then click **Apply**.
- Filter the application list to names provided by selected sources. Select the applicable “Show sources” criteria and click **Apply**.
- Specify which sources of Auto-Recognized application names are used for the look-up and auto-complete features used elsewhere in NetProfiler. (General and URL-based application names are always offered as auto-complete options.) In the “Include applications from these sources in lists” section, select one or more sources and click **Save Settings**.

The application definitions listed on this page are read-only with the exception of custom Layer 7 applications that were defined before version 10.9.5 of the product. Legacy Layer 7 definitions that are based on hex numbers or text strings are preserved when the product is updated. They become read only. They can be deleted but not modified. They will continue to be pushed to Cascade Sensor devices and they can continue to be used "as is" on NetProfiler or NetExpress. However, they cannot be pushed to NetShark or AppResponse 11 when the application definitions on those products are synchronized with NetProfiler or NetExpress.

Figure 4-5. Definitions > Applications page Auto-Recognized tab

Applications ?

General

URL

Auto-Recognized (read-only)

Auto-Recognized Applications

Application name:
Show sources:

- ☒ Sensor
- ☒ AppResponse 11
- ☒ SteelConnect Manager
- ☒ Palo Alto Networks
- ☒ AppFlow
- ☒ SteelHead
- ☒ NBAR
- ☒ Packeteer
- ☒ User Defined
- ☒ NetShark

Apply

Application autocomplete configuration

Include applications from these sources in lists
(autocomplete, lookup and dashboard)

Include:

- ☒ Sensor
- ☐ AppResponse 11
- ☐ SteelConnect Manager
- ☐ Palo Alto Networks
- ☐ AppFlow
- ☒ SteelHead
- ☐ NBAR
- ☐ Packeteer
- ☒ NetShark

Save Settings

Applications 1 - 20 of 1754

Application name +	Sources	Description	Actions
050Plus	NetShark	The traffic consists of data from logging in or making calls with the 050Plus application.	

Host groups

The appliance enables you to assign hosts to groups so that you can track, report and alert on organizationally meaningful categories of traffic, such as traffic by host function or traffic by host location. This allows you to view the traffic of the same hosts from multiple perspectives. For example, email servers in New York could belong to a group named “email” if you are using the by-function view of the network, or to a group named “New York” if you are using the by-location view of the network.

You can use any of the following approaches to create a host group:

- Manually define a group. You can use an edit box to enter a list of hosts that define a host group.
- Create a host group from a table. When you run a report that displays a table with columns for host names or host IP addresses, you can use the hosts in the table to create a new host group, redefine an existing host group, or replace an existing host group.
- Import a text file. You can identify the members of a group in a text file and then import the file to the appliance as a group definition.

In addition, the NetProfiler or NetExpress itself creates certain host groups. When SteelHead appliances are configured to send configuration information to the NetProfiler or NetExpress, the NetProfiler or NetExpress automatically defines a host group type for each SteelHead appliance. Within that host group type, each SteelHead site is treated as a host group. Within the host group for each SteelHead site, traffic between hosts is reported just as traffic between hosts that are not associated with a SteelHead.

Because there may be a large number of SteelHead appliances in a network, the NetProfiler and NetExpress hide SteelHead groups by default. If you want to include SteelHead group types and host groups (SteelHead site traffic) in reports that display host groups, you must enable the display of SteelHead appliance-based group types and groups. This is done in the Favorites column of the Definition > Host Groups > Manage Host Group Types page.

The number of host groups defined for the host group type used in service monitoring (by default the ByLocation host group type) should be limited to 500. However, you can define thousands of host groups of other host group types.

Refer to the online help system for details on creating or modifying host groups.

Host grouping pages

The appliance is shipped with three types of grouping already defined: ByFunction, ByInternalHosts and ByLocation. These group types are listed on the submenu under Definitions > Host Groups.

Each group type is organized on the basis of some common host attribute, such as their function, their address being inside or outside of your network, or their physical location. Hosts that perform the same function or hosts that are in the same location can be tracked, reported, and alerted on as groups.

Host groups can be named after the functions, locations, or other attributes of their members. For example, for the ByFunction view of the network, you organize hosts into groups such as Web, Email, DNS, DMZ, etc. Similarly, for the ByLocation view, you organize hosts into groups named after their locations.

Host group names must not have spaces or special characters.

The page has two sections: Groups and Members of Group.

Groups

The Groups section can be sorted by host group name or by the size of the group. The Host Count column reports how many hosts belong to each group.

Figure 4-6. Definitions > Host Groups page ByFunction view

Manage Host Group Types ?

Host Group Type: ByFunction

Manage Host Group Types

Description: Groups based on the function of their member hosts, such as Email, Web, etc.

Groups 1 - 10 of 20

Edit Groups...

Members of Group: DB

View Definition...

Name ↑	Host Count	Actions
(+) add filter	(+) add filter	
DB	0	View members
Desktops	0	View members
DMZ	0	View members
DNS	0	View members
Email	0	View members
Exchange	0	View members
FinanceApp_AppServers	0	View members
FinanceApp_DBServers	0	View members
FinanceApp_WebServers	0	View members
NotesSrvs	0	View members

1 2 go to page 1

Show: 10 entries per page

Host IP ↑	Host Name
No Data Available.	

The Add Filter control in the Name column enables you to limit the list of groups to just those groups whose names match specified filter criteria. The Add Filter control in the Host Count column enables you to limit the list of groups to just those having a specified size. The values (filter phrases) used for filtering the table contents are specified the same way as for report table filtering.

Left-click or right-click the host group name to run a report about the group. Click View Members in the entry for a host group to display a list of the hosts that belong to the group.

The Edit Groups link in the title bar of the Groups section opens a window in which you can modify the definitions of the groups of this group type.

Members of Group

The Members of Group section lists the hosts belonging to the group that is highlighted in the Groups section. Click the Host IP column heading to sort the list of hosts by IP address. If the appliance has DHCP integration configured, you can also view the members of the group by their host names.

The View Definitions button in the title bar of the Members of Group section displays the definition of the group whose members are displayed in that section.

Figure 4-7. Definitions > Host Groups page ByFunction view Edit Groups function

Edit Group Type ByFunction

Group Type Information

To create a view, provide a name. The name cannot contain spaces.

Group type name:

Description:

Identify Groups in this Group Type

A host can appear in only one group (within this group type). To create a group, specify a group definition and name, using the format shown below. Click Import to import group definitions from a file ([view the proper file syntax](#)).

```

10.0.0.1/32 Web
10.0.0.18/32 DNS
10.1.4.0/24 PoS
10.7.0.0/24 PoS_backend
10.7.3.1/32 FinanceApp_AppServers
10.8.0.0/16 DMZ
10.8.0.61/32 PCI_Servers
10.8.0.153/32 FinanceApp_WebServers
10.9.0.0/16 DMZ
10.9.0.1/32 PCI_Servers
10.10.2.30/32 Desktops

```

Figure 4-8. Definitions > Host Groups page ByFunction view View Definitions function

'ByFunction' definition

The definitions for the selected group are highlighted.

```

0.0.0.4/32 DB
10.0.0.1/32 Web
10.0.0.18/32 DNS
10.1.4.0/24 PoS
10.7.0.0/24 PoS_backend
10.7.3.1/32 FinanceApp_AppServers
10.8.0.0/16 DMZ
10.8.0.61/32 PCI_Servers
10.8.0.153/32 FinanceApp_WebServers
10.9.0.0/16 DMZ
10.9.0.1/32 PCI_Servers
10.10.2.30/32 Desktops
10.10.2.57/32 FinanceApp_DBServers
10.12.14.100/32 FinanceApp_WebServers
10.12.15.102/32 Desktops
10.12.16.102/32 Desktops
10.12.21.100/32 FinanceApp_WebServers
10.49.2.67/32 NotesSrvs
10.49.2.68/32 NotesSrvs

```

Defining host groups

Define host groups by specifying an address range and a group name, using one definition per line. You can use either or both of two syntaxes for specifying address ranges:

- CIDR - an IP address with a prefix that specifies how many bits of the host address must match the group definition
- Subnet mask - an IP address with a subnet mask that indicates just which bits of the host address must match the group definition

CIDR notation may be simpler if your network organizes addresses consecutively by function. The subnet mask technique may be better suited to networks with repeating address schemes.

Defining host group membership using CIDR notation

On each line, specify the address range using CIDR notation, followed by a space, followed by a group name with no spaces in it. For example,

```
10/8 group1
172.168.1.1 group2
192/8 group1
```

In this example, both 10/8 and 192/8 are assigned to group1.

Note: If you use overlapping IP address ranges in the custom group definitions, the appliance assigns a host to the custom group whose definitions has the longest matching prefix. For example, if you are specifying custom host groups corresponding to network segments “net-a” and “net-b,” a specification file containing:

```
10.0.0.0/8 net-a
10.15/16 net-b
```

will cause an address such as 10.15.16.23 to be assigned to the net-b group.

Defining host group membership using subnet mask notation

Where greater flexibility is required, you can specify address ranges using standard 4-quad bit mask notation. The bit mask specifies which bits of a host IP address must match the bits in the group definition in order to be included in the group.

On each line, specify the address range using bit mask notation, followed by a space, followed by a group name with no spaces in it. For example,

```
192.168.0.100/255.255.0.255 MyServers
```

Note: If you use overlapping IP address ranges in the custom group definitions and a host address matches more than one group definition, the appliance applies the following rules of precedence to determine the group under which the host is tracked.

1. Most matching bits - The host is assigned to the group for which it has the largest number of matching bits.
2. Highest value bits - If both matches involve the same number of bit matches, the appliance assigns the host to the group for which it has the largest value of matching bits.
3. Higher address - If the number and value of the matching bits are both the same, the appliance assigns the host to the group with the higher (larger) IP address in its definition.
4. Undefined - If none of these rules can be applied, the appliance assigns the host to one or another of the matching groups so that its IP address will be tracked.

Examples

CIDR notation technique

The CIDR technique is usually adequate if you organize your hosts such that they have consecutive IP addresses. For example, assume that addresses are assigned first to email servers and then to database servers:

192.168.1.1 - Boston_mail_server

192.168.1.2 - LA_mail_server

192.168.1.3 - Chicago_mail_server

192.168.2.1 - Boston_database_server

192.168.2.2 - LA_database_server

192.168.2.3 - Chicago_database_server

In this case, you could define two host groups using CIDR notation:

192.168.1.0/24 mail_servers

192.168.2.0/24 database_servers

Subnet mask technique

The subnet mask technique may be required for more complex address assignment schemes. For example, assume that a company assigns its addresses first by its divisions and then, within each division, by function:

192.168.1.1 - Boston_mail_server

192.168.1.2 - Boston_database_server

192.168.2.1 - LA_mail_server

192.168.2.2 - LA_database_server

192.168.3.1 - Chicago_mail_server

192.168.3.2 - Chicago_database_server

In this case, all the mail server addresses are x.x.x.1 and all the database server addresses are x.x.x.2. So you can use the subnet mask technique to ignore the third octet of the host IP address, which identifies the division or location but not the server:

192.168.0.1/255.255.0.255 mail_servers

192.168.0.2/255.255.0.255 database_servers

Managing host group types

The Definitions > Host Groups > Manage Host Group Types page lists all the currently defined group types.

Figure 4-9. Definitions > Host Groups > Manage Host Group Types page

Manage Host Group Types

NetProfiler provides enterprise-wide views of the entire monitored network based the type of groups you define. For example, you can assign hosts to host groups on the basis of their locations, and then view all host groups of the group type ByLocation. This page lists the types of groups by which you can organize hosts on the network. Each group type includes all hosts on the monitored network, organized into groups of that group type. For each group type, you can view the definitions of individual groups that are defined for that group type. For user-defined groups, you can also modify these definitions.

Group Types 1 - 10 of 11

New...

Favorites	Name ↓	Description	Type	Actions
<input checked="" type="checkbox"/>	ByApp	demo_ByApp	User-created	View Edit Delete
<input checked="" type="checkbox"/>	ByCompliance	demo_ByCompliance	User-created	View Edit Delete
<input checked="" type="checkbox"/>	ByFunction	Groups based on the function of their member hosts, such as Email, Web, etc.	User-created	View Edit Delete
<input checked="" type="checkbox"/>	ByInternalHosts	Groups containing hosts with addresses in the ranges specified as Inside Addresses on the Profiler Setup > General Settings page.	System-created	View Edit Delete
<input checked="" type="checkbox"/>	*ByLocation	Groups based on the location of their member hosts, such as NY, Dallas, DataCenter1, etc.	User-created	View Edit Delete
<input type="checkbox"/>	SH-Austin		System-created	View Edit Delete
<input type="checkbox"/>	SH-Columbus		System-created	View Edit Delete
<input type="checkbox"/>	SH-DataCenter		System-created	View Edit Delete
<input type="checkbox"/>	SH-Phoenix		System-created	View Edit Delete
<input type="checkbox"/>	SH-SanFrancisco		System-created	View Edit Delete

1 2 go to page 1 Show: 10 entries per page

* 'ByLocation' is your default group type, according to your [UI Preference](#).

The Manage Host Group Types page provides following controls:

- Favorites column check boxes - Default group types and user-defined group types are selected as favorites by default. This means that they are available on all pages where you can select host group types. This includes look-up tools, drop-down list boxes and fields that auto-complete as you enter a name.

System-created group types are deselected by default. The NetProfiler and NetExpress automatically create a group type for each SteelHead appliance that sends them information. A large network may have hundreds of SteelHead appliances. To keep list boxes manageable, these group types are hidden from selection lists unless you select them as favorites on the Definitions > Host Groups > Manage Host Group Types page.

- View - View a list of groups that have been defined for a group type by clicking **View** in the entry for that group type. This displays a page listing the groups of the selected group type. On that page you can also view and edit the members of each group of the group type.
- Edit - Edit the name or description of a group type by clicking the **Edit** in the entry for that group type.
- Delete - Delete a group type by clicking the **Delete** in the entry for that group type.
- New - Define a new group type (i.e., a new way of viewing hosts on the network) by clicking the **New** button.

Interface groups

The NetProfiler and NetExpress appliances track traffic volumes and utilization percentages (where available) on a per-interface basis for all interfaces from which it receives traffic information. For convenience, you can aggregate interface statistics into groups. You can define policies for interface groups to generate an alert if a specified condition occurs. You can also generate reports to provide an interface-oriented view of network performance.

To simplify network monitoring and troubleshooting, you can define views of your network based on regions, locations, business groups, functions or other classification attributes. Each “network view” can include all relevant interface groups. Each interface group can contain subgroups and individual devices and interfaces. All devices and device interfaces that are sending traffic information to the appliance can be listed by a search tool for easy selection and inclusion in an interface group or a network view.

Adding a device to a group adds all the device’s interfaces that are sending data to the appliance. Adding a “reporting device,” such as the Flow Gateway appliance, adds all that device's routers and all the routers' interfaces. If additional interfaces on that device begin sending data to the appliance at some future time, they are automatically added to the interface group also.

Figure 4-10. Definitions > Interface Groups page

Interface Groups [?](#) [See Tutorials](#)

Network Views

- WAN
 - Non-optimized
 - Optimized**
- VXLAN
 - hr
 - oper
 - sales

System Interface Group: Edit

Name: /WAN/Optimized
Description: WAN interfaces of Steelhead and other WAN optimization devices

Members of System Interface Group: Optimized [Find Steelheads](#) [Delete selected](#) [▼](#)

Type	Name	Description	Device Address	Interface Index
SH-Austin:wan0_0	Steelhead NetFlow	10.99.16.252	2	
SH-Columbus:wan0_0	Steelhead NetFlow	10.99.14.252	2	
SH-DataCenter:wan0_0	Steelhead NetFlow	10.100.100.252	2	
SH-LosAngeles:wan0_0	Steelhead NetFlow	10.99.12.252	2	
SH-Phoenix:wan0_0	Steelhead NetFlow	10.99.13.252	2	
SH-SanFrancisco:wan0_0	Steelhead NetFlow	10.99.15.252	2	
SH-Seattle:wan0_0	Steelhead NetFlow	10.99.11.252	2	

go to page 1 Show: 10 entries per page

You can use the Definitions > Interface Groups page to:

- Define a network view.
- Define interface groups within a network view.
- Add interfaces and devices to an interface group.
- Define subgroups within an interface group.
- Add interfaces and devices to a network view.
- Move or copy groups, devices or interfaces between groups using drag & drop.
- Import or export an interface group or network view.
- Delete interfaces, devices, interface groups and network views.

Refer to the online help system for descriptions of each of these procedures. Note that VXLAN views are not editable except for the names and descriptions assigned to their virtual network identifiers.

After interface groups and network views have been set up, interface performance can be monitored on the Home > Navigate Network page.

Port names

The Port Names page allows Operators and Administrators to:

- View a histogram of the traffic volumes of selected ports or all ports that are using TCP or UDP or both.
- Add new ports to the list of ports that the appliance knows by name.
- Rename ports. The ports tracked by default correspond to the standard services defined by the Internet Assigned Numbers Authority (IANA).
- Import a standard /etc/services file so that the appliance displays and reports use your custom names for ports.
- Specify ports as being server ports.
- Specify ports for which the system automatically creates an application.

The Page Settings section allows you to filter the list of ports displayed in the Selected Ports section.

Figure 4-11. Definitions > Port Names page

Port Names ⓘ

Page Settings

Select Type:

Select Protocol:

Select Port Numbers: (e.g., 80, 512-556)

Select Port Names: (e.g., http, exec)

☐ Show Port Traffic Histogram

Click Apply to show ports

...

Show: entries per page

Selected Ports From Database (1 - 10 of 100)

<input type="checkbox"/>	Name	Protocol	Port ↑	Avg Bits/Second*	Server Port	Grouped
<input type="checkbox"/>	tcpmux	TCP	1	0	yes	no
<input type="checkbox"/>	compressnet	TCP	2	0	no	no
<input type="checkbox"/>	compressnet	TCP	3	0	no	no
<input type="checkbox"/>		TCP	4	0	no	no
<input type="checkbox"/>	rje	TCP	5	0	yes	no
<input type="checkbox"/>		TCP	6	0	no	no
<input type="checkbox"/>	echo	TCP	7	0	yes	no
<input type="checkbox"/>		TCP	8	0	no	no
<input type="checkbox"/>	discard	TCP	9	0	yes	no
<input type="checkbox"/>		TCP	10	0	no	no

* Counters accumulated between: May 26, 2016 8:53 AM - Jun 6, 2016 5:24 PM

The port list includes all currently defined ports.

To define additional ports

1. Go to the Definitions > Port Names page.
2. Click **New** at the top of the table listing the ports.
3. Select the protocol and enter the name and number of the new port.
4. Click **Server Port** if applicable. This is necessary to ensure proper tracking.

5. Click **Generate App Mapping** to have the system automatically create an application for tracking and reporting traffic on this port. The application name will be based on the port name.
6. Define additional ports as necessary.
7. Click **OK**.

Refer to the online help system for descriptions importing and editing port definitions.

DSCP

The appliance tracks DSCP markings associated with traffic flows in the network. It can report which markings were seen by devices that report flow data. The presence or absence of specified DSCP markings can be used as reporting and alerting criteria.

DSCP marking reporting is based on the 6-bit Differentiated Services Code Point (DSCP). By default, the appliance uses a standard set of definitions for DSCP values. You can modify these or define additional names and descriptions on the Definitions > DSCP page.

The DSCP page lists DSCP markings by their decimal, binary, and hexadecimal values, and by names and descriptions. Click any column heading to sort by ascending or descending order.

Figure 4-12. Definitions > DSCP page

DSCP Marking (QoS) ⓘ

The NetProfiler tracks and allows reporting on the Quality of Service, using DSCP Marking, associated with flows in the network.

DSCP
Edit

DSCP	Binary	Hex	Name	Description
0	000000	00	Default	Default
1	000001	01		
2	000010	02		
3	000011	03		
4	000100	04		
5	000101	05		
6	000110	06		
7	000111	07		
8	001000	08	CS1	Class Selector 1
9	001001	09		
10	001010	0A	AF11	Assured Forwarding Class 1 Low Drop
11	001011	0B		
12	001100	0C	AF12	Assured Forwarding Class 1 Medium Drop
13	001101	0D		
14	001110	0E	AF13	Assured Forwarding Class 1 High Drop
15	001111	0F		
16	010000	10	CS2	Class Selector 2

Sensors/NetSharks and SteelHeads

When links in a network are using WAN optimization, the NetProfiler or NetExpress must receive data from a Sensor or NetShark monitoring traffic on the LAN side of the SteelHead that is located on the server side of the optimized connection. This is necessary in order to determine server delay time and network response time.

The Definitions > Sensors/NetSharks & SteelHeads page enables you to specify Sensors and NetSharks that are monitoring the LAN on the server side of the WAN optimization devices.

Figure 4-13. Definitions > Sensors/NetSharks & SteelHeads page

Sensors/NetSharks & SteelHeads ⓘ

For accurate reporting of server delay and response times, identify all Sensors/NetSharks that are monitoring the LAN-side traffic of SteelHeads that are likely to act in the role of server-side SteelHead for optimized traffic flows. Check the dynamic assignments and make static assignments as necessary.

Sensors/NetSharks & SteelHeads New...

Sensor/NetShark Address	Sensor/NetShark Hostname	SteelHead Address	SteelHead Hostname	Type ↓	Actions
10.99.11.253	shark-Seattle	10.99.11.252	SH-Seattle	Static	Edit Delete
10.99.12.253	shark-LosAngeles	10.99.12.252	SH-LosAngeles	Static	Edit Delete
10.99.13.253	shark-Phoenix	10.99.13.252	SH-Phoenix	Static	Edit Delete
10.99.14.253	shark-Columbus	10.99.14.252	SH-Columbus	Static	Edit Delete
10.99.15.253	shark-SanFrancisco	10.99.15.252	SH-SanFrancisco	Static	Edit Delete
10.99.16.253	shark-Austin	10.99.16.252	SH-Austin	Static	Edit Delete
10.100.100.253	shark-DataCenter	10.100.100.252	SH-DataCenter	Static	Edit Delete

⏪ ⏩ 1 ⏪ ⏩ go to page Show: entries per page

When the WAN optimization is being performed by Riverbed SteelHeads, the NetProfiler or NetExpress requires the following information in order to measure server delay and compute response time for reporting network performance:

- SteelFlow Net or SteelFlow Net-compatible data from the SteelHeads at both ends of the WAN.
- Traffic statistics from a Sensor that is monitoring the LAN that the server-side SteelHead is connected to.

The NetProfiler automatically discovers which Sensors are associated with SteelHeads that are acting in the role of being on the server side of the WAN. It does this whenever it has sufficient data to make the association. It adds these associations to the Sensors/NetSharks & SteelHeads section and lists them as “Dynamic” in the type column. They are dynamic in the sense that the NetProfiler automatically deletes them when they become stale and reassigns them when new associations are discovered, based on its analysis of the role that the SteelHeads are performing.

The NetProfiler does not automatically discover which NetShark is closest to the LAN side of a SteelHead. For NetShark appliances, and for Sensors that the NetProfiler did not have enough data to discover automatically, you must make the association manually as a “Static” assignment. Click **New** on the Definitions > Sensors/NetSharks & SteelHeads page to display a section in which to make the assignment.

When you make a static assignment, your assignment remains in effect until you edit it or delete it. The dynamic discovery and maintenance features do not affect your static assignments.

For accurate reporting of server delay and response times, use this page to identify all Sensors and NetSharks that are monitoring the LAN-side traffic of SteelHeads that are likely to act in the role of server-side SteelHead for optimized traffic flows.

WAN

In order to analyze WAN performance and identify opportunities for WAN optimization, the NetProfiler or NetExpress appliance must know which network interfaces are part of a WAN, which of these are using a WAN optimization device, and which are not. It automatically creates Optimized and Non-optimized interface groups. It recognizes WAN interfaces that are on SteelHead devices of version 5.5.3 or higher if the SteelHead is exporting NetFlow 5.1 or SteelFlow Net and automatically adds these Optimized interface group. You can use the Find SteelHeads button to automatically populate the group with SteelHead WAN interfaces. Other WAN interfaces must be added to the groups using the browse tool.

Figure 4-14. Definitions > WAN page

System Interface Group: [Edit](#)

Name: /Optimized
Description: WAN interfaces of Steelhead and other WAN optimization devices

Members of System Interface Group: Optimized [Find Steelheads](#) [Delete selected](#) [▼](#)

Type	Name	Description	Device Address	Iface Index
SH-Austin:wan0_0	SH-Austin:wan0_0	Steelhead NetFlow	10.99.16.252	2
SH-Columbus:wan0_0	SH-Columbus:wan0_0	Steelhead NetFlow	10.99.14.252	2
SH-DataCenter:wan0_0	SH-DataCenter:wan0_0	Steelhead NetFlow	10.100.100.252	2
SH-LosAngeles:wan0_0	SH-LosAngeles:wan0_0	Steelhead NetFlow	10.99.12.252	2
SH-Phoenix:wan0_0	SH-Phoenix:wan0_0	Steelhead NetFlow	10.99.13.252	2
SH-SanFrancisco:wan0_0	SH-SanFrancisco:wan0_0	Steelhead NetFlow	10.99.15.252	2
SH-Seattle:wan0_0	SH-Seattle:wan0_0	Steelhead NetFlow	10.99.11.252	2

1 Show: 10 entries per page

The WAN interface groups displayed on the Definitions > WAN page are a special case of the entire set of interface groups displayed on the Definitions > Interface Groups page. You can add, delete and move WAN interfaces the same way you do other interfaces on the Definitions > Interface Groups page, with the following exceptions:

- The WAN view can contain only the Optimized and Non-optimized interface groups. You cannot create other interface groups, devices or interface subgroups within the WAN network view.
- If you move an optimized WAN interface for a SteelHead appliance of version 5.5.3 or higher out of the Optimized group, the appliance will move it back into the Optimized group the next time it receives flow information from the SteelHead and recognizes it as a WAN optimization device.
- If you drag and drop or otherwise move an interface into the Non-optimized group, the appliance will treat it as a non-optimized WAN interface.

CHAPTER 5 Enterprise Integration

This chapter describes the main features for integrating the SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliances into the core infrastructure of your network. It includes the following sections:

- [“SteelHead QoS Shaping,”](#) next
- [“Vulnerability scanning”](#) on page 119
- [“External links”](#) on page 122
- [“Host switch port discovery”](#) on page 123
- [“API access”](#) on page 123
- [“Identity sources”](#) on page 124
- [“Load balancers”](#) on page 124
- [“DHCP integration”](#) on page 125

These features are available from the Integration submenu of the Configuration menu.

SteelHead QoS Shaping

The NetProfiler and NetExpress appliances provide unified monitoring and reporting of the effectiveness of SteelHead outbound Quality of Service shaping policies deployed on SteelHead appliances across the network. This requires collecting two types of information from the SteelHead devices.

- Traffic attributes - SteelHead QoS classification ID, Application ID and DSCP marking. The SteelHead appliances must be configured to include this information in the SteelFlow Net or NetFlow v9 data that they are sending to the NetProfiler (via a Flow Gateway appliance) or NetExpress.
- Configuration information - SteelHead QoS shaping policy configuration settings. The SteelHead appliances must be configured to allow the NetProfiler or NetExpress to query their REST API to retrieve QoS configuration information.

The NetProfiler or NetExpress uses REST API queries to poll the SteelHead appliances for QoS configuration information once every 24 hours to stay synchronized with the actual SteelHead settings. Newly-added SteelHead appliances are polled as soon as the NetProfiler discovers them. You can also initiate polling manually.

The NetProfiler or NetExpress use the SteelHead QoS configuration data to interpret the class and application IDs in the flow data it receives from the SteelHead appliances via SteelFlow Net or NetFlow v9. This enables it to report the traffic shaping performance of each SteelHead. Additionally, the NetProfiler and NetExpress can aggregate all traffic data by QoS class name and report the overall performance of classes across the network.

Preparation for reporting SteelHead QoS shaping policy performance involves configuration on both the SteelHead and NetProfiler appliances. The following tasks are described in the sections that follow:

1. **“Export SteelHead statistics to NetProfiler or NetExpress”** - Set the SteelHead to send flow statistics, QoS class IDs and application IDs to the NetProfiler (via a Flow Gateway) or to the NetExpress.
2. **“Grant access to the SteelHead REST API”** - Set the SteelHead to allow the NetProfiler or NetExpress to access its REST API.
3. **“Poll the SteelHead”** - Configure the NetProfiler or NetExpress to poll the SteelHead appliance for QoS configuration information and application identification definitions.
4. **“Verify configuration information”** - Optionally, verify the SteelHead QoS shaping configuration information that the NetProfiler or NetExpress receives from the SteelHead appliance.

When the communication between the SteelHead appliances and the NetProfiler or NetExpress is configured, you can run reports on SteelHead outbound QoS shaping policy performance. The reports are described in [Chapter 13, “Reporting.”](#)

Export SteelHead statistics to NetProfiler or NetExpress

1. On the SteelHead appliance Configure > Networking > Flow Statistics page, enable flow export, and set the SteelHead to also export QoS and application statistics to SteelFlow Net collectors.

Figure 5-1. SteelHead Configure > Networking > Flow Statistics page Flow Export section

Configure > Networking > Flow Statistics ?

Flow Statistics Settings

☒ Enable Application Visibility

☒ Enable WAN Throughput Statistics

☐ Enable Top Talkers

☒ 24-hour Report Period (Higher Granularity)

☐ 48-hour Report Period (Lower Granularity)

Flow Export Settings

☒ Enable Flow Export

☒ Export QoS and Application Statistics to CascadeFlow Collectors

Active Flow Timeout: seconds

Inactive Flow Timeout: seconds

- Also on the Configure > Networking > Flow Statistics page, add the Flow Gateway or NetExpress as a SteelFlow Net collector.

Figure 5-2. SteelHead Configure > Networking > Flow Statistics page Flow Collectors section

Flow Collectors:

▼ Add a New Flow Collector — Remove Selected

Collector IP Address:	10.38.8.62	Port:	2055
Version:	CascadeFlow		
Packet Source Interface:	primary (Interface used for the source IP of the flow packets.)		
LAN Address:	<input checked="" type="checkbox"/> Show		
Capture Interface primary:	None		
Capture Interface lan0_0:	All		
Capture Interface lan0_1:	All		
Capture Interface lan1_0:	All		
Capture Interface lan1_1:	All		
Capture Interface wan0_0:	All		
Capture Interface wan0_1:	All		
Capture Interface wan1_0:	All		
Capture Interface wan1_1:	All		

Note that the port to which the SteelHead is sending SteelFlow Net must be identified as a NetFlow/IPFIX data source on the Flow Gateway or NetExpress Configuration > General Settings page. The default SteelFlow Net source port of the SteelHead matches the default destination port on the Flow Gateway or NetExpress.

Figure 5-3. Flow Gateway or NetExpress Configuration > General Settings page Data Sources section

Data Sources

<input checked="" type="checkbox"/> Use NetFlow/IPFIX	Port: 2003, 2055	<p>The NetExpress can be configured to receive traffic flow information from NetFlow (versions 1, 5, 7 and 9), IPFIX, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). Specify one or more ports in a comma-separated list for each type of flow data, up to a combined total of 50 ports. Do not assign a port to receive more than one type of flow data. That is, each port can be listed only once. The combined capacity of these data sources is 90,000 flows/minute. The common default ports for NetFlow are 2055, 9555, 9995 and 9996.</p>
<input checked="" type="checkbox"/> Use sFlow Port:	6343	
<input checked="" type="checkbox"/> Use Packeteer	Port: 9800	
Allowed on interface:	<input checked="" type="checkbox"/> Management <input type="checkbox"/> AUX	
Excluded Sources:	<input type="text"/> ?	

When the Flow Gateway or NetExpress receives SteelFlow Net data from the SteelHead, it registers the SteelHead as a data source that it can subsequently poll for configuration information.

Grant access to the SteelHead REST API

- On the SteelHead Configure > Security > REST API Access page, enable REST API access to the SteelHead.

Figure 5-4. SteelHead Configure > Security > REST API page Access Settings section

Configure > Security > REST API Access ? [send feedback](#)

REST API Access Settings

☒ Enable REST API Access

[Apply](#)

This allows a NetProfiler or NetExpress with the correct access code to poll a SteelHead for QoS configuration.

The NetProfiler or NetExpress cannot poll a SteelHead for QoS configuration information unless both appliances are using the same access code. However, you can set up:

- A different access code for each individual SteelHead.

- Different access codes for different organizations. For example, SteelHead appliances belonging to one organization use one access code, and those belonging to a different organization use a different access code.
 - A default access code that NetProfiler or NetExpress uses for all SteelHead appliances except those to which you have assigned a custom access code.
2. Also on the SteelHead Configure > Security > REST API Access page, generate an access code to give to the NetProfiler or NetExpress.

Figure 5-5. SteelHead Configure > Security > REST API page Access Codes section

Access Codes:

▼ Add Access Code — Remove Selected

Description of Use:

☒ Generate New Access Code

☐ Import Existing Access Code

Add

3. Paste the SteelHead access code into the NetProfiler or NetExpress on the System > Devices/Interfaces page Synchronization tab as follows.

Figure 5-6. NetProfiler System > Devices/Interfaces page Synchronization tab

Devices/Interfaces ?

Devices & Interfaces (Tree) Interfaces (List) Devices (List) Synchronization (List) Preferred Interfaces (List)

Synchronization initializing
 Synchronization succeeded
 Synchronization failed
 Synchronization not available
 Device access disabled

Device type: ☒ SteelHeads ☐ NetSharks ☐ CBQoS Devices

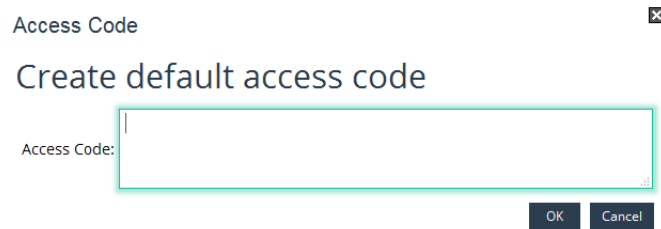
Devices

Selected Actions ... Global Actions ...

<input type="checkbox"/>	Device Address	Device Hostname	Access Code	Polling	App Poll Status	QoS Poll Status
<input type="checkbox"/>	10.100.100.252	SH-DataCenter	Not Configured	Enabled		
<input type="checkbox"/>	10.99.16.252	SH-Austin	Not Configured	Enabled		
<input type="checkbox"/>	10.99.15.252	SH-SanFrancisco	Not Configured	Enabled		
<input type="checkbox"/>	10.99.14.252	SH-Columbus	Not Configured	Enabled		
<input type="checkbox"/>	10.99.13.252	SH-Phoenix	Not Configured	Enabled		
<input type="checkbox"/>	10.99.12.252	SH-LosAngeles	Not Configured	Enabled		
<input type="checkbox"/>	10.99.11.252	SH-Seattle	Not Configured	Enabled		

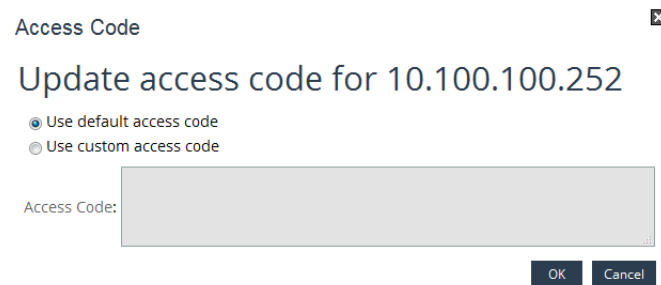
1 go to page Show: 10 entries per page

- Default access code - To specify a default access code for the NetProfiler or NetExpress to use to connect to SteelHead appliances, pull down the Global Actions menu, choose Create Default Access Code, and paste the SteelHead access code into the edit box.

Figure 5-7. NetProfiler System > Devices/Interfaces page Synchronization tab - Create Default Access Code


After you have specified a default access code, all SteelHead appliances that begin sending SteelFlow Net to the NetProfiler or NetExpress are polled using that default access code until you set up custom access codes for them.

- Custom access code - To specify a custom access code for the NetProfiler or NetExpress to use to connect to one or more SteelHead appliances, select the appliances from the list. (A SteelHead is not listed until the NetProfiler or NetExpress receives SteelFlow Net data from it.) Then pull down the Selected Actions menu, choose Update Access Code, select “Use custom access code” and paste the access code into the edit box. The NetProfiler or NetExpress then uses this access code to authenticate itself to the selected SteelHead appliances.

Figure 5-8. NetProfiler System > Devices/Interfaces page Synchronization tab - Custom Access Code


You can also use the Selected Actions menu > Update Access Code window to switch between using the default access code or using a custom access code.

Poll the SteelHead

The NetProfiler or NetExpress automatically polls SteelHead appliances for configuration information:

- The first time it receives SteelFlow Net data from a SteelHead.
- Every 24 hours after it first receives SteelFlow Net data from a SteelHead.

You can also manually poll SteelHead appliances. Polling is controlled by the NetProfiler System > Devices/Interfaces page Synchronization tab.

Figure 5-9. NetProfiler System > Devices/Interfaces page Synchronization tab

Devices/Interfaces ?

Devices & Interfaces (Tree) Interfaces (List) **Devices (List)** Synchronization (List) Preferred Interfaces (List)

Synchronization initializing
 Synchronization succeeded
 Synchronization failed
 Synchronization not available
 Device access disabled

Device type: ☒ SteelHeads ☐ NetSharks ☐ CBQoS Devices

Devices Selected Actions ... ▼ Global Actions ... ▼

<input type="checkbox"/>	Device Address	Device Hostname	Access Code	Polling	App Poll Status	QoS Poll Status
<input type="checkbox"/>	10.100.100.252	SH-DataCenter	Not Configured	Enabled		
<input type="checkbox"/>	10.99.16.252	SH-Austin	Not Configured	Enabled		
<input type="checkbox"/>	10.99.15.252	SH-SanFrancisco	Not Configured	Enabled		
<input type="checkbox"/>	10.99.14.252	SH-Columbus	Not Configured	Enabled		
<input type="checkbox"/>	10.99.13.252	SH-Phoenix	Not Configured	Enabled		
<input type="checkbox"/>	10.99.12.252	SH-LosAngeles	Not Configured	Enabled		
<input type="checkbox"/>	10.99.11.252	SH-Seattle	Not Configured	Enabled		

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 249

Figure 5-10. NetProfiler Configuration > Integration > SteelHead QoS Shaping page

SteelHead QoS Shaping

SteelHead QoS Settings Synchronize all				
SteelHead Name	QoS Shaping and Enforcement	Configuration Mode	Last Success Sync Time	Status
SH-Austin	Enabled	Basic Mode	Aug 2, 2014 8:38 AM	success
SH-DataCenter	Enabled	Advanced Mode with Hierarchical Classes	Aug 2, 2014 8:52 AM	success
<ul style="list-style-type: none"> SteelHead IP : 10.100.100.252 Local WAN Oversubscription : Disabled QoS Marking : Enabled Export QoS and Application Statistics to CascadeFlow Collectors : Enabled 				
SH-Seattle	Enabled	Basic Mode	Aug 2, 2014 8:38 AM	success
SH-LosAngeles	Disabled	Basic Mode	Aug 2, 2014 8:38 AM	success
SH-Phoenix	Enabled	Basic Mode	Aug 2, 2014 8:38 AM	success
SH-Columbus	Enabled	Basic Mode	Aug 2, 2014 8:38 AM	success
SH-SanFrancisco	Enabled	Basic Mode	Aug 2, 2014 8:38 AM	success
Entries per page 10 Page 1 of 1 Displaying SteelHeads 1 - 7 of 7				

The Synchronize All button causes the NetProfiler or NetExpress to poll all the SteelHead appliances listed on the page for QoS configuration information so that the NetProfiler or NetExpress has the latest information. Polling all the SteelHead appliances to synchronize the information this way can require up to 30 minutes, depending on your network.

If a polling status message in the Status column indicates something other than success, confirm that the NetProfiler or NetExpress has access to the SteelHead and the SteelHead is configured correctly. If you cannot identify the error, record the status message and contact Riverbed Support.

Vulnerability scanning

The appliance provides the client side of vulnerability scanning. You must install vulnerability scanning software on a server that is accessible to the appliance in order to manage scanning from the appliance GUI.

The appliance provides both manual and automatic vulnerability scans of hosts on the network. You can initiate a scan manually by right-clicking a host IP address on any report in the appliance and choosing **Vulnerability Scan** on the shortcut menu. Alternatively, you can click **Run Scan** on the Configuration > Integration > Vulnerability Scan page. You can also set the appliance to automatically initiate a scan in response to any specified traffic event of any specified severity.

Two types of vulnerability scans can be defined: Quick scans and Deep scans. The Quick scan is intended to use a shorter list of plugins and perhaps simpler options than the Deep scan. However, their configuration and operation is otherwise the same. Both can be run while you wait or run in the background. Also, they can be run from different scan servers.

Vulnerability scan reports are saved in the Completed Reports table of the Reports > Saved Reports page. They can be viewed, printed, and emailed. They can also be saved indefinitely, like other reports. Vulnerability scan reports are subject to the same disk space management rules as other reports.

The running of vulnerability scans is recorded in the audit log, which Administrators can view on the System > Audit Trail page.

Types of vulnerability scans

Vulnerability scan configurations are specified using the Configuration > Integration > Vulnerability Scanning page. The Vulnerability Scan page has three tabs:

- **Quick Scan** - specifies the connection information, authentication method, and settings for the scanner used for a Quick Scan.
- **Deep Scan** - same fields and buttons as the Quick Scan tab, except that it specifies the configuration required for a Deep Scan.
- **Auto Scan** - specifies the event types and alert levels that are to trigger automatic vulnerability scans.

The setup tabs for the Quick scan and the Deep scan are the same. However, they are independent of one another. You can, for example, have Quick scans performed by a scanner running on one scanner server and Deep scans performed by another scanner.

The appliance supports Nessus, Rapid7, Qualys, nCircle and Foundstone/McAfee scanners. The appliance offers more configuration options for Nessus than for the others because the other scanning systems are configured primarily through their own user interfaces.

Figure 5-11. Configuration > Integration > Vulnerability Scan Setup page Quick Scan tab

Vulnerability Scan Setup ?

Quick Scan | Deep Scan | Auto Scan

Quick Scan Configuration Setup

Step 1: Enter connection information for the scanner server and click Apply.

Scanner:

Host name:

Port:

Step 2: Enter additional configuration information to complete the setup.

Step 3: Run a scan now (optional).

Configuring automatic scans

After specifying the Quick Scan and Deep Scan parameters, you can set the appliance to automatically run scans in response to specified types of alerts.

The Vulnerability Scan Setup page lists the type of network events that cause the appliance to send traffic-related alerts. For each level of alert these events can trigger, you can specify a scan action to be taken: No Scan, Quick Scan, or Deep Scan.

Fields near the bottom of the page provide for limiting the volume and rate of scanning to protect your network from being overwhelmed by scan traffic. The appliance reports up to 256 hosts involved in an event. It runs up to 4 scans concurrently and up to 12 scans per hour.

The scan traffic is recorded in the appliance flow logs and becomes part of the traffic profile.

Figure 5-12. Configuration > Integration > Vulnerability Scan Setup page Auto Scan tab

Vulnerability Scan Setup ?

Quick Scan Deep Scan **Auto Scan**

Clear Selection Set Scan ▼

To select a cell in the table, click it.
To select an entire row or column, click the label for that row or column.

	Low	Medium	High
DoS/Bandwidth Surge	No Scan	No Scan	No Scan
Host Scan	No Scan	No Scan	No Scan
New Host	No Scan	No Scan	No Scan
New Server Port	No Scan	No Scan	No Scan
Port Scan	No Scan	No Scan	No Scan
Suspicious Connection	No Scan	No Scan	No Scan
User-defined Policy	No Scan	No Scan	No Scan
Worm	No Scan	No Scan	No Scan

Maximum number of hosts to scan per event:

Maximum number of concurrent scan requests:

Maximum number of scan requests per hour:

Apply

What is scanned

The event that triggers an automatic scan also determines which hosts are scanned, as follows:

Type of event that triggered scan	What is scanned
Denial of Service/Bandwidth Surge	Attacker hosts
Host Scan	Scanner host
New Host	New host
New Server Port	Host that provided or consumed a service over the port
Port Scan	Victim hosts
Suspicious Connection	Source and victim
User-defined Policy	Source and destination or client and server hosts involved in the event.
Worm	Victim hosts

Only hosts identified as having “inside addresses” are scanned. Inside addresses are specified on the Configuration > General Settings page.

Manually initiating a vulnerability scan

Operators and Administrators can manually initiate a vulnerability scan by either of two methods:

- Click Run Scan on the Quick Scan tab or Deep Scan tab of the Configuration > Integration > Vulnerability Scanning page.
- Right-click the host on a report and choose Vulnerability scan on the shortcut menu.

You can add more hosts if you want to scan hosts in addition to the one you right-clicked, for a total of up to 256.

Note: Manual scans are not subject to the rate limit on the Auto Scan tab. However, they are counted towards the limit when the next automatic scan runs.

When a scan run in the background is complete, a scan report is automatically saved in the Completed Reports table of the Reports > Saved Reports page. Reports from foreground scans appear automatically and can be saved, printed, and emailed. The content and format of a report are determined by the type of scanner you are using. Refer to your scanner documentation for descriptions of the information contained in the reports. The appearance of a report may vary from the appearance of the report available from the scanner GUI, depending on the scanner used.

External links

The appliance provides a means for contacting other network devices for additional information about a host, data source device, MAC address, interface, port, user or BGP Autonomous System. Right-clicking the entity and choosing an external link from the shortcut menu sends a query to the other network device. A new browser window opens to display the response from that device.

Likewise, right-clicking a username and choosing an external link from the shortcut menu sends a query on the username to the other network device and opens a new browser window to display the response.

External links must be specified on the Configuration > Integration > External Links page in order to be available on the right-click menu. They must be specified using the syntax that the external device expects. Refer to the online help system for syntax examples.

Figure 5-13. Configuration > Integration > External Links Setup page

External Links

External Links

Link Type	Label	URL	Actions
Host		<input type="text" value="http://ExternalServer?hostname={HOSTNAME}?hostip={HOSTIP}?hostmac={MAC}"/>	Add
ASN	Hurricane Electric	http://bgp.he.net/AS/{ASN}	Edit Delete
Host	ARIN WHOIS Search	http://whois.arin.net/ui?queryinput={HOSTIP}	Edit Delete
Host	Geotool	http://www.geoiptool.com/en/?IP={HOSTIP}	Edit Delete
Host	Malware Domain List	http://www.malwaredomainlist.com/mdl.php?search={HOSTIP}&colsearch=IP&quantity=50	Edit Delete
Host	McAfee TrustedSource	http://www.trustedsource.org/query/{HOSTNAME}	Edit Delete
Host	On-demand SNMP poll (Solar Winds)	http://oriondemo.solarwinds.com/Orion/NetPerfMon/Resources/NodeSearchResults.aspx?Property=IP_Address&SearchText={HOSTIP}	Edit Delete
Host	SANs IP Lookup	http://isc.sans.org/ipinfo.html?ip={HOSTIP}	Edit Delete
Host	Traceroute to this Host	http://www.net.princeton.edu/cgi-bin/traceroute.pl?target={HOSTIP}	Edit Delete
Host	TrustedSource Research Portal	http://www.trustedsource.org/query.php?q={HOSTIP}	Edit Delete
Host	View http	http://{HOSTIP}	Edit Delete
Host	View https	https://{HOSTIP}	Edit Delete
MAC	Coffer MAC Address Lookup	http://www.coffer.com/mac_find?string={MAC}	Edit Delete

Host switch port discovery

As part of the Host Information Report, the appliance identifies the switch port to which a host is connected. This requires the appliance to know about the switches that the host's traffic passes through. The appliance attempts to find the outermost switch on which a host was seen. If it knows about all the switches, then this will be the access switch and the appliance will report the port to which the host is connected.

The Configuration > Integration > Switch Port Discovery page allows you to identify your switches to the appliance so that the host switch port information will be included in the Host Information Report.

Figure 5-14. Configuration > Integration > Switch Port Discovery page

Switch Port Discovery [?]

Polling Settings

Total time to poll switches (min):

Number of simultaneous scans allowed:

Apply

Devices Actions ... ▾

<input type="checkbox"/>	Name	IP Address ↓	Type	Last Connection State	Last Good Connection	Last Connection Attempt	Actions
<input type="checkbox"/>	dc_Switch1	10.100.100.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 1:29:01 PM	Poll now Edit
<input type="checkbox"/>	Hartford_Switch1	10.99.18.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 12:09:01 PM	Poll now Edit
<input type="checkbox"/>	Philadelphia_Switch1	10.99.17.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 1:49:00 PM	Poll now Edit
<input type="checkbox"/>	Austin_Switch1	10.99.16.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 12:29:01 PM	Poll now Edit
<input type="checkbox"/>	SanFrancisco_Switch1	10.99.15.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 11:29:01 AM	Poll now Edit
<input type="checkbox"/>	Columbus_Switch1	10.99.14.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 12:49:01 PM	Poll now Edit
<input type="checkbox"/>	Phoenix_Switch1	10.99.13.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 11:49:01 AM	Poll now Edit
<input type="checkbox"/>	LosAngeles_Switch1	10.99.12.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 1:09:01 PM	Poll now Edit
<input type="checkbox"/>	Seattle_Switch1	10.99.11.251	Switch	Scan failed due to improper configuration		Jun 11, 2016 11:09:01 AM	Poll now Edit

1

go to page

Show: entries per page

API access

The information that the appliance collects about network assets, traffic flows, and events is made available for use by other products through APIs (application program interfaces). Management systems can send requests for information to the appliance. The appliance will respond by sending the HTML or CSV data for traffic reports or event reports, or XML data for asset reports.

Access to the APIs are protected by authentication. The RESTful API can authenticate users by Basic, Session (Cookie) or OAuth 2.0 authentication. The Reporting, Assets and Event Report APIs use ACLs (access control lists). The Configuration > Integration > API Access page enables you to generate OAuth 2.0 access codes for the RESTful API and add users to the access control list for the other APIs. Changing or deleting an ACL specification does not affect users that are currently logged in until they log out.

The API Authorization page is available to Administrators and Operators.

Figure 5-15. Configuration > Integration > API Access page

APIs Access

APIs

Module Name	Authentication	Example URL	For more information...
RESTful API	Basic, Session (Cookie), OAuth 2.0	https://cam-doc.lab.nbttech.com/api/common/1.0/info	Click here.
Network Traffic API	ACL	https://cam-doc.lab.nbttech.com/profiler/api/report.php?username=admin&report_type=2	Click here.
Asset API	ACL	https://cam-doc.lab.nbttech.com/profiler/api/asset.php?username=admin&score_by=0&min=1&max=3&limit=100	Click here.
Event Viewer	ACL	https://cam-doc.lab.nbttech.com/event_viewer.php?username=admin&id=1	Click here.

ACLs

☐ Enable ACL login system

IP Ranges for APIs using ACL	User	Actions
<input type="text"/>	admin ▾	Add

Identity sources

The appliance can collect user identity information for reports on network users. Identity information sources are listed on the Configuration > Integration > Identity Sources page.

The appliance receives the identity information from Microsoft Active Directory domain controllers. These are configured separately from the NetProfiler setup and administration activities.

Once configured with the Riverbed connection utility, the Active Directory devices send user identity information to the appliance. If a source produces too much data or data that is not interesting, you can configure the appliance to ignore identity data that it receives from that source.

If a source is no longer being used, you should disable the collector utility at the source so that it stops sending data. Then delete the entry for that source from the list on the Configuration > Integration > Identity Sources page.

User identity information is available to user accounts that an Administrator has enabled to view it. You can use the Configuration > Account Management > User Accounts page to enable or disable user identity viewing, as appropriate.

Figure 5-16. Configuration > Integration > Identity Sources page

Identity Sources

Identity Sources

Connector Source	SSL Hash	Status	Connected	Last Heard From	Actions
No Data Available.					

Load balancers

Use the Configuration > Integration > Load Balancer page for identifying load balancers as service components. When a load balancer has been defined as a service component, you can add it from a list when you define a service on the Services > Manage Services page.

Figure 5-17. Configuration > Integration > Load Balancer page

Load Balancers ⓘ

Use this page to manage the list of load balancers.

Load Balancers						Options ▾
Name	Type	Management IP/Port	Username	Status	Last Update	Actions
DataCenterF5	F5	10.100.120.5	user	success	Jun 11, 2016 11:09 AM	Edit Delete Refresh

The page lists load balancers by name, type, address, user name and status. The Status column indicates if the NetProfiler or NetExpress appliance was able to query the load balancer for information successfully. The Last Update column lists the last time the load balancer information was updated. The appliance queries the load balancer for its Virtual IP Addresses and SNAT configuration. Currently the product obtains this information from Riverbed SteelApp Traffic Manager and F5 Version 9 and Version 10 Local Traffic Manager load balancers. Information for other devices must be entered manually when you define a service.

The Load Balancer page enables you to manage your list with the following features on the Options menu:

- **Add** - Enter the information that NetProfiler needs to query the load balancer. This includes the name, type, address, user name and password of the device. For creating a new load balancer component of type “Other,” you can leave the Management IP and Ports box blank.
- **Export** - Exports all information in the list of load balancers to a JSON file that you can save on your local machine.
- **Import** - Imports a JSON file containing load balancer definitions. Does not import XML or CSV files, such as load balancer definition files exported from earlier versions of NetProfiler.

Additionally, for each load balancer in the list, you can edit or delete the definition.

Refer to the online help system for additional details.

DHCP integration

If parts of your network are managed by DHCP address allocation, then host machines may be assigned new IP addresses when their leases expire. In order to develop and display the profile of a host's activity, the appliance must continue to track the connection behavior of the host when its IP address lease expires and the DHCP server assigns it a new IP address.

The appliance uses lease information from the DHCP server as the basis for tracking hosts. This requires a mechanism for transferring lease information from the DHCP server to the appliance. The specifics of the mechanism depend on the DHCP implementation.

Lease data file format

The appliance accepts DHCP data in two formats.

Alcatel-Lucent QIP-compatible format

This format contains one lease record per line in the following order:

```
IP Address | MAC address | DNS name | domain | lease-start date time | lease-end date time | status
```


For example (on one line):

```
192.168.10.1|aa:bb:cc:dd:0a:01|host-10-1|example.com
|2009-05-01 15:26:15Z|2009-05-08 15:26:15Z|Active
```

Note that time stamps are expected to be in UTC format. To specify time stamps in local time, use the “20090501 15:26” format instead:

For example:

```
192.168.10.1|aa:bb:cc:dd:0a:01|host-10-1|example.com
|20090501 15:26|20070508 15:26|Active
```

ISC-compatible format

This format is compatible with POSIX-compliant DHCP packages distributed by Internet Systems Consortium, Inc. (www.isc.org).

```
lease 10.128.2.219 {
    starts 2 2008/08/15 16:09:09;
    ends 2 2008/08/15 20:09:09;
    tstp 2 2008/08/15 20:09:09;
    binding state free;
    hardware ethernet 00:02:a5:ba:53:9b;
    uid "\001\000\002\245\272S\233";
}
lease 192.168.255.100 {
    starts 1 2009/02/19 01:28:33;
    ends 1 2009/02/19 13:28:33;
    tstp 1 2009/02/19 13:28:33;
    binding state free;
    hardware ethernet 00:04:23:c4:02:30;
}
```

Transfer mechanism

When transferring DHCP lease data to the appliance from a DHCP package that uses one of the data formats the appliance supports, you can transfer the data in its native format to the appliance.

When integrating with a Windows DHCP domain controller, you need to convert the data format. Riverbed provides a conversion script and instructions for its use. You can download these from the appliance help system.

Typically, the transfer of lease information to the appliance is implemented as follows:

1. Enable the DHCP server to log in to the appliance via SSH. SSH on the appliance must be configured with the public key of the DHCP server. On the appliance, SSH configuration files are in `/usr/mazu/var/dhcp/.ssh`. The appliance supports SSH v2.
2. Set up a script on the DHCP server so that every *n* minutes, a client process obtains lease information from the DHCP server and writes it into a file. In the case of a Windows DHCP implementation, use the Riverbed script to convert the data format before transferring the file to the appliance.
3. Set up a scheduler to execute the scripts to dump, convert (if Windows), and transfer the DHCP lease data information to the appliance. The lease data file must be transferred to the appliance as a file named `data`. Typically, it is transferred into the DHCP data directory on the appliance.
4. After the scheduler has transferred the lease data, it must transfer a file named `data-new` into the same directory as the `data` file. This file indicates to the appliance that the new lease data is available.

The data and data-new files can be transferred using commands such as:

```
scp <dump_file> dhcp@<appliance_name>:/usr/mazu/var/dhcp/data
scp data-new dhcp@<appliance_name>:/usr/mazu/var/dhcp/data-new
```

or

```
scp <dump_file> dhcp@<appliance_name>:./data
scp data-new dhcp@<appliance_name>:./data-new
```

Both the data and data-new files are removed after the appliance has imported the new lease data. They must be written again by each subsequent data transfer.

If the appliance receives an IP address in flow data that does not appear in the lease data file, it assumes the address to be static.

Riverbed provides instructions for integrating the appliance with QIP, ISC, and Windows DHCP software.

Update intervals

The interval for updating the appliance DHCP information can be based on DHCP lease times, lease update intervals and the times when new leases are most frequently requested on your network. A DHCP client on a network with no outages may update its lease when half the lease time has expired. That is, it obtains a new lease at an interval of lease-length/2.

Update scheduling can vary widely, depending on network conditions and security policies. Some general guidelines for sending new DHCP data to the appliance are as follows.

- If your script for sending DHCP information to the appliance sends incremental updates (i.e., just what has changed since the last update), have it send the appliance updates every hour.
- If your script sends complete DHCP lease information for every update, have it send the appliance updates based on the length of the leases, as follows:

Lease length	Update interval
More than 4 days	1 update per day (around 10:00 AM)
4 days	2 updates per day
24 hours	6 updates per day
12 hours	12 updates per day
6 hours	24 updates per day
Less than 6 hours	24 updates per day

CHAPTER 6 System Verification

This chapter describes how to ensure that the SteelCentral™ NetProfiler and SteelCentral™ NetExpress are properly configured before you begin routine operational use. It includes the following sections:

- [“System information,”](#) next
- [“Data sources”](#) on page 136
- [“Audit trail”](#) on page 146
- [“Shutdown/Reboot”](#) on page 161
- [“Update”](#) on page 161
- [“Backup”](#) on page 162

System information

The System > Information page lists the status, name, IP address and serial number of the NetProfiler or NetExpress. For an Enterprise NetProfiler, the page lists this information for each module.

The page also lists:

- Flow statistics
- Available flow logs and their start and end times
- Available identity information logs and their start and end times
- Capture job status and interfaces (NetExpress only; not included in CAX360 model.)
- Usage of licensed policy capacity
- Storage status (See more below.)
- DNS server status
- NTP server status
- Active user sessions by name, address, login time, and last access time
- Active OAuth tokens - These can be php, perl, .NET, or other script clients connecting to NetProfiler to get data using the REST API.
- SteelCentral Collect diagnostic tool

- System messages

Refer to the online help system for descriptions of each of these.

Flow statistics

Flow statistics are reported in the following sections of the System > Information page:

- Flow Capacity Stats
- Flow Capacity History
- Flow Capacity Usage
- Raw Flows Processed/Over Limit
- Reduction of Raw Flows from Deduplication

Flow Capacity Statistics

The Flow Capacity Statistics section summarizes the flow statistics based on the latest data. “Raw flows” are flows reported by switches and routers that are sending flow data to the NetProfiler or NetExpress appliance. The appliance saves the IP address of the reporting device and information the device reports about the flow for use in topology reports and deduplicates the flow records so that flows are not counted more than once.

The “Current deduplicated flow rate” is the number of flows that were reported during the most recent minute. Each flow is counted only once, regardless of how many different network devices reported it. These are also reported as a percent of licensed capacity and as a percent of total raw flows.

Figure 6-1. Flow Capacity Statistics

NetProfiler Flow Capacity Stats

Metric (Flows / Minute)	Value
Licensed limit after deduplication	600,000
Current deduplicated flow rate	8,939 (1% of capacity) (31% of raw flows)
Current raw flow rate	29,092

Flow Capacity History

The Flow Capacity History section reports the average, peak and minimum flow rates for raw and deduplicated flow data for the last day and the last week. It also reports over limit statistics. Flow data that exceeds the licensed limit for the minute during which it is received is not processed.

Figure 6-2. Flow Capacity History

Flow Capacity History

Metric (Flows / Minute)	Average	Peak	Min
Deduplicated flow rate for the last day	7,848 (1% of capacity)	13,632 (2% of capacity)	6,859 (1% of capacity)
Deduplicated flow rate over limit for the last day	0	0	0
Raw flow rate for the last day	24,370	45,919	20,646
Raw flow rate over limit for the last day	0	0	0
Deduplicated flow rate for the last week	7,964 (1% of capacity)	24,705 (4% of capacity)	6,859 (1% of capacity)
Deduplicated flow rate over limit for the last week	0	0	0
Raw flow rate for the last week	24,877	107,938	20,646
Raw flow rate over limit for the last week	0	0	0

Flow Capacity Usage

The Flow Capacity Usage section shows how much of the licensed flow capacity is being used. When the number of deduplicated flows approaches the license limit, the licensed limit is shown as a dashed line on the graph.

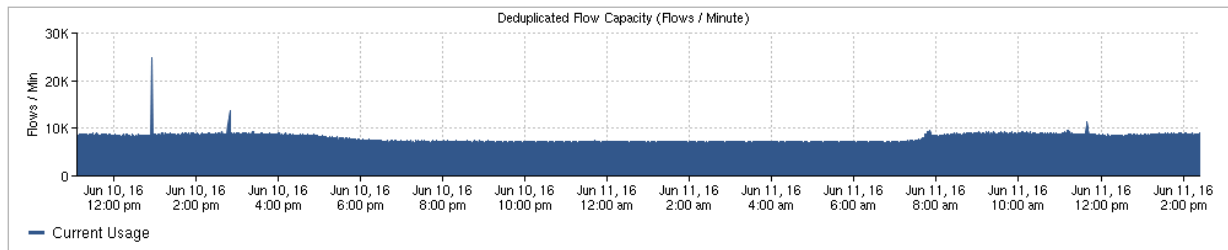
If the number of deduplicated flows in a 1-minute period exceeds the license limit, flows that are over the limit are not processed. The graph shows the number of deduplicated flows that exceeded the licensed limit.

NetProfiler

NetProfiler displays flow capacity usage on one graph.

Figure 6-3. NetProfiler Flow Capacity Usage

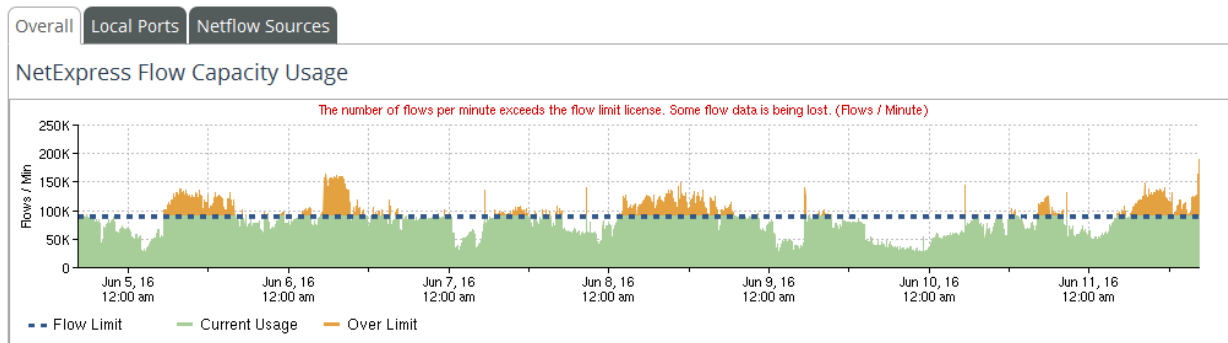
NetProfiler Flow Capacity Usage



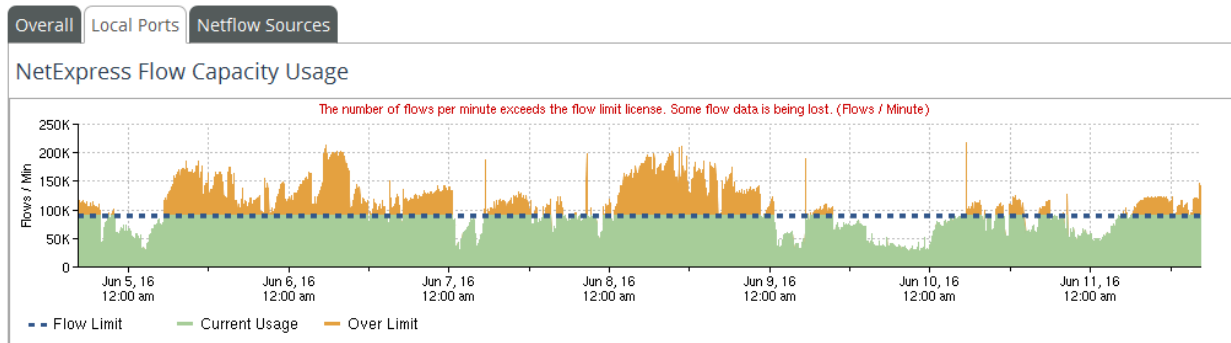
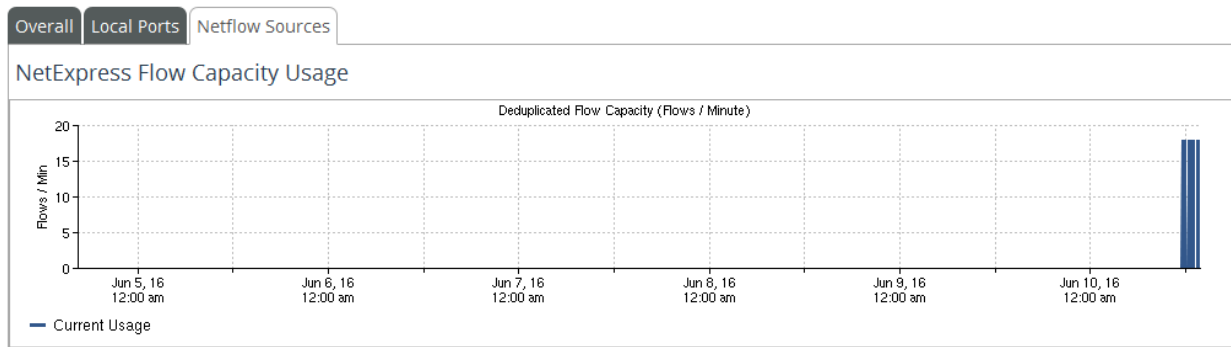
NetExpress

On NetExpress, the display has three tabs: Overall, Local Ports and NetFlow Sources

Figure 6-4. NetExpress Flow Capacity Usage - Overall



- **NetFlow Sources** - based on flow data that is sent to NetExpress from flow collecting devices.
- **Local Ports** - based on flow data compiled by NetExpress about traffic seen on its network monitoring ports.
- **Overall** - the total of flows received from NetFlow sources, local ports and other sources (such as a Flow Gateway).

Figure 6-5. NetExpress Flow Capacity Usage - Local Ports**Figure 6-6. NetExpress Flow Capacity Usage - NetFlow Sources**

The Overall flow volume could be less than the sum of the NetFlow Sources and Local Ports volumes if the combined total of NetFlow Sources and Local Ports volumes exceeds the license limit. If this were to happen, NetExpress would process flow data for traffic seen by the local ports (the monitoring ports) first and then process data from NetFlow sources up to the license limit.

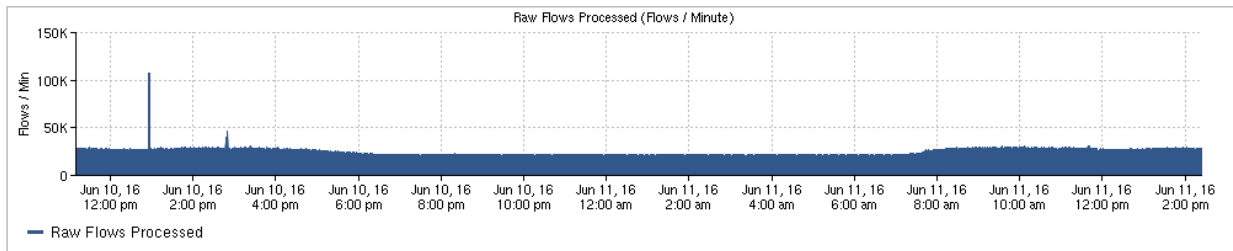
The Overall volume could be greater than the sum of the NetFlow Sources and Local Ports volumes if NetExpress is also receiving traffic information from a Flow Gateway.

Raw Flows Processed/Over Limit

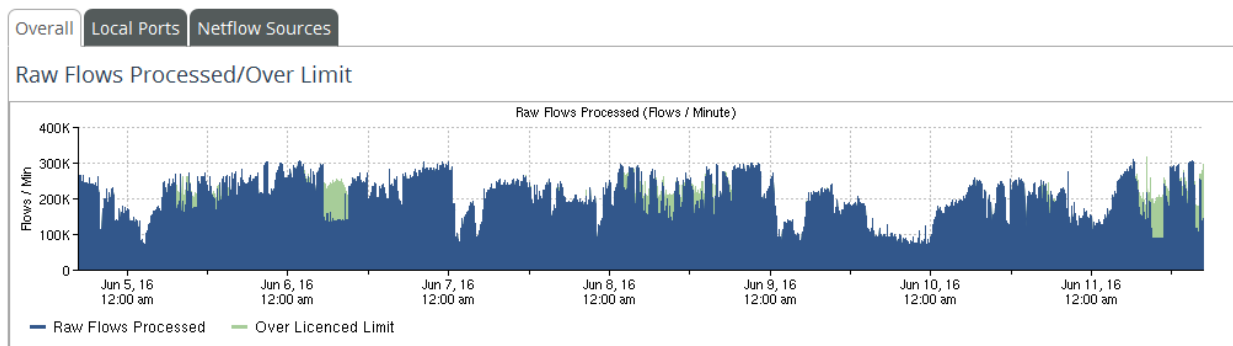
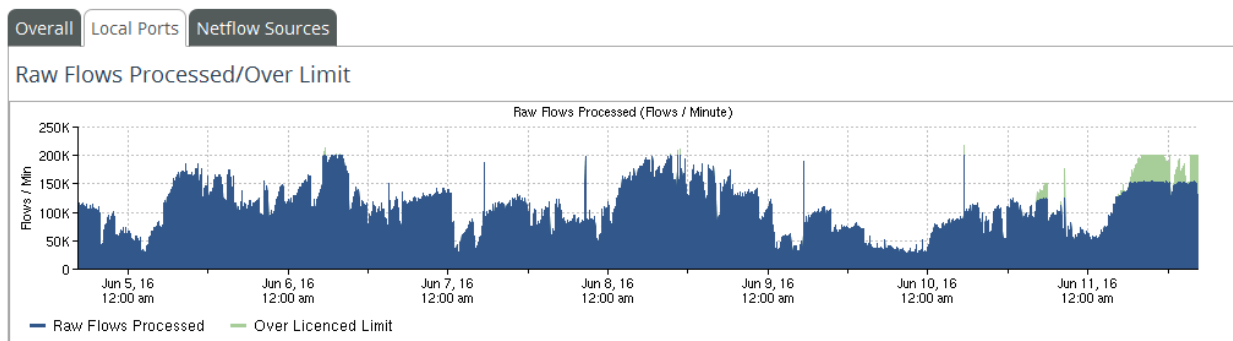
The Raw Flows Processed/Over Limit section displays the number of flows per minute that have been processed. Processing includes collecting and storing topology information and deduplicating flow data. For example, assume that a router sends a flow record to NetExpress or Flow Gateway. The appliance checks to see if the flow was already reported by another device. If it was, then the appliance adds the topology information from this flow record to the record it already has for the flow.

If the flow was not reported before, the appliance checks to see if adding it would exceed the license limit for deduplicated flow records. If recording the flow would exceed the license limit, the appliance drops the flow record.

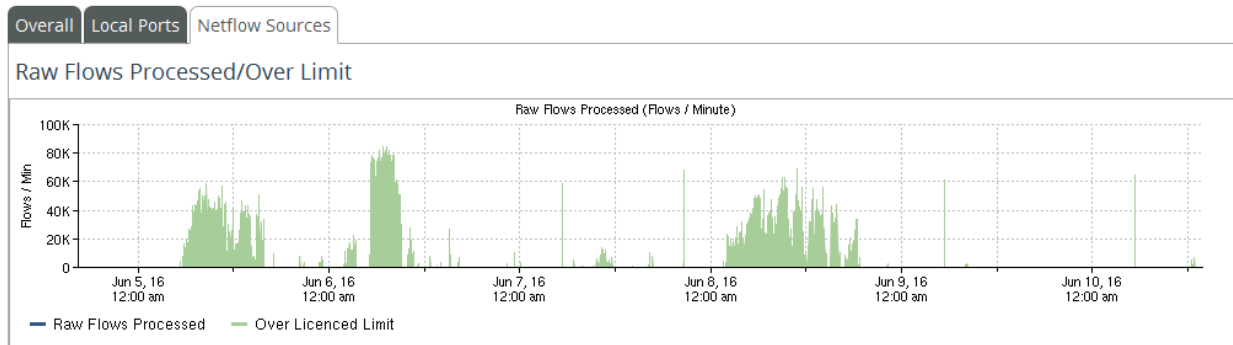
NetProfiler displays these statistics on one graph.

Figure 6-7. NetProfiler Raw Flows Processed/Over Limit**Raw Flows Processed/Over Limit**

NetExpress breaks out the statistics into Overall, Local Ports and NetFlow Sources, as in Flow Capacity Usage section.

Figure 6-8. Raw Flows Processed/Over Limit - Overall**Figure 6-9. Raw Flows Processed/Over Limit - Local Ports**

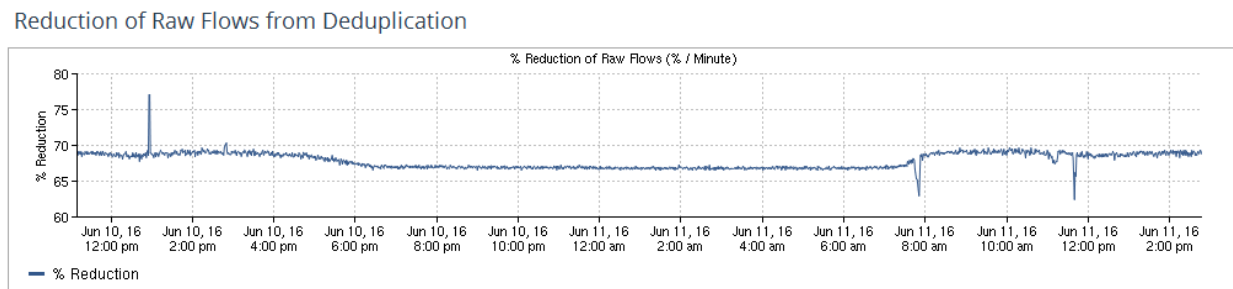
In addition to indicating flow records that were not processed because of the license limit, the NetFlow Sources tab also indicates flows for which not all the topology information could be processed because the flows were reported by too many devices.

Figure 6-10. Raw Flows Processed/Over Limit - NetFlow Sources

Reduction of Raw Flows from Deduplication

The Reduction of Raw Flows from Deduplication section displays the percentage by which the number of raw flows was reduced by deduplication.

NetProfiler displays the reduction on one graph.

Figure 6-11. Reduction of Raw Flows from Deduplication

NetExpress breaks it out into Overall, Local Ports and NetFlow Sources, as in Flow Capacity Usage section.

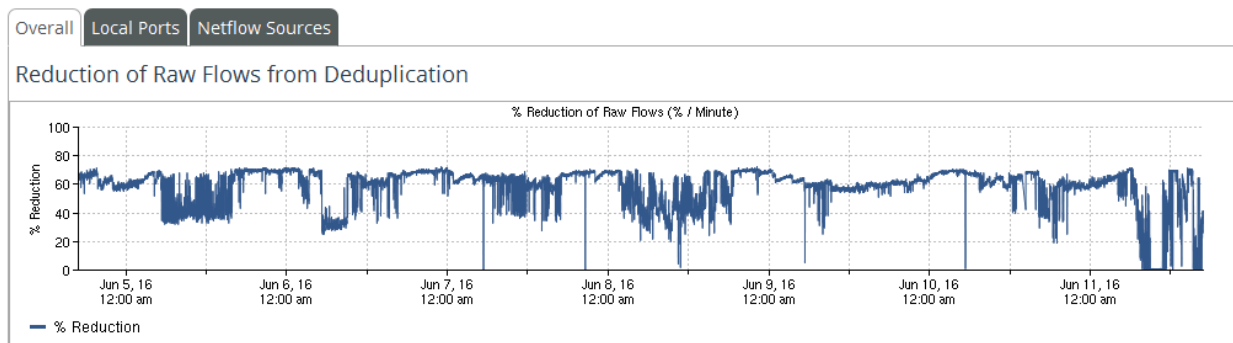
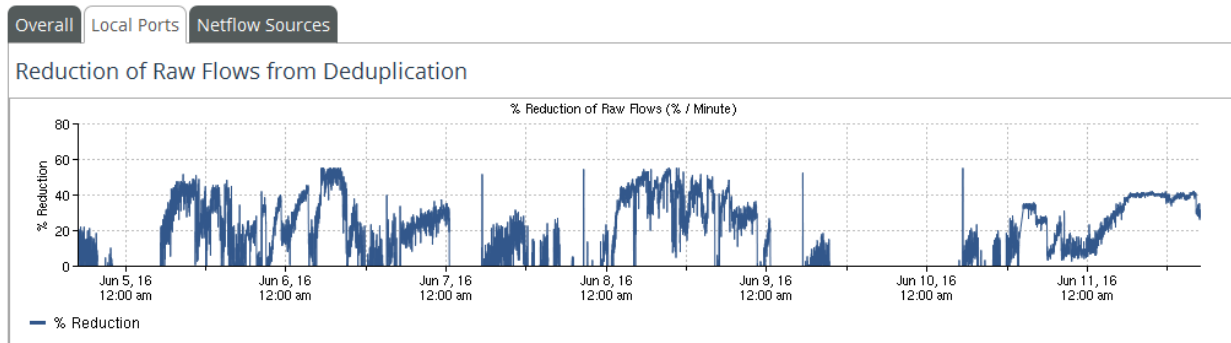
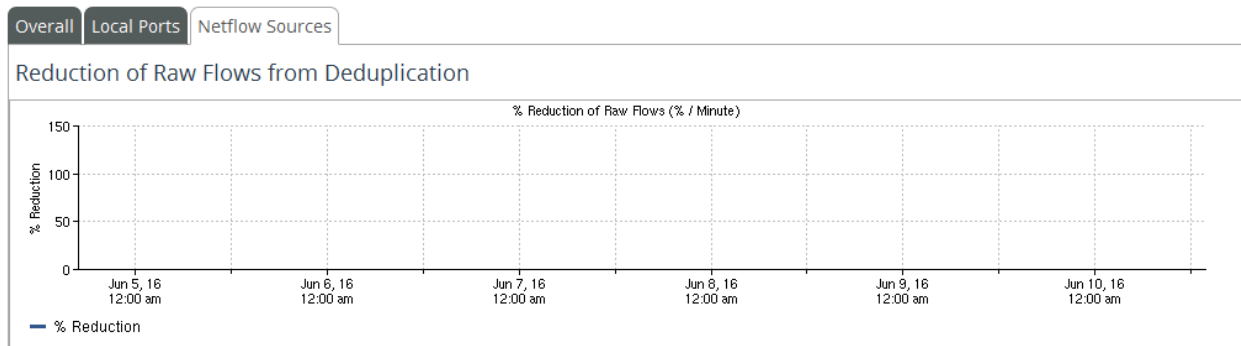
Figure 6-12. Reduction of Raw Flows from Deduplication - Overall

Figure 6-13. Reduction of Raw Flows from Deduplication - Local Ports**Figure 6-14. Reduction of Raw Flows from Deduplication - NetFlow Sources**

Storage status

The Overall status of the NetProfiler and NetExpress storage systems can be:

- Green - OK; everything performing normally
- Yellow - Warning; low disk space
- Red - Alert; an alert condition is displayed; a high-severity SNMP trap and an email notification are sent if configured

Figure 6-15. Storage Status - Normal

If the Overall storage status is not “OK,” then a Drives or Partitions subsection is displayed to report any of the following problems:

- Drives
 - Failed
 - Missing

- Partitions
 - Degraded
 - Not Mounted
 - Mounted as read-only
 - Rebuilding
 - Low space
 - No space

In addition to the status messages, an image of the chassis is displayed to indicate the location of disk drives. The image shows a red box outline over the location of a disk drive that is missing or reporting a problem. Hover your mouse over the red box to display the name and serial number of the disk drive.

The image indicates the good disk drives with gray boxes over their locations.

Figure 6-16. NetProfiler System > Information page Storage Status section

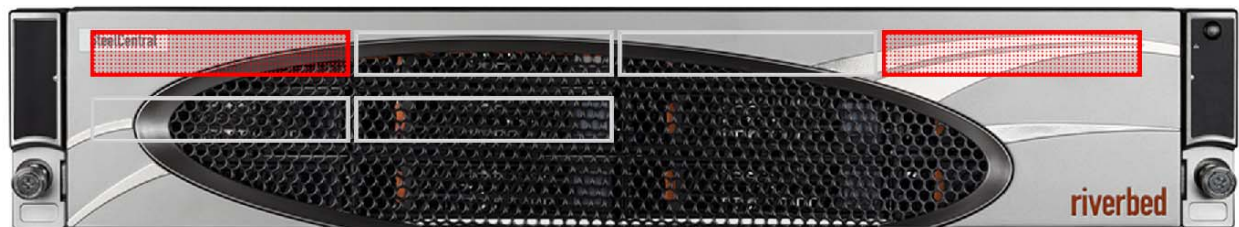


Figure 6-17. NetExpress System > Information page Storage Status section



Data sources

The appliance reports its sources of traffic data on the System > Devices/Interfaces page. Using list entries or mouse-rollover pop-ups, this page provides the following information for devices and their interfaces from which the appliance is receiving data:

- Devices
 - Status
 - IP address
 - Device type (in terms of what type of data is being sent)
 - Time synchronization - Reports NTP synchronization for Sensor and Flow Gateway sources, and PTP synchronization for NetShark sources.
- Device Interfaces
 - Status
 - IP Address:Index of interface
 - Interface name (ifDescr; assigned on the data source device)

- Interface label (as assigned on the appliance)
- Interface description (ifAlias; assigned on the data source device; the appliance displays up to 65 characters)
- MAC address
- Interface type (e.g., Ethernet CSMA/CD RFC3635)
- MTU (maximum transmission unit)
- Traffic rate (traffic in bits per second that the appliance tracks)
- Utilization (percent of device speed that the appliance currently sees being used)

Much of this information must be obtained from the data source devices. For devices that send flow data directly to the NetExpress, the NetExpress uses SNMP to obtain the information. For sources that send data to Flow Gateways, the Flow Gateways use SNMP to obtain the information. They then send it to the NetProfiler.

You can specify which version of SNMP and what community name the NetExpress or the Flow Gateways use to contact the devices. You can assign labels to interfaces. The appliance uses these labels when displaying interface information.

The data source devices must be configured to send flow data (NetFlow, SteelFlow Net, sFlow, IPFIX) to the SteelCentral appliance. NetExpress or Flow Gateway can also receive NSEL (NetFlow Security Event Logging) from Cisco ASA (Adaptive Security Appliance) version 9.1(2) or later. However, it uses only the flow byte counts, the same as it would when receiving NetFlow from a router.

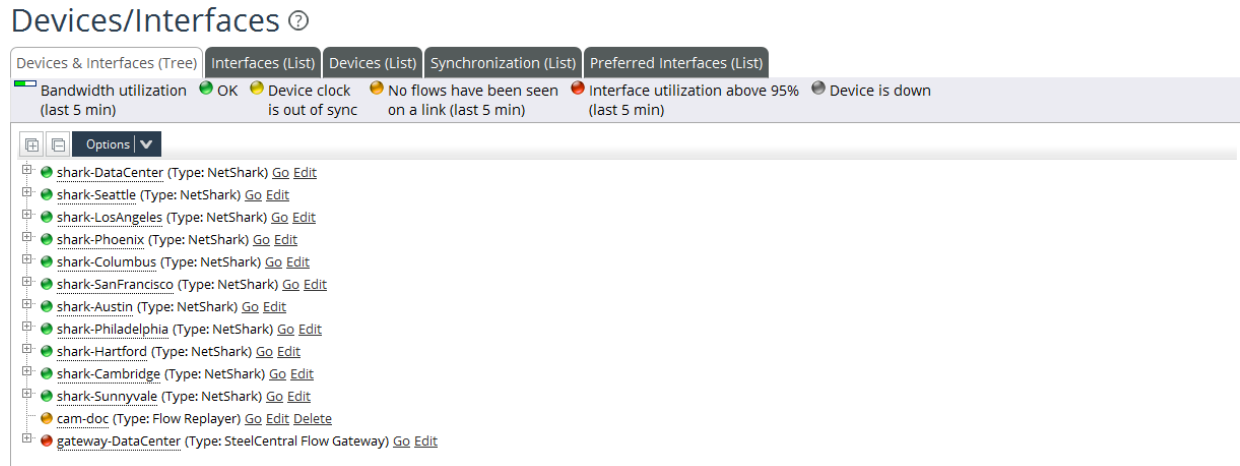
When the appliance receives data from a device, either directly or via a Flow Gateway, it automatically lists the device IP address, name, type, and status on the System > Devices/Interfaces page.

The NetExpress or the Flow Gateway then attempt to obtain the detailed information using SNMP. Both use the default settings for SNMP unless you have specified other settings.

Additionally, NetProfiler and NetExpress obtain Layer 7 application definitions from NetShark and SteelHead appliances.

The information and controls for monitoring and labeling data sources are displayed on four tabs of the System > Devices/Interfaces page:

- Devices & Interfaces
- Interfaces List
- Devices List
- Synchronization

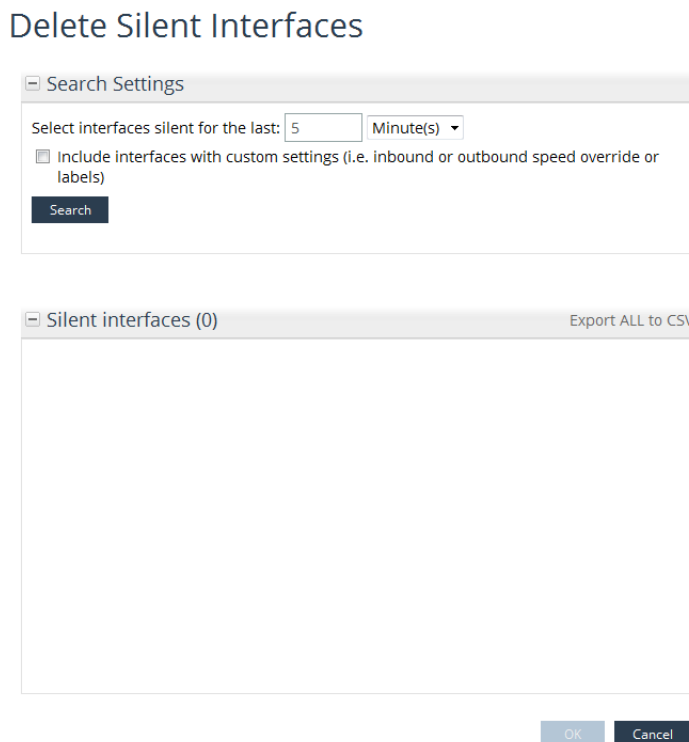
Figure 6-18. System > Devices/Interfaces page

Options menus

The Devices & Interfaces tab, Interfaces tab and Devices tab each have an Options menu. Choices on the Options menu include the following, as applicable to the tab:

Delete Silent Interfaces

The Option menus for the Devices & Interfaces tab, Interfaces tab and Devices tab each include an option to delete interfaces that have been silent for at least 5 minutes and up to 48 hours (2880 minutes).

Figure 6-19. System > Devices/Interfaces page Delete Silent Interfaces option

When deleting silent interfaces, you can prevent the deletion of customized interfaces by clearing the “Include interfaces with custom settings (i.e. inbound or outbound speed override or labels)” check box.

To discover and delete silent interfaces:

1. On the System > Devices/Interfaces page Options menu, choose **Delete Silent Interfaces** to open a popup page.
2. On the Delete Silent Interfaces popup, specify the duration for which an interface must have been silent in order to be included in the search results.
3. Select or clear the option to include customized interfaces in the search.
4. Click **Search**.
5. When the search completes and the silent interfaces are discovered, the **Export all to CSV** link becomes active. You can use this option to export a list of silent interfaces in comma-separated-value text format to a file on your local machine before you delete them. The results section title indicates how many are displayed and the total number discovered.
6. Click **OK** to delete the silent interfaces. This removes up to 100,000 interfaces from the Devices/Interfaces page and from any interface groups they are assigned to. This may take a few minutes to complete, depending on the number of silent interfaces. If there are more than 100,000 interface, repeat the search and delete process.

Global SNMP settings

SNMP settings can be set globally or by device. Settings made for a individual device override the global settings.

Global settings - On the System > Devices/Interfaces page Devices & Interfaces tab or Devices tab, choose Global SNMP Settings from the Options menu to display a window in which you can enable or disable SNMP polling and specify the default SNMP settings.

When you enable polling globally, the “Poll unresolved interfaces data every day”setting does not apply to AppResponse 11.

Select "Update defaults for all devices" to have the NetProfiler propagate these settings to all data source devices whose SNMP Version field is set to Default. Leave the option deselected to have the settings affect only new devices and not overwrite the settings of existing devices.

Individual settings - Each device can be identified as using default settings or custom settings. When a setting for a Flow Gateway is changed, the change is automatically applied to the settings for all devices that are sending data to that Flow Gateway. However, you can change the setting for any individual device.

Assume, for example, that you have a Flow Gateway that is set to use the Default SNMP settings when obtaining device information from each of four devices that are sending it NetFlow data. If you change the SNMP setting for the Flow Gateway to V2c, it will automatically switch to using SNMP Version 2c for contacting all four NetFlow devices.

Continuing this example, you could subsequently set one of the four NetFlow device entries to V1. In this case, the Flow Gateway would use Version 1 to communicate with that device and Version 2c to communicate with the other three.

When you edit the SNMP settings of a switch or lookup router that is listed on the System > Devices/Interfaces page, you can copy those settings to the Configuration > Integration > Switch Port Discovery page.

Export Interfaces

On the Interfaces tab Option menu, choose **Export Interfaces** to export the list of interfaces in comma-separated-value text format to a file on your local system.

Figure 6-20. System > Devices/Interfaces page Global SNMP Settings option

SNMP Polling

SNMP Polling

☐ Enable polling

Poll unresolved interfaces data every: hour(s)

Refresh existing interfaces data every: hour(s)

☐ Update defaults for all devices

SNMP Settings

SNMP Version: ☒ v1 ☐ v2c ☐ v3

SNMP Community (read):

OK

Cancel

Import Interfaces

On the Interfaces tab Option menu, choose **Import Interfaces** to import a list of interfaces in comma-separated-value text format from a file. The CSV file must have two key columns with predefined names: “Device Address” and “Index.” It must also have at least one of the following data columns: “Label,” “Inbound Speed Override (bps),” and “Outbound Speed Override (bps).” The key columns must identify only interfaces present in the system. All other data columns will be ignored on import.

Export Devices

On the Devices tab Option menu, choose **Export Devices** to export the list of devices in comma-separated-value text format to a file on your local system.

Device & Interface tab

The format of the System > Devices/Interfaces page Devices & Interfaces tab displays data source information in the following format:

Figure 6-21. System > Devices/Interfaces page Devices & Interfaces tab

Devices/Interfaces ?

Devices & Interfaces (Tree)

Interfaces (List) | Devices (List) | Synchronization (List) | Preferred Interfaces (List)

Bandwidth utilization (last 5 min)

OK

Device clock is out of sync

No flows have been seen on a link (last 5 min)

Interface utilization above 95% (last 5 min)

Device is down

Options

shark-DataCenter (Type: NetShark) Go Edit

shark-Seattle (Type: NetShark) Go Edit

shark-LosAngeles (Type: NetShark) Go Edit

shark-Phoenix (Type: NetShark) Go Edit

shark-Columbus (Type: NetShark) Go Edit

shark-SanFrancisco (Type: NetShark) Go Edit

shark-Austin (Type: NetShark) Go Edit

shark-Philadelphia (Type: NetShark) Go Edit

shark-Hartford (Type: NetShark) Go Edit

shark-Cambridge (Type: NetShark) Go Edit

shark-Sunnyvale (Type: NetShark) Go Edit

cam-doc (Type: Flow Replayer) Go Edit Delete

gateway-DataCenter (Type: SteelCentral Flow Gateway) Go Edit

Sensor

Interface

(Device entry line 1)

(Interface entry line)

140

SteelCentral™ NetProfiler and NetExpress User's Guide

Flow Gateway	(Device entry line 1)
Data source device	(Device entry line 2)
Device interface	(Interface entry line)
Device interface	(Interface entry line)
NetShark	(Device entry line 1)
SteelHead	(Device entry line 1)
AppResponse	(Device entry line 1)
Third-party device (NetFlow, sFlow, IPFIX)	(Device entry line 1)
Device interface	(Interface entry line)
Device interface	(Interface entry line)

Device entry line 1 identifies the Sensor, Flow Gateway, NetShark, AppResponse, SteelHead or flow data source that is sending data to the appliance.

Device entry line 2 is used in the case of Gateways to identify the devices that are sending data to the Gateways.

The Interface entry lines provide information about each of the devices interfaces. Additionally, each entry has one or more of the following links and indicators:

Status indicator

Color represents status, as described in the legend. The status color is propagated upward. That is, when the display is collapsed, the status of the parent entry shows the status of the most degraded child entry.

Name link

Rolling your mouse over a device name or interfaces name displays a summary of information about each. You can also left-click or right-click the device or interface name links for additional information. The appliance uses SNMP lookups, if available, to obtain the names of the flow source devices, instead of using DNS name resolution.

Go link

Sensor, Flow Gateway, NetShark and AppResponse entries include a **Go** link that opens the user interface login page of the respective device.

Edit link

On device entries, the **Edit** link opens a window in which you can edit the SNMP settings that the appliance or the Flow Gateway use when contacting the data source devices and their interfaces.

On interface entries, the **Edit** link opens a window in which you can edit the interface label that the appliance uses when displaying information about the interface.

Delete link

If a device or interface is no longer carrying traffic, a **Delete** link is displayed. You can delete the entry for a device that is no longer sending data. If the device resumes sending traffic information, it will automatically be added to the list.

Poll link (NetExpress only)

A **Poll** link is included on entries for devices that are sending NetFlow, SteelFlow Net, sFlow, or Packeteer Flow Detail Records to the appliance. Clicking this link causes the appliance to place the device at the head of the polling queue. This allows you to receive updated information about this device without waiting for its normal turn in the SNMP polling queue. NetShark, Sensor and Flow Gateway products do not have Poll links because they are in continuous communication with the appliance.

Utilization indicator

If the appliance is obtaining utilization information from an interface, then the entry for the interface displays a utilization indicator. Roll your mouse over this indicator to see the percent utilization of the interface.

Interfaces tab

The System > Devices/Interfaces page Interface List tab displays the following information about each interface of the data source devices with which the appliance can communicate:

Figure 6-22. System > Devices/Interfaces page Interfaces list

Devices/Interfaces ?

Devices & Interfaces (Tree) Interfaces (List) Devices (List) Synchronization (List) Preferred Interfaces (List)

Bandwidth utilization (last 5 min) OK Device clock is out of sync No flows have been seen on a link (last 5 min) Interface utilization above 95% (last 5 min) Device is down

Search by Device Address or Hostname (e.g., 172.31/16 or localhost)

Interfaces 1 - 10 of 118

Status	Device Address	Device Hostname	Index	Name (ifDescr)	Label	Description (ifAlias)	MAC	Type	Type Description
OK	10.99.11.252	SH-Seattle	1	lan0_0					
OK	10.99.11.252	SH-Seattle	2	wan0_0					
OK	10.99.11.253	shark-Seattle	1	mon0			00:04:11:99:99:07	ethernetCsmacd	Ethernet CSMA/CD RFC3635
OK	10.99.12.252	SH-LosAngeles	1	lan0_0					
OK	10.99.12.252	SH-LosAngeles	2	wan0_0					
OK	10.99.12.253	shark-LosAngeles	1	mon0			00:04:12:99:99:07	ethernetCsmacd	Ethernet CSMA/CD RFC3635

- Status (as explained by the color legend on the right side of the page)
- IP address
- Host name
- Index of the interface
- Name of the interface (as defined on the device)
- Label (which you can define on this page)
- MAC address of the interface
- Type of interface
- Type name
- MTU (maximum transmission unit)
- Speed (bits per second)
- Utilization (percent of maximum bandwidth utilization)

You can use the search feature to search for particular devices by IP address or CIDR address range. Performing a search restricts the content of the page to the specified IP address or CIDR address range.

Devices tab

The System > Devices/Interfaces page Device List tab displays the following information about each data source device with which the appliance can communicate:

Figure 6-23. System > Devices/Interfaces page Devices list

Devices/Interfaces ⓘ

Devices & Interfaces (Tree) Interfaces (List) Devices (List) Synchronization (List) Preferred Interfaces (List)

Bandwidth utilization (last 5 min) OK Device clock is out of sync No flows have been seen on a link (last 5 min) Interface utilization above 95% (last 5 min) Device is down

Search by Device Address or Hostname (e.g., 172.31/16 or localhost)

Devices 1 - 10 of 36

Status	Device Address	Device Hostname	Type	Version	Time Synchronization	SNMP	Poll
●	10.38.129.70	cam-doc	Flow Replayer	N/A		Edit	Poll
●	10.99.11.252	SH-Seattle	SteelHead NetFlow	CascadeFlow		Edit	Poll
●	10.99.11.253	shark-Seattle	NetShark				Poll
●	10.99.12.252	SH-LosAngeles	SteelHead NetFlow	CascadeFlow		Edit	Poll
●	10.99.12.253	shark-LosAngeles	NetShark				Poll
●	10.99.13.252	SH-Phoenix	SteelHead NetFlow	CascadeFlow		Edit	Poll
●	10.99.13.253	shark-Phoenix	NetShark				Poll
●	10.99.14.252	SH-Columbus	SteelHead NetFlow	CascadeFlow		Edit	Poll
●	10.99.14.253	shark-Columbus	NetShark				Poll
●	10.99.15.252	SH-SanFrancisco	SteelHead NetFlow	CascadeFlow		Edit	Poll

1 2 3 4 go to page 1 Show: 10 entries per page

- Status (as explained by the color legend)
- IP address
- Host name
- Type of data
- Version of the communication link software
- Time Synchronization - Reports NTP synchronization for Sensor and Flow Gateway sources, and PTP synchronization for NetShark sources.
- SNMP version that the appliance is to use for obtaining information
- SNMP community name that the appliance is to use

On the SteelCentral™ NetExpress, the entry for device that is sending NetFlow, SteelFlow Net, sFlow, or Packeteer Flow Detail Records to the appliance includes a **Poll** link. Clicking this link causes the appliance to place the device at the head of the polling queue. This allows you to receive updated information about this device without waiting for its normal turn in the SNMP polling queue. Cascade Sensors and Gateways do not have Poll links because they are in continuous communication with the appliance.

You can use the search feature to search for particular devices by IP address or CIDR address range. Performing a search restricts the content of the page to the specified IP address or CIDR address range.

Synchronization tab

The Synchronization tab of the System > Devices/Interfaces page lists the polling status of SteelHead and NetShark appliances, and of Cisco devices using class-based QoS configurations. It polls these devices to get the following data:

- SteelHead - Application identification information and SteelHead QoS shaping configuration information. Polling begins as soon as NetProfiler or NetExpress receives SteelFlow Net data from a SteelHead.
- NetShark - Application identification information. Polling begins when NetShark sends data to NetProfiler or NetExpress.
- AppResponse 11 - URL and Auto-Recognized application identification information. Polling begins when AppResponse sends data to NetProfiler.
- Class-based QoS devices - Statistics and configuration information for traffic classes and traffic policies defined in the Cisco router's Quality of Service configuration. Polling begins when NetProfiler receives NetFlow data from a properly-configured router.

Figure 6-24. System > Devices/Interfaces page Synchronization - SteelHead

Devices/Interfaces ?

Devices & Interfaces (Tree)
Interfaces (List)
Devices (List)
Synchronization (List)
Preferred Interfaces (List)

Synchronization initializing
 Synchronization succeeded
 Synchronization failed
 Synchronization not available
 Device access disabled

Device type: ☒ SteelHeads ☐ NetSharks ☐ AppResponses ☐ CBQoS Devices

Devices Selected Actions ... Global Actions ...

<input type="checkbox"/>	Device Address	Device Hostname	Access Code	Polling	App Poll Status	QoS Poll Status
<input type="checkbox"/>	10.33.131.203	pandafood	Not Configured	Enabled		
<input type="checkbox"/>	10.33.131.63	falconcf1	Custom	Enabled		
<input type="checkbox"/>	10.1.11.175	sf-fishsfe2_old	Not Configured	Enabled		

1
go to page
Show: 10 entries per page

NetProfiler or NetExpress poll these devices every 24 hours. Additionally, you initiate polling on any or all devices manually from the Selected Actions menu or the Global Actions menu. Select the Device Type to see the polling status.

The polling status can be:

- Synchronization initializing - The appliance has received traffic statistics from the device and is now polling it for information.
- Synchronization succeeded - The appliance successfully obtained information from the device and has updated its databases.
- Synchronization failed - The appliance was unable to obtain application definitions or SteelHead QoS shaping configuration information. This can happen if:
 - REST access is disabled on the SteelHead.
 - Authentication failed (for example, the SteelHead and the NetProfiler are not using the same access code).
 - The SteelHead is not using SteelFlow Net, SteelFlow Net-compatible, or NetFlow v9 format for exporting flow data.
 - There is a network communication error, such as a firewall blocking the REST API access port.
- Synchronization not available - The NetShark is running an older software version that does not support using the REST API for application synchronization. (This applies to only NetShark appliances.)
- Device access disabled - Polling has been disabled on the NetProfiler. This could mean that someone has used the Selected Actions menu and disabled polling of this particular appliance, or someone has used the Global Actions menu and disabled polling of all devices.

Hover your mouse over the status indicator to see the time that the status was determined.

The list of devices is sortable by column. Click the column heading to sort the table by a column.

The table has two menus:

- Selected Actions - Applies to only those devices that are selected in the check box column.
- Global Actions - Applies to all devices in the list.

The menu selections differ slightly between NetShark and SteelHead appliances. The “Device type” selection toggles the display between NetShark appliances and SteelHead appliances.

To check polling status or configure polling options for a NetShark appliance, set the “Device type” to NetShark. To check polling status or configure polling options for a SteelHead appliance, set the “Device type” to SteelHead. To check polling status or configure polling options for a Cisco router, set the “Device type” to CBQoS Devices. Refer to the on-line help system for additional requirements for class-based QoS polling.

Note that “synchronization” on Synchronization tab of the System > Devices/Interfaces page refers to the NetProfiler or NetExpress getting application definition information from the NetShark, AppResponse 11 and SteelHead appliances and getting SteelHead QoS configuration information from SteelHead appliances. It does not include sending information to the NetShark, AppResponse 11 or SteelHead appliances.

The NetShark and AppResponse 11 appliance have synchronization features that causes the NetProfiler or NetExpress to send port names and user-defined application information to them. That synchronization is initiated from the NetShark and AppResponse 11 appliance, and is not performed from the NetProfiler user interface.

Figure 6-25. System > Devices/Interfaces page Synchronization - NetShark

Devices/Interfaces ?

Devices & Interfaces (Tree) | Interfaces (List) | **Devices (List)** | Synchronization (List) | Preferred Interfaces (List)

☐ Synchronization initializing
 ☒ Synchronization succeeded
 ☐ Synchronization failed
 ☐ Synchronization not available
 ☐ Device access disabled

Device type: ☐ SteelHeads ☒ NetSharks ☐ AppResponses ☐ CBQoS Devices

Devices Selected Actions ... Global Actions ...

Device Address	Device Hostname	Polling	App Poll Status
10.38.133.227	cam-tarpon-exp1	Enabled	<input checked="" type="radio"/>

1 go to page 1 Show: 10 entries per page

Devices supporting Class-based QoS

NetProfiler and NetExpress can poll Cisco routers to retrieve statistics and configuration information for traffic classes and traffic policies defined in the router’s Quality of Service configuration. NetProfiler and NetExpress display class-based QoS (CBQoS) traffic statistics in the Reports > Shortcuts > Interface Information report.

The appliance stores the statistics for 30 days. The status of CBQoS polling is displayed on System > Devices/Interfaces page Synchronization tab when you select CBQoS Devices as the Device type.

To poll Cisco routers for CBQoS information, NetProfiler and Net Express require the following:

- The router must support the CISCO-CLASS-BASED-QOS MIB.
- QoS policies and traffic classes must be defined on the router.
- The router must enforce persistence across all CBQoS MIB indexes, including cbQosConfigIndex, cbQosObjectsIndex, and cbQosPolicyIndex. Refer to the Cisco document titled “QoS CBQoS MIB Index Enhancements” for details.

- NetProfiler must be configured to use SNMP v2c or 3 to poll the Cisco router for CBQoS information. This is set in the SNMP Polling popup window. Open the window by choosing Edit in the list of devices on either the System > Devices/Interfaces page Devices & Interfaces (Tree) tab or the System > Devices/Interfaces page Devices (List) tab. The per-device SNMP version setting overrides the Global SNMP version setting.

SNMP polling of CBQoS information can be enabled or disabled for each device. Note that SNMP polling for CBQoS information is separate and independent from SNMP polling for other switch and router information. When the “Copy SNMP settings to Switch Port Discovery” option is selected on the SNMP Polling popup window, CBQoS polling information is not included in the settings that are copied.

CBQoS polling is disabled by default. You can enable it in the SNMP Polling popup window for a supported device and choose a polling interval of 5 or 15 minutes.

NetProfiler or NetExpress polls the CBQoS source device for traffic statistics every 5 or 15 minutes, as specified. It polls the CBQoS source device for configuration information once each 24 hours.

You can manually initiate polling on the System > Devices/Interfaces page Synchronization tab by selecting CBQoS Devices as the Device Type and choosing a Poll selection from the Selected Actions or Global Actions menu.

If you disable polling for a device, the polling configuration and statistics are discarded. If you change the polling interval, the CBQoS statistics are discarded, but the polling configuration is saved.

Figure 6-26. System > Devices/Interfaces page Synchronization - CBQoS Devices

Devices/Interfaces ?

Devices & Interfaces (Tree) Interfaces (List) Devices (List) Synchronization (List) Preferred Interfaces (List)

☐ Synchronization initializing
 ☒ Synchronization succeeded
 ☐ Synchronization failed
 ☐ Synchronization not available
 ☐ Device access disabled

Device type: ☐ SteelHeads ☐ NetSharks ☒ CBQoS Devices

Devices

Selected Actions ... Global Actions ...

Device Address	Device Hostname	Polling Interval	CBQoS Config Poll Status	CBQoS Stat Poll Status
<input type="checkbox"/> 10.38.151.2	sgsinpdc05or02.dbs.com.sg-13-2-1-2-2	300	<input checked="" type="radio"/>	<input checked="" type="radio"/>
<input type="checkbox"/> 10.38.129.20	cam-1941-1	300	<input checked="" type="radio"/>	<input checked="" type="radio"/>

go to page Show: 10 entries per page

Preferred Interfaces tab

Refer to [“Selecting preferred interfaces” on page 26](#) for a description of the System > Devices/Interfaces page Preferred Interfaces tab.

Audit trail

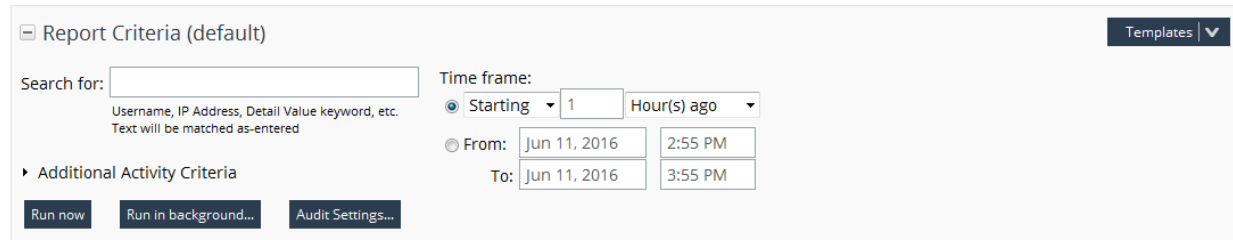
Changes and activities occurring on the appliance can be recorded and reported. The System > Audit Trail page enables you to generate a report of all significant configuration and usage activities that have occurred on the appliance. You can limit the report to activities associated with a specific user name, IP address or event in the appliance during a specified time frame.

Report Criteria

The Report Criteria section determines what the report will contain, what time frame it will cover, and how it will be run.

Figure 6-27. System > Audit Trail Report page Report Criteria section

Audit Trail



Search for text box

The **Search for** box accepts a free-form text term. This limits the report to audit records that contain the specified term. The term can be any:

- User host IP address
- Module
- IP address (for Enterprise NetProfiler modules)
- User
- Name
- Details (any value that appears in the Details column of the report)

The **Search for** box requires only enough text to uniquely identify the term.

Time frame

You can specify the time frame of the report relative to the current time or as an absolute time interval.

Relative to the current time

Starting - Specify the most recent number of minutes, hours, days, weeks, months or years that the report is to cover, ending now. For example, if you specify the **Starting** value as 1 week ago, then the time frame of the report will start at this time last week and end now. If you specify 1 year ago, the time frame will start at this time on this date last year and end now.

Previous - Specify the most recently ended full minute, hour, day, week, month or year before the current minute, hour, day, week, month or year, respectively. For example, if the current time is 10:17 AM Wednesday and you specify the Previous value as 1 hour, then the time frame of the report will start at 9:00 AM and end at 10:00 AM today. If you specify the previous 1 week, the time frame will start at 12:00 AM Monday of last week and end at 12:00 AM Monday of this week. If you specify the previous year, then the time frame will start at 12:00 AM, January 1st of last year and end at 12:00 AM, January 1st of this year.

As an absolute time interval

From/To - Specify the time frame either by entering dates and times manually or by:

- Clicking the date to display a calendar tool, then choosing a date from the calendar.
- Clicking a time to display a list box of times, then choosing a time from the list.

The time frame starts at the “From” time and ends at the “To” time.

Additional Activity Criteria

This section further limits the report to activities or events caused by a user specified in the Username box and to types and subtypes of activities.

Username

The Username can be web interface user account name or shell account user name. Activities caused by the system itself (not originated by a user) are reported with the user name **system**.

Placing a user account in the Username box restricts the report to just those activities or events that the user caused. This is different from placing a user account name in the **Search for** box. For example, if you put the user name “jdoe” in the **Search for** box, the report could include the audit record of an administrator editing jdoe’s user account profile. In that case the change was made by the administrator, but it will be reported because it involved jdoe.

Activity Type and Subtype

The Activity Type field limits the report to a major category of activity. The Subtype field limits the report to only a specific sub-category of activities within the selected Activity Type. By default, three System activity subtypes are disabled:

- Encryption and Decryption
- Hash Operation
- Command Execution

These activity subtypes are considered to be the most chatty. When the FIPS Compatible Cryptography or Strict Security mode are enabled on the Configuration > Appliance Security > Security Compliance page, logging of all activity types and subtypes is enabled. However, logging of these three subtypes can be switched off after the appliance has been booted in the FIPS Compatible Cryptography or Strict Security mode.

Activity types and subtypes are described in a separate section below.

Run now

Click **Run now** to run the report and display the results as soon as they are available.

Run in background

Clicking **Run in background** opens a window for you to specify the title of the report and select options for saving and emailing the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

If an email server has been specified on the Configuration > General Settings page, you can enter a list of email addresses to which the report will be mailed. You can also enter a message to go into the email and specify if the report is to be attached as an HTML, PDF or Comma-Separated-Value file.

Audit Settings

This feature determines what types and subtypes of events are logged and for how long. Note that this affects all audit reports because activities that are not logged cannot be reported.

The default setting is to log all audit events for 90 days. To reduce the number of activities that are logged, select **Log custom set of audit events** and select the events that are to be logged.

When you click **OK** the settings are applied to future audit logging. Existing logs are not deleted until they reach the age specified in the **Pruning Settings** section.

Figure 6-28. System > Audit Trail Report page Run in Background setup

Run in background

Name:

Keep report

Keep report until: ☒ Space is needed for new reports
☐ I delete it

Report distribution

Distribute via email to: Message:

Format: ☒ HTML ☐ PDF ☐ CSV

Figure 6-29. System > Audit Trail Report page Change Audit Settings

Change Audit Settings

Pruning Settings

Number of days audit trail should be kept:

Logging Settings

☐ Log all audit events ☒ Log custom set of audit events

Data Change (Check: all none)

- ☒ User Change
- ☒ Settings Change
- ☒ Notification Change
- ☒ Policy Change
- ☒ Group Change
- ☒ Time Change
- ☒ Topology Change

Notification (Check: all none)

- ☒ Traps Sent
- ☒ Email Sent

Report results

When the report completes it displays an activity list giving the:

- Time – the time of an activity is logged in UTC but displayed in local time
- Type and Subtype – activities specified in the Report Criteria section
- Module Name – if the appliance is an Enterprise NetProfiler, then this column is displayed by default instead of the User Host Name column. The Module Name is the resolved name of the Enterprise NetProfiler module that logged the activity.
- User – the user who originated the activity. This may be a human user or the system.
- Successful – indicates if the activity was successful.
- Event Count – how many identical events occurred within a 1-minute time frame. Rather than report each event individually, the report de-duplicates identical events that happened within the same time frame and tells you how many there were at that time.
- Details – additional information about the activity

Figure 6-30. System > Audit Trail Report page - Report results

Audit Trail ⓘ

Report Criteria (default) Templates ▼

Audit Events Report (Jun 11, 2016, 4:57 PM - 5:57 PM EDT) Report Options ▼ ✕

riverbed Activity Type: All

Activities

Activity List 1 - 20 of 65 ▼

Time	Type	Subtype	User Host Name	User	Successful	Event Count	Details								
Jun 11, 2016 5:42:36 PM	User	Authentication Check	jerry1-w7	admin	Yes	1	<table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>URL</td> <td>/api/profiler/1.6/interfaces.json</td> </tr> <tr> <td>Authentication type</td> <td>COOKIE (SESSION)</td> </tr> <tr> <td>User Role</td> <td>Administrator</td> </tr> </tbody> </table>	Field	Value	URL	/api/profiler/1.6/interfaces.json	Authentication type	COOKIE (SESSION)	User Role	Administrator
Field	Value														
URL	/api/profiler/1.6/interfaces.json														
Authentication type	COOKIE (SESSION)														
User Role	Administrator														
Jun 11, 2016 5:40:35 PM	User	Authentication Check	jerry1-w7	admin	Yes	1	<table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>URL</td> <td>/api/profiler/1.6/cbqos/devices.json</td> </tr> <tr> <td>Authentication type</td> <td>COOKIE (SESSION)</td> </tr> <tr> <td>User Role</td> <td>Administrator</td> </tr> </tbody> </table>	Field	Value	URL	/api/profiler/1.6/cbqos/devices.json	Authentication type	COOKIE (SESSION)	User Role	Administrator
Field	Value														
URL	/api/profiler/1.6/cbqos/devices.json														
Authentication type	COOKIE (SESSION)														
User Role	Administrator														

The following additional columns can be added to the report by choosing **Add/Remove Columns...** on the Activity List menu:

- **Module IP** – if the appliance is an Enterprise NetProfiler, this is the IP address of the module on which the activity was logged.
- **Process ID** – the ID of the process that originated the activity. This may be a user or the system.
- **Session ID** – the ID of your browser session
- **User Host Name** – the resolved host name of IP address from which the user listed in the activity caused the activity that was logged.
- **User IP** – the IP address from which the user listed in the activity caused the activity to occur. This could be a user's IP address or localhost for system user activities.

All columns except the Details column can be sorted in ascending or descending order.

Report controls

The report controls include:

- Activity List section menu
- Templates menu at the top of the page
- Page display control icon at the upper-right corner of the report results section
- Report Options menu at the top of the report results section

Activity List section menu

The menu beside the title of the Activity List section of the report offers the following actions:

Add/Remove Columns – opens a column chooser tool that allows you to add more columns to the report where applicable. This can provide additional detail for some types of activities.

Change Number of Rows – controls how many activity entries are displayed on a page.

Show Filter – displays a filtering tool that allows you to limit the display to specific values appearing in each column. The use of the filter tool is described in the online help system.

Export to Host Group – uses the IP addresses in the User IP or Module IP column to create a host group. This allows you to track and alert on a group of IP addresses of interest.

Export to CSV – exports the contents of the report to a comma-separated-value file for use with other tools.

Templates menu

Use the Templates menu to perform any of the following:

Save As/Schedule – opens a page on which you can:

- Save the current settings as a template for generating reports.
- Schedule the appliance to generate reports (once or periodically) using these settings. The name of the report template is used with the date of the report as the report name.
- Specify whether the generated reports should be saved until you delete them or until the storage space is needed for new reports. (When the storage capacity is exhausted, the appliance overwrites the oldest reports with new reports unless you indicate that they should be saved until you delete them.) Saved reports are accessible on the Reports > Saved Reports page.
- Specify who the scheduled reports should be emailed to, and in which format.

Specify an email message to be included when reports are distributed.

Figure 6-31. System > Audit Trail Report page Save/Schedule option

Save / Schedule template

Name:

Report generation schedule

☒ Add schedule ☐ Show Time Zones ?

☒ One time

☐ Hourly

☐ Daily

☐ Weekly

☐ Monthly

☐ Quarterly

Start from: Run at:

Run one time.

Not scheduled!

Keep report

☒ Keep report until: ☒ Space is needed for new reports ☐ I delete it

Report distribution

Distribute via email to: Message:

Format: ☒ HTML ☐ PDF ☐ CSV

If an outgoing mail server has been configured on the Configuration > General Settings page, the Save as/Schedule page includes a field for entering email addresses to which the report will be sent. The number of rows included in an email report is set on the Configuration > UI Preferences page.

Save as Default – saves the current Report Criteria settings and any modifications that have been made to a report that is currently being displayed.

Load Default Template – loads the default report criteria. If you have modified the criteria you can return to what you have previously saved as the default criteria.

Page display control icon

A small page icon at the upper-right corner of the report results section allows you to run additional reports without closing the first one. Click this icon to transfer the report in a new window.

Figure 6-32. Page display control



Report Options menu

Use the Report Options menu to perform any of the following:

Save as – saves the report on the Reports > Saved Reports page.

Schedule – opens a page on which you can schedule the running of the report and specify the email distribution list and file format, as described under “Templates” above.

Print – prints the report using your machine's printing facilities.

Email – emails the report to one or more email addresses. The report is mailed in HTML format or attached to the email as a PDF or CSV file. If you select the PDF or CSV option, you can specify the name of the attached file. The name can include characters that will be replaced by the date and time that the email was sent, as follows:

%d is replaced by the date in MMDDYY format. For example, 021509.

%t is replaced by the time in HHMM format. For example, 1536.

This option requires a mail server to have been identified in the Outgoing Mail Server (SMTP) Settings section of the Configuration > General Settings page.

Export – exports report as CSV (comma-separated values) file, HTML archive file or PDF file.

Keeping reports

Reports are normally saved until you delete them or until the limit of the storage capacity is reached. When no storage capacity is left, the appliance deletes the oldest report to make room for the next one to be saved.

You can modify this behavior with the Keep feature. To ensure that a report does not get deleted, select the check box for the report and then click Keep/Unkeep. This displays an asterisk beside the report to indicate that it will be saved indefinitely, until you specifically delete it.

If the storage limit has already been reached, the appliance deletes the oldest report not marked to be kept indefinitely before saving a new report. If enough reports are saved indefinitely to reach a 10 Gigabyte storage limit, then no more reports can be saved. That is, you can still view an existing report or run a query on any of the Audit Trail Report page and view the results. However, the query results will not be saved as a report.

Running a query in the background or scheduling a query to be run in the background automatically saves the report. Therefore, these background operations are not available if the report storage capacity is completely consumed by reports marked to be kept. You must first delete enough indefinitely saved reports to free the space necessary for the new report to be saved. To delete a report, select the check box for the report and then click Delete.

The Report Storage % field indicates what percent of the 10 Gigabyte storage capacity is in use. The rate at which storage capacity is used depends on the size of your reports.

Time zones for scheduled reports

Reports can be scheduled in terms of the time zone your account uses or in terms of any other time zone, such as the time zone of the main activity that you are monitoring. If you want a report to be generated at a consistent time of day, schedule the time of day in terms of the time zone of the activity that you are monitoring.

Each report template can be scheduled independently. For example, one might be scheduled to generate reports at 12:00 AM in London, and another might be scheduled for 12:00 AM in Hong Kong.

When you schedule a time for a report template to generate a report, the schedule becomes part of the report template. You can modify the template either by choosing **Save as/Schedule** from the **Templates** menu on a report or by going to the **Saved Reports** page and modifying the template there and clicking **Save as/Reschedule** in the **Templates** section. Both these paths open the **Save/Schedule** template page.

By default, the **Start from** and **Run at** date and time settings on the **Save/Schedule** template page are based on the time zone that your account uses.

To use a different time zone:

1. Click **Show Time Zones** to display a drop-down list of available time zones.
2. Select the time zone in which you want the **Run at** time to apply.

Note: You can select a time zone using the **Continent/City** convention, the **Country/Zone** convention, or the time zone abbreviation. However, to ensure that the selected time zone is automatically adjusted for summer and winter time changes, it is preferable to select it using the **Continent/City** convention instead of the **Country/Zone** convention or its abbreviation.

Note on run times

Reports always cover the time frame that they are specified to cover. However, they do not start running exactly at the end of the time frame. It requires several minutes to collect and process the data for the time frame. Therefore, the **Run Time** listed in the **Reports** section is later than the **Next Run Time** displayed in the **Templates** section for the template that generates the report.

The **Next Run Time** corresponds to the end of the time frame that the report is to cover. That is, the report is run “as of” that time, rather than exactly at that time. However, the **Run Time** displayed in the **Reports** section is the time at which the report actually was run or will be run.

Table filters

Table filters enable you to limit the length of a table to just the entries of interest. On report pages, use the menu to switch table filters on or off.

On each table where a table filter is enabled, it is displayed in the first row of the table. It offers a drop-down list of operations that apply to that particular table. Table filtering includes the following operations, depending on the information that is to be filtered.

Operation	Results of filtering operation
=	Lists only the name, number, address, or other table column entry that exactly matches the filter phrase. This operation is case-sensitive.
Not=	Lists all table column entries except for the one that exactly matches the filter phrase. This operation is case-sensitive.

Operation	Results of filtering operation
<	Lists only the numeric, date, time, or duration entries in the table column that are less than the filter phrase.
>	Lists only the numeric, date, time, or duration entries in the table column that are greater than the filter phrase.
Like	Lists all table column entries that include the filter phrase. For example, “Like 10” lists all table column entries that have “10” in their IP address or name. This operation is case-insensitive.
Not Like	Lists all table column entries that do not include the filter phrase. For example, “Not Like dep” lists all entries that do not include the string “dep.” That is, it does not list groups with names that include “dept” and “department.” This operation is case-insensitive.
Word	Lists all the “words” in a table column that exactly match the filter phrase. A “word” in this case can be the “tcp” component of “tcp/80” A slash (/) is recognized as a word delimiter. (An underscore is not recognized as a word delimiter, and spaces in entries are not permitted.) This operation is case-insensitive.
CIDR	Lists all table column entries that include an address within the CIDR block specified as the filter phrase. For interfaces, the contents of the table are filtered for the IP address of the device that has the interface.
Range	Lists all the numbers or dates in the column that are within a specified range. A calendar tool is provided for choosing start and end dates.
Day	Lists all table column entries that match the date specified in the filter phrase.

Note on run times

Reports always cover the time frame that they are specified to cover. However, they do not start running exactly at the end of the time frame. It requires several minutes to collect and process the data for the time frame. Therefore, the Run Time listed in the Reports section is later than the Next Run Time displayed in the Templates section for the template that generates the report.

The Next Run Time corresponds to the end of the time frame that the report is to cover. That is, the report is run “as of” that time, rather than exactly at that time. However, the Run Time displayed in the Reports section is the time at which the report actually was run or will be run.

Activity Types and Subtypes

The Audit Trail report can include all activities or be limited to any one of the following types of activities:

- Data Change
- Notification
- User
- System

Each of these types of activities includes subtypes, which are more detailed categories of activities. The sections below identify the Web UI pages for which activities are logged.

Data Change activities

The Data Change activity type includes the following subtypes:

User Change

This subtype reports changes on or related to the following UI pages:

- Configuration > Account management > User Accounts
- Configuration > Change Password
- RADIUS user first log in
- Configuration > Account Management > ODBC DB Access

Settings Change

This subtype reports changes on or related to the following UI pages:

- System > Devices/Interfaces
 - Global SNMP Settings
 - Edit device (edit device SNMP settings)
- System > Audit Trail > Audit Settings...
- System > Devices/Interfaces > SNMP Settings > Copy to router/switch
- Definition > Sensors/NetSharks & SteelHeads
- Configuration > Packet Capture (NetExpress only)
- Configuration > Flow Log > Reallocation and Re-balancing
- Configuration > Integration > Identity sources
- Configuration > Integration > Load balancers
 - Add...
 - Import...
 - Edit/Delete
- Configuration > Integration > Switch port discovery
 - Add Device...
 - Import...
 - Edit/Delete
- Configuration > Account Management > Remote Authentication
- Configuration > Account Management > User accounts > Settings...
- Configuration > Appliance Security > Password Security
- Configuration > Behavior Analysis > Security tab > Security Profile button
- Configuration > Appliance Security > Security Compliance
- Configuration > General Settings > Edit /etc/hosts...
- Configuration > Flow Forwarding (Flow Gateway only)
- Configuration > NetProfiler Export
- Configuration > Licenses
- Configuration > General Settings > Edit DNS settings

- Configuration > General Settings > Edit NTP settings
- Configuration > General Settings > Edit SNMP settings

Notification Change

This subtype reports changes on or related to the following UI pages:

- Behavior Analysis > Notifications
- Behavior Analysis > Notifications > Recipients

Policy Change

This subtype reports changes on or related to the following UI pages:

- Services > Manage Services > Settings... button
- Services > Manage Services > Actions > Tune
- Behavior Analysis > Policies > Services > Actions > Tune and “Tune” from the right-click menu
- Behavior Analysis > Policies > Performance & Availability > New...
- Behavior Analysis > Policies > Performance & Availability > Actions > Tune
- Behavior Analysis > Policies > Security & Health tab
- Behavior Analysis > Policies > Security & Health tab > Threshold table
- Behavior Analysis > Policies > User-defined tab
- Event detail report > Snooze
- Services – The following service operations are audited:
 - Committing a service into production for the first time - event of type “Created”
 - Committing a service into production - event of type “Modified”
 - Deleted service - event of type “Deleted” (whether or not the service was in use)

When the service location group type is changed on the General Settings page or the Host Grouping page, a Service type configuration change is logged with old name and new name.

Group Change

This subtype reports changes on or related to the following UI pages:

- Definitions > Host Groups
- Definitions > Applications > Application mappings
- Definitions > Applications > Application fingerprints
- Definitions > Interface Groups
- Definitions > Port names
- Definitions > DSCP
- Configuration > Integration > External links

Time Change

This subtype reports that a user changed the Set System Time settings or NTP settings on the Configuration > General Settings page Time Configuration section.

Topology Change

This subtype reports changes on or related to the following UI pages:

- System > Devices/Interfaces – Label, In User Speed, Out User Speed
- System > Devices/Interfaces > Interfaces tab
 - Edit multiple interfaces
 - Import interfaces info
- Any page: right-click Interface and choose View/Edit...

Notification activities

The Notification activity type includes the following subtypes:

Traps Sent

Reports what SNMP notifications the appliance sent to other systems and whether they succeeded or failed.

Email Sent

Reports what email the appliance sent to other systems or users and whether they succeeded or failed.

User activities

The User activity type includes the following subtypes:

Login

Reports login attempts, name, role, time, success or failure; authentication (local appliance database or remote authentication server) and remote authentication server type.

Logout

- Reports account name, session length and time of logout.
- Reports when a user cancels a login by clicking Cancel to reject the requirements of a login banner.

Session Timeout

Reports the length of a session that has timed out because of inactivity.

Account Locked

Reports that an account has been locked because of three consecutive unsuccessful login attempts.

Account Unlocked

Reports that a user has successfully logged in after the account had been locked because of three consecutive unsuccessful login attempts. This is the first successful login after a lockout period.

Secret Verification

Reports that a password change has been verified. This occurs when a:

- User account login name or password is created or updated.
- User changes a password because it was required on the first or next login.
- Shell account password is changed on the Appliance Security > Security Compliance page.

Note: Any verification that occurs on the client side (such as too few characters in a password field) does not trigger an auditing event.

Re-authentication

Reports that a user has been re-authenticated because they:

- Shut down the system on the System > Shutdown/Reboot page.
- Changed their password because of a requirement to change it on the first or next login.
- Changed their password using the change password feature.

Authentication Check

- RADIUS server check – reports the results of a user clicking the Test link in the Actions column of the Configured Servers section of the Configuration > Account Management > Remote Authentication page RADIUS tab.
- RADIUS user check – reports the results of a user clicking the Test User button in the Roles-Attributes Mapping section of the Configuration > Account Management > Remote Authentication page TACACS+ tab.
- TACACS+ server check - reports the results of a user clicking the Test link in the Actions column of the Configured Servers section of the Configuration > Account Management > Remote Authentication page TACACS+ tab.
- TACACS+ user check - reports the results of a user clicking the Test User button in the Roles-Attributes Mapping section of the Configuration > Account Management > Remote Authentication page TACACS+ tab.
- Shell password change – reports an attempt to change the password of a shell account on the Configuration > Appliance Security > Security Compliance page. Successful or unsuccessful.

Audit Access

Reports that a user generated a new audit report or viewed a saved audit report.

System activities

The System activity type includes the following subtypes:

Key Generation

When an encryption key is generated on the Configuration > Appliance Security > Encryption Key Management page, the Audit report includes the:

- Name of the application (mnmp, ssh, apache, etc.).
- Algorithm used to generate key.

- Length of generated key (bits).

Key Destruction

When an encryption key is deleted on the Configuration > Appliance Security > Encryption Key Management page, the Audit report includes the:

- Name of the application (mnmp, ssh, apache, etc.).
- Algorithm used to generate key.
- Length of generated key (bits).

Key Zeroization

When a key is deleted, the memory where it was stored is overwritten with zeros. The success or error of this operation is reported.

Certificate Generation

When an encryption certificate is generated on the Configuration > Appliance Security > Encryption Key Management page, the Audit report includes the:

- Name of the application (mnmp, ssh, apache, etc.)
- Type of certificate (local or peer)
- Certificate authority (always self-signed)
- Length of time the certificate is valid (days)
- Creator contact information

Certificate Destruction

When an encryption certificate is deleted on the Configuration > Appliance Security > Encryption Key Management page, the Audit report includes the:

- Name of the application (mnmp, ssh, apache, etc.)
- Type of certificate (local or peer)
- Certificate authority (always self-signed)
- Length of time the certificate is valid (days)
- Creator contact information

Encryption and Decryption

When an encrypted connection is established or closed, the source, type of encryption, and any associated errors are reported. Additionally, an activity is recorded when the internal use of a password (such as for SNMP or third party applications) is cloaked or revealed.

Hash Operation

The type and result (success or failure) of hash operations are reported.

Replay

Reports that there was a packet error on an established connection. This could indicate a replay attack on the MNMP connection with other SteelCentral appliances.

Test

When the appliance is booted, it performs self-tests. If the results of the tests are anything other than a pass or fail, they are reported.

Update

Reports that a product update on the System > Update page has started.

Command Execution

Reports the user name, path, and Syslog message when a user or program executes an su, runuser, or sudo command in a shell account.

Startup and Shutdown

Reports the account name and time that a user has shut down or rebooted the appliance on the System > Shutdown/Reboot page.

Also reports on internal programs that stop or start services and power off or power on the appliance. For example, a system reboot shows five events of this type:

- Reboot selected (as user account)
- Reboot initiated (as system account)
- SteelCentral services stopped (as system account)
- System bootup (as system account)
- SteelCentral services started (as system account)

Backup

Reports the time that a backup operation was started on the System > Backup page.

Licenses

Reports that a user has added, deleted or fetched a license key using the Configuration > Licenses page.

Certificate Expiration

Reports that an encryption certificate has expired or that a user has been notified that a certificate will soon expire. This includes the:

- Name of the application (mnmp, ssh, apache, etc.) that uses the certificate
- Certificate Type (Peer, or Local)
- The number of days before expiration, if less than 15

Linux Audit

The appliance runs a modified and extended version of Scientific Linux and reports the following Linux events:

- Setting the System Clock – serial number, command and Syscall
- User login/logout – serial number, command and terminal
- Run level change – serial number, command and old and new value of SYSTEM_RUNLEVEL

NTP Time

Time changes and resynchronizations are recorded and reported.

Shutdown/Reboot

The System > Shutdown/Reboot page enables users with Administrator accounts to shut down or reboot the appliance.

1. Authorize the shutdown or reboot by entering the password of the Administrator account you are currently using.
2. Select the **Reboot** option if you want to restart the product without powering off the appliance.
3. Click **Reboot** or **Shutdown**, as applicable, to initiate the process.

Figure 6-33. System > Shutdown/Reboot page

The screenshot shows the 'Shutdown/Reboot' page. At the top, the title 'Shutdown/Reboot' is followed by a help icon. Below the title is the subtitle 'Shutdown/Reboot the system'. A warning message states: 'Shutdown or reboot may take several minutes. Do not physically disconnect power to your system until you can verify that it powered down or rebooted successfully.' Below the warning, there is a 'Password:' label followed by a text input field. Underneath the password field is a 'Reboot system:' label followed by a checkbox. At the bottom right of the form area is a dark blue button labeled 'Shutdown'.

Note: If you shut down the appliance, do not disconnect chassis power until the appliance has powered off.

Update

The System > Update page indicates the current version of the NetProfiler and NetExpress software and lists any new versions that are available for installation. You can install the update software from this page and specify who is to receive an email notification of the installation.

If the appliance has been configured to automatically download update packages, then you can perform an update from the System > Update page whenever you observe that an update package is available.

If you do not use automatic update downloading, then you must download the update package manually.

When the appliance detects that an update package has been downloaded and is ready to run, it displays the update version on the System > Update page. If it does not detect any updates, then the page displays a message that no updates are available.

Figure 6-34. System > Update page

Update ?

cascade-profiler-VE: No updates downloaded [Update Availability and Settings](#)

Current version: **10.9 (release 20160606_1237)** [Information about system update](#)

▼ Add a different update version

☒ Upload file:

☐ Remote file URL:

▼ Configure notifications

If you would like to be notified of an update by email, please enter a list of semicolon separated email addresses you would like the notification to be sent to.

[-] Associated SteelCentral Products [Distribute auto-downloaded updates now](#)

Name ↑	Type	Version	Status
No Data Available.			

[-] Software Revision History

Version	Date installed
10.9	

You can use the System > Update page to:

- Install software update packages that have been downloaded to the NetProfiler or NetExpress.
- Retrieve update packages from the Riverbed downloads web site.
- Load update packages from your local machine or from a remote server.
- Distribute automatically downloaded updates to SteelCentral appliances that are connected to this appliance.
- Check the current version, available updates, and the revision history.

Refer to the online help system for detailed instructions on managing updates.

Backup

The backup feature securely copies traffic and configuration information to a specified backup system. NetExpress packet logs and index files are not backed up. Additionally, capture jobs are not restored if the backup and restore operations are performed from a physical NetExpress to a virtual edition or vice versa.

The System > Backup page displays the current backup status of the appliance and controls what information is backed up, where it is backed up to, and who is notified when a backup is completed.

Figure 6-35. System > Backup page

Backup ?

Backup Status

Last successful backup performed on: Friday, June 10, 2016 1:05 PM EDT

Last backup status: Last backup successfully completed.

Run Backup

Excluded file types

☒ Exclude flow, rollup and identity logs

Backup location

Username Hostname/IP Path

@ :/

Encryption Password

Create a password to protect the sensitive data in the backup file.
Restoring the appliance from this backup will require the user to enter this password. Safeguard the password.

Notification

Notify this email address when the backup is completed

Run Backup

Backup Status

This section reports the date that the last backup operation was run and whether it completed successfully or failed. It also reports if a backup operation is currently in progress.

Excluded file types

Most NetProfiler appliances have a very large storage capacity. This depends on the expanded memory options (or optional SAN devices, if applicable). A full backup of all information could require significant time and bandwidth. You can use the Exclude option to limit the backup to:

- System setup and configuration information
- User settings that are accessible from the web user interface
- Saved reports
- Analytic and security profiles
- Event details

Select the **Exclude flow, rollup and identity logs** option to exclude the following files from the backup:

- Traffic flow logs
- Rollup logs (This is the information that makes it possible to report on traffic volumes with selectable data resolutions.)
- Identity logs (These are records of user logins, logouts and login attempts.)

Backup location

The backup machine and account must be fully specified in the format:


```
admin@backup-server.company.com: /backup/steelcentral
```

If the backup machine is not configured for SSH, the NetProfiler attempts to automatically set up SSH keys before performing the backup. You will be prompted to enter login information.

The backup operation saves the current set of files plus one previous set in the backup location. That is, the third time you perform the backup operation, it deletes the first set that was backed up. If you need to save more than two versions, change the backup location.

Encryption Password

All sensitive data in the backup image is encrypted with AES256 encryption using this password. This password is required in order to restore the image, so it should be saved and safeguarded.

Notification

Enter an email address for the person or system to be notified when the backup operation completes. Note that in order for the NetProfiler to send email notifications, the Outgoing Mail Server (SMTP) Settings on the Configuration > General Settings page must be specified.

Running the backup operation

When the backup location and notification information has been entered, click **Run Backup** to begin the backup operation. The Backup Status section of the page will indicate that the backup is in progress. A notification of the success or failure of the backup operation will be emailed when the operation completes. This date and status information is also displayed in the Backup Status section of the page until the next backup operation is performed.

If the backup machine is not configured for SSH connections from the NetProfiler, a message is displayed to advise you that this is a prerequisite for performing the backup operation.

Restore operation

The restore operations are performed manually from the command line interface. For additional information, refer to [Appendix B, “Restoring a system”](#) or the online help system.

CHAPTER 7 Service Policies

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for monitoring the services provided by your network. It includes the following sections:

- [“Overview,”](#) next
- [“The Services Policies page”](#) on page 166

Overview

Service policies are created when you configure services to monitor metrics, as described in *Chapter 3, Monitoring Services*. A policy is automatically created for each metric that a service segment is configured to monitor. Higher-level policies are created for all metric categories, front end locations, segments, and services.

Each service segment policy can monitor and alert on multiple service metrics. Each can be tuned individually, except for the segment that includes the end user components, which has a policy for each end user location. These can all be tuned individually.

The NetProfiler and NetExpress provide analytics for monitoring each of the following service metrics:

- Active Connections
- Bandwidth
- New Connections
- Number of TCP Resets
- TCP Retransmission Bandwidth
- Average Application Throughput per Connection
- Average Connection Duration
- Response Time
- Jitter
- MOS
- Packet Loss
- Percent Packet Loss
- R-factor

Depending on the metric, the analytics can analyze the rate, volume and variability of the metric, and can detect spikes or dips that exceed normal ranges. You can tune the amount of variability the analytic tolerates before it indicates that the metric is outside of its normal range.

Policies can be set to generate alerts and notifications when the value of a metric exceeds the range that is normal for the period being analyzed.

The Services Policies page

The Services Policies page provides tools for tuning service policies. It displays the status of all service policies and provides controls for adjusting the tolerance to change for each metric a policy is monitoring. It can be accessed from the **Services > Service Policies** or the **Behavior Analysis > Policies** menu choices.

The Service Policies page has two sections:

- Configured Policies
- Tune Policies

For efficient use of display space, opening one section closes the other section.

Figure 7-1. Services > Service Policies page Configured Policies section

Service Policies

Service			
Performance & Availability			
User-defined			
Security			
Health			
Configured Policies			
Name	Status	Enabled	Actions
ERP	Ready (monitoring)	Yes	Select...
Exchange	Ready (monitoring)	Yes	Select...
FinancePortal	Ready (monitoring)	Yes	Select...
HR-Portal	Ready (monitoring)	Yes	Select...
Sharepoint	Ready (monitoring)	Yes	Select...
VoIP-Calls	Ready (monitoring)	Yes	Select...
Austin-Phoenix	Ready (monitoring)	Yes	Select...
LA-Phoenix	Ready (monitoring)	Yes	Select...
VoIP	Ready (monitoring)	Yes	Select...
MOS	Ready (monitoring)	Yes	Select...
Packet Loss	Ready (monitoring)	Yes	Select...
Percent Packet Loss	Ready (monitoring)	Yes	Select...
R-Factor	Ready (monitoring)	Yes	Select...
Phoenix-Austin	Ready (monitoring)	Yes	Select...
Phoenix-LA	Ready (monitoring)	Yes	Select...

Configured Policies section

The Configured Policies section displays a tree diagram of service policies that monitor at least one metric. For each service policy listed, the diagram is expandable and collapsible, allowing you to show or hide:

- Policies for service segments within the service.
- Policies for end-user locations (applies to only segments that include an end user component).
- Policies for categories of metrics that are monitored for a segment.

- Policies for individual metrics within metric categories.

Each entry in the policy tree diagram includes the status of the policy, whether or not it is enabled, and a list of actions that you can take on the policy, such as disabling it, tuning it and running a report on it.

Status column

Each policy indicates the status of the best of any subordinate policies. For example, if a segment policy includes several metrics policies, and one of the metric policies is in the Ready (monitoring) condition, then that is the status that is shown for the segment policy.

The status of each policy is one of the following:

- **Ready (monitoring)** – The policy is in effect. Baselines are being updated, reports can be run, and the policy can detect events and send alerts and notifications.
- **Ready (baselining)** – The policy is ready, the baselines are being updated, and reports can be run. However, the policy has not been set to detect spikes or dips in metric values, so no events will be detected and no alerts or notifications will be sent.
- **Initializing Baseline** – The analytics used by the policy are still collecting data and creating a model of normal network behavior. The policy is not ready for use yet.
- **Queued** – The appliance has queued the request to create a policy, but other tasks must be completed first.
- **Analytics License Expired** – The policy uses one or more analytics for which no current license can be found.
- **Unknown** – This message is very unlikely to occur. It indicates that there is a problem that requires help from Riverbed Support.
- **Disabled** – The policy has been disabled. The baseline is no longer being updated and no alerts or notifications will be sent.

Enabled column

The Enabled column indicates **Yes**, **No**, or **Mixed**.

- **Yes** – the policy is enabled. This means that when the status of the policy is Ready (monitoring) or Ready (baselining), you can run a Service Level Objective Report, Service Incident Report, or Service Performance Report. For metric policies (the lowest-level or base policies), it also means that the policy can generate alerts and notifications if the value of the metric is outside the normal baseline behavior by more than a specified tolerance.
- **No** – the policy is disabled. This means that the baselines for the metrics being monitored are not updated and reports are not available. For metric policies, it also means that no alerts or notifications are generated. Note that a metric policy continues to count toward your license limit when it is disabled.
- **Mixed** – the policy includes subordinate policies (e.g., a metric policy is subordinate to a metric category policy, which is subordinate to a segment policy). One or more subordinate policies is enabled and one or more is disabled.

Actions column

The actions column of each entry in the policy tree diagram provides a drop-down list of actions you can perform on the policy. The status of a policy determines which actions are available for the policy. The actions include:

- **Enable** – enables this policy and all subordinate policies. This is available for policies that have the Enabled status of **No** or **Mixed**. A message box tells you how many metric policies (the lowest level of the tree hierarchy) will be enabled if you enable this policy.

- **Disable** – disables this policy and all subordinate policies. This is available for policies that have the Enabled status of **Yes** or **Mixed**. A message box tells you how many metric policies (the lowest level of the tree hierarchy) will be disabled if you disable this policy.
- **Tune** – opens the Tune <service> Policies section of the page, in which you can modify the operation of the analytics for each metric that the policy monitors. This option is not available for the service policy, which is the highest level policy, or for the policy of the segment that includes the end users component. Additionally, this option is available to only Administrator or Operator accounts. Monitor accounts can view the policy settings, but not tune them.
- **View SLO Report** – opens a page on which you can run the Service Level Objective report for this policy. This option is not available for the service policy, which is the highest level policy, or for the policy of the segment that includes the end users component.
- **View Incident Report** – opens a page on which you can run the Service Incident Report for this policy.
- **View Performance Report** – opens a page on which you can run the Service Performance Report for this policy.

The Actions choices are inactive while a policy is being tuned. Exit the policy tuning section by clicking **OK** or **Cancel** to reactivate the Actions choices.

Tune Policies section

The Tune <service> Policies section of the page opens when you choose **Tune** from the Actions list for a policy. If you click **Tune** for the lowest level of the service hierarchy, which contains only service metric policies, then this section displays controls for tuning individual policies. If you click **Tune** for a level of the service hierarchy that could use the same analytic more than once for various elements of the service that it includes, then this section displays controls for simultaneously tuning multiple policies (bulk tuning).

Tuning an individual service policy

Use the Tune Policy page to edit the tolerance, noise floor and alerting characteristics of individual policies.

Setting tolerance

The variability tolerance is specified in sigmas (standard deviations) set by the sliders. If the value of the metric differs from the computed typical value by an amount that exceeds the setting of the lower slider, it triggers a low-level alert. If it exceeds the setting of the upper pointer, it triggers a high-level alert.

Before making any tolerance adjustments, examine the graph for the metric to see how the policy has been performing for the past week. In particular, consider how often and by how much the plot of actual traffic went beyond the tolerance range with the current tolerance settings.

Note that multiple excursions outside the tolerance range (“outliers”) might be determined to be part of the same event. Because of the number of factors analyzed in determining if a policy violation event has occurred, the number of outliers does not directly indicate how many events will be detected. However, looking at how many outliers would result from a particular tolerance setting can give you a good sense of whether that setting will produce many events or few events. In this way the graph can help you tune the tolerance settings to the characteristics that are typical for your network.

If there are no outliers, or if there are too many, adjust the tolerance sliders for the metric until more or fewer points on the plot line of actual data lie outside the green tolerance range. The graph will show you how the policy would have performed over the past week with different tolerance settings.

Decreasing the number of sigmas of tolerance reduces the width of the tolerance range and thereby results in more outliers. Having more outliers generally means having more policy violation events detected.

Figure 7-2. Service Policies page Tune Policy section

Service Policies ?

Service **Performance & Availability** User-defined Security Health

+ Configured Policies

Edit VoIP-Calls > LA-Phoenix Policy OK Cancel

Metrics being monitored

☒ Show advanced settings

MOS Status: Ready (monitoring) (details...) OK Cancel

☐ Detect spikes

☒ Detect dips

Set Tolerance (sigmas) Low 2 3 4 5 6 High

Duration intervals x 15 minutes

Noise floor

Packet Loss Status: Ready (monitoring) (details...) OK Cancel

☒ Detect spikes

☐ Detect dips

Set Tolerance (sigmas) Low 2 3 4 5 6 High

Duration intervals x 15 minutes

Noise floor packets/s

R-Factor Status: Ready (monitoring) (details...) OK Cancel

☐ Detect spikes

☒ Detect dips

Set Tolerance (sigmas) Low 2 3 4 5 6 High

Duration intervals x 15 minutes

Noise floor

Percent Packet Loss Status: Ready (monitoring) (details...) OK Cancel

☒ Detect spikes

☐ Detect dips

Set Tolerance (sigmas) Low 2 3 4 5 6 High

Duration intervals x 15 minutes

Noise floor % Loss

Alerting and Notification

You can set notifications by editing service [VoIP-Calls](#)

Enabled	Alert Level	Recipient
<input checked="" type="checkbox"/>	Low	* Log Only
<input checked="" type="checkbox"/>	High	* Log Only

OK Cancel

Duration

The presence of an outlier triggers an alert if its duration equals or exceeds the number of 15-minute intervals specified in the Duration section.

Noise floor

If the value of the metric is very regular, then the analytic adjusts to expect only a small range of changes from the typical value. Therefore, a relatively small change could trigger an alert because it is more than the expected deviation from typical behavior.

You can prevent this by specifying the minimum amount of change that is to be considered significant. This is the Noise floor. Setting a lower limit on the amount of change that can be seen as a policy violation allows the tolerance setting to accommodate both periods of high variability and periods of low variability over the course of the day or week. Select **Show advanced settings** to show the Noise floor setting.

Alerting on spikes or dips

Each service policy can alert on a spike (an INCREASE in the value of a metric from what has been baselined) or a dip (a DECREASE in the value of a metric from what has been baselined) or both. Select **Show advanced settings** to enable the options to specify whether the metric policy triggers alerts on spikes, dips or both.

Alerting and Notification

Alerting and notification settings are specified in the service definition and apply to all policies in the service. They are displayed on this page for reference and are read-only. Click the link to the service definition if it is necessary to modify these settings.

Tuning service policies as a group

Use the Tune Policies page to edit the tolerance, noise floor and alerting characteristics of all policies at or below the level of the item you selected. All changes can be undone until you click **OK**.

Setting tolerance

The tolerance of service policies to changes from baseline levels is specified in sigmas (standard deviations). There are two methods for adjusting the tolerance settings: **Explicit** and **Relative**

Both methods affect all existing policies at or beneath the level at which you are tuning. They do not affect the policies of other services or of higher-level objects in this service. Also, they do not change the global default settings. New policies added to this service continue to be given the default settings unless edited in the service definition.

Explicit tolerance settings - Tolerances can be set explicitly by sliding the Low or High pointer to the setting you want to propagate to all policies in this part of the service that are using the metric. If different policies have different settings, the pointer is positioned to the right side of the slider and labeled Set. Hover the mouse over the Set pointer to see the range of tolerance values used by the policies for the metric and the global default setting for the metric.

Click **Set** to set the tolerance to the default value. Alternatively, click the slider at the number of sigmas of tolerance you want to set for the policies. If you make changes and then decide to revert to the original settings, click Reset to undo all your changes.

Figure 7-3. Service Policies page Tune Policies section - Explicit tolerance tuning

Service Policies ⓘ

Service Performance & Availability User-defined Security Health

Configured Policies

Tune VoIP-Calls Policies

OK Cancel

Use this page to tune policies related to VoIP-Calls. There are 10 policies grouped by metric allowing tolerance parameters for all policies in the group to be explicitly set or adjusted higher or lower relative to each policy's current tolerance setting

Metrics being monitored

Select Tolerance Tuning Method: Explicit ☒ Show advanced settings

MOS (4 policies) Reset

Set Tolerance (sigmas) Low 2 3 4 5 6 High

☐ Detect spikes

☒ Detect dips

Duration 1 intervals x 15 minutes

Noise floor 0

Packet Loss (4 policies) Reset

Set Tolerance (sigmas) Low 2 3 4 5 6 High

☒ Detect spikes

☐ Detect dips

Duration 1 intervals x 15 minutes

Noise floor 0 packets/s

Relative tolerance settings - When you choose Relative in the Select Tolerance Tuning Method box, the displays change to show boxes in which you can specify a number of sigmas for Low alerts and High alerts. The relative setting applies the same amount of change to all policies, regardless of their current settings. For example, if you want to reduce the number of High alerts by increasing the tolerance settings by 1.5 sigmas, you could use the arrows to increase the High tolerance by 0.5 sigma at a time. Alternatively, you could enter 1.5. (The number you enter gets rounded to the nearest one half sigma.) This enables you to increase the tolerance of all policies to 1.5 sigmas above whatever they are set to now.

Duration

The presence of an outlier triggers an alert if its duration equals or exceeds the number of 15-minute intervals specified in the Duration section.

Noise floor

If the value of the metric is very regular, then the analytic adjusts to expect only a small range of changes from the typical value. Therefore, a relatively small change could trigger an alert because it is more than the expected deviation from typical behavior.

You can prevent this by specifying the minimum amount of change that is to be considered significant. This is the noise floor. Setting a lower limit on the amount of change that can be seen as a policy violation allows the tolerance setting to accommodate both periods of high variability and periods of low variability over the course of the day or week. Select **Show advanced settings** to show the Noise floor setting.

If different policies have different settings, the Noise floor box says **Mixed**. Entering a value sets the noise floor of all the policies to the value you enter. If you make changes and then decide to revert to the original settings, click **Reset** to undo all your changes.

Figure 7-4. Service Policies page Tune Policies section - Relative tolerance

Service Policies ⓘ

Service: Performance & Availability User-defined Security Health

+ Configured Policies

- Tune VoIP-Calls Policies

OK Cancel

Use this page to tune policies related to VoIP-Calls. There are 10 policies grouped by metric allowing tolerance parameters for all policies in the group to be explicitly set or adjusted higher or lower relative to each policy's current tolerance setting

Metrics being monitored

Select Tolerance Tuning Method: Relative ▾ ☒ Show advanced settings

- MOS (4 policies) Reset

Adjust Tolerance High	0.0 ▾	 	<input type="checkbox"/> Detect spikes
(by sigmas) Low	0.0 ▾	 	<input checked="" type="checkbox"/> Detect dips
			Duration 1 intervals x 15 minutes
			Noise floor 0

- Packet Loss (4 policies) Reset

Adjust Tolerance High	0.0 ▾	 	<input checked="" type="checkbox"/> Detect spikes
(by sigmas) Low	0.0 ▾	 	<input type="checkbox"/> Detect dips
			Duration 1 intervals x 15 minutes
			Noise floor 0 packets/s

Alerting on spikes or dips

Each service policy can alert on a spike (an INCREASE in the value of a metric from what has been baselined) or a dip (a DECREASE in the value of a metric from what has been baselined) or both. Select **Show advanced settings** to enable the options to specify whether the metric policy triggers alerts on spikes, dips or both.

If different policies have different settings, the spikes or dips selection box indicates an indeterminate state instead of a check mark. Selecting or deselecting a box selects or deselects the option for all policies. If you make changes and then decide to revert to the original settings, click **Reset** to undo all your changes.

Alerting and Notification

Alerting and notification settings are specified in the service definition and apply to all policies in the service. They are displayed on this page for reference and are read-only. Click the link to the service definition if it is necessary to modify these settings.

CHAPTER 8 Performance and Availability Policies

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for monitoring the performance and availability of your network. It includes the following sections:

- [“Overview,”](#) next
- [“Types of policies”](#) on page 173
- [“Managing policies”](#) on page 174
- [“Creating new performance and availability policies”](#) on page 177
- [“Tuning a policy”](#) on page 178

Overview

Performance and availability policies are defined on the Behavior Analysis > Policies page Performance and Availability tab.

You can define many policies of several types, depending on your license. Each policy specifies a set of traffic to which it applies, a set of metrics (bytes per second, number of clients per second, etc.) to be monitored, and a set of parameters within which operation is considered to be acceptable.

Each policy includes a specification for the level of alert (High or Low) that is to be generated if a policy violation occurs. It also specifies who is to be notified for each level of alert. The level of alert generated is based on the severity of the event.

The appliance compares current traffic with mathematically derived models of what is expected traffic for the current time of day and day of the week. Based on the differences, it detects the occurrence of network events that violate your policy.

Types of policies

The appliance provides analytics for implementing the following types of performance and availability policies:

- Application Availability
- Application Performance
- Link Congestion

- Link Outage

Managing policies

Performance and availability policies are created and managed on the Behavior Analysis > Policies page Performance and Availability tab. The tab has a Configured Policies section, which is always visible, and a section for creating, editing, and viewing policy definitions, which is visible only while you are performing one of those operations

Figure 8-1. Behavior Analysis > Policies page

Policies ?

Service Performance & Availability User-defined Security Health

Configured Policies New...

Type	Name ↑	Status	Enabled	Actions
Link Congestion	Hartford-WAN	Ready (monitoring)	Yes	Select...
Link Congestion	LosAngeles-WAN	Ready (monitoring)	Yes	Select...
Link Congestion	RTR-DataCenter:Ethernet11	Ready (monitoring)	Yes	Select...

1 2 3 go to page 1 Show: 10 entries per page

Managing configured policies

The Configured Policies section of the page lists the name, status, and actions available for each policy. You can sort the list by the type of analytic the policy uses, by the policy name, or by the policy status. Controls and indicators in the Configured Policies section include:

New button

To create a new policy, click **New** and choose the type of policy you want to create. This opens a Create New section in which you can specify what the policy applies to, the settings for the metrics to be monitored, and who is to be notified of alerts.

Status column

Each policy indicates the status of the best of any subordinate policies. For example, if a segment policy includes several metrics policies, and one of the metric policies is in the Ready (monitoring) condition, then that is the status that is shown for the segment policy.

The status of each policy is one of the following:

- **Ready (monitoring)** – The policy is in effect. Baselines are being updated, reports can be run, and the policy can detect events and send alerts and notifications.
- **Ready (baselining)** – The policy is ready, the baselines are being updated, and reports can be run. However, the policy has not been set to detect spikes or dips in metric values, so no events will be detected and no alerts or notifications will be sent.
- **Initializing Baseline** – The analytics used by the policy are still collecting data and creating a model of normal network behavior. The policy is not ready for use yet.
- **Queued** – The appliance has queued the request to create a policy, but other tasks must be completed first.

- **Analytics License Expired** – The policy uses one or more analytics for which no current license can be found.
- **Unknown** – This message is very unlikely to occur. It indicates that there is a problem that requires help from Riverbed Support.
- **Disabled** – The policy has been disabled. The baseline is no longer being updated and no alerts or notifications will be sent.

Enabled column

The Enabled column indicates **Yes** or **No**.

- **Yes** – The policy is enabled. When the status of the policy is Ready (monitoring) or Ready (baselining), you can run a Service Level Objective Report. Also, the policy can generate alerts and notifications if the value of the metric is outside the normal baseline behavior by more than a specified tolerance.
- **No** – The policy is disabled. The baselines for the metrics being monitored are not updated and reports are not available. No alerts or notifications are generated. Note that a monitored metric continues to count toward your license limit when it is disabled.

Actions column

The actions column of each entry in the policy tree diagram provides a drop-down list of actions you can perform on the policy. The status of a policy determines which actions are available for the policy. The actions include:

- **Enable** – Enables this policy and all subordinate policies. This is available for policies that have the Enabled status of **No** or **Mixed**. A message box tells you how many metric policies (the lowest level of the tree hierarchy) will be enabled if you enable this policy.
- **Disable** – Disables this policy and all subordinate policies. This is available for policies that have the Enabled status of **Yes** or **Mixed**. A message box tells you how many metric policies (the lowest level of the tree hierarchy) will be disabled if you disable this policy.
- **Tune** – Opens the **Edit Service Policy** section of the page, in which you can modify the operation of the analytics for each metric that the policy monitors. This option is not available for the service policy, which is the highest level policy, or for the policy of the segment that includes the end users component. Additionally, this option is available to only Administrator or Operator accounts. Monitor accounts can view the policy settings, but not tune them.
- **View SLO Report** – Opens a page on which you can run the Service Level Objective report for this policy.

Creating or Editing Performance and Availability policies

The Create section of the page is displayed when you click **New** in the title bar of the Configured Policies section of the page. It displays editable fields for identifying the policy and which elements of the network it is to monitor.

The Edit section of the page opens when you choose **Tune** from the Actions list for a policy. It identifies the policy and displays the analytic settings for the metrics being monitored.

In both the Create mode and the Edit mode, this section has two subsections:

- Metrics Being Monitored
- Alerting and Notification

Metrics Being Monitored

This section displays the settings of the analytics for each metric that the policy monitors. You can expand and collapse metric sections to optimize screen space.

The controls and indicators in this section are as follows:

Show advanced settings – Displays or hides the settings options. Depending on the type of policy, the options may include:

- Detect spikes
- Detect dips
- Duration
- Noise floor
- Detect when interface utilization exceeds a specified percentage

In order for the policy to generate alerts and notifications for a metric, one or more of the following options must be enabled.

- Detect spikes
- Detect dips
- Detect when interface utilization exceeds a specified percentage

This places the policy in the Ready (monitoring) state.

If none of these are selected for a particular metric, then the analytic for that metric continues to update the baseline of typical behavior, but does not detect or alert on any changes in behavior. The policy remains in the Ready (baselining) state.

Status – The status of the policy for the individual metric, as described for the Status column above.

Tolerance – Determines how much variability in the value of the metric is necessary to exceed the normal range and low alert range of behavior. The upper slider determines the amount of variability tolerated for the normal range, which is represented in green. The lower slider determines the amount of variability tolerated for the low alert range, which is represented in yellow. The variability tolerance is specified in sigmas (standard deviations). If the value of the metric differs from the computed typical value by an amount that exceeds the normal range, a low alert is generated. If it differs enough to also exceed the low alert range, then a high alert is generated.

Detect spikes – Enables the analytic to detect increases in the value of the metric that exceed the normal or low alert tolerance ranges.

Detect dips – Enables the analytic to detect decreases in the value of the metric that exceed the normal or low alert tolerance ranges.

Duration – The presence of an outlier triggers an alert if its duration equals or exceeds the number of 15-minute intervals specified in the Duration section.

Noise floor – Specifies the minimum amount of change that the policy can treat as a deviation from normal behavior. This may be necessary to avoid having too small a change produce an alert.

Graph – The river graph depicts the computed typical value of the metric as a gray line. The normal range of variability from the typical value is indicated by the green area. This area is increased or decreased by adjusting the upper Tolerance slider. The low alert range of variability from the typical value is indicated by the yellow area. This area is increased or decreased by adjusting the lower Tolerance slider.

Alerting and Notifications section

The Alerting and Notification section indicates who is to be notified of low and high alert conditions. Recipients are specified on the Behavior Analysis > Notifications page Recipients tab.

Creating new performance and availability policies

To create a new performance or availability policy,

1. Navigate to the Behavior Analysis > Policies page Performance & Availability tab.
2. Click **New** and choose the type of policy you want to create. This opens the Create New Policy section of the page.
3. Enter a **Policy Name** to be displayed in the Configured Policies list.
4. Ensure that **Enabled** is selected if you want the policy to be operational as soon as it has enough data to be initialized.
5. If the policy includes a field for limiting it to an interface (Link policies only), enter the interface. Use the Browse feature to select the interface. Alternatively, you can enter the interface manually. Refer to the online help system for syntax examples.
6. Specify the **Applications** that the policy applies to. Use the Browse feature to select the applications. Alternatively, you can enter the applications manually.
7. If you want to limit the policy to particular protocols or ports, specify them in the **Protocols or ports** field. Use the Browse feature to select the protocols or ports. Alternatively, you can enter them manually.
8. If you want to limit the policy to traffic flows that are marked for a particular level of service, specify the marking in the **DSCP Marking** field. Use the Browse feature to select the markings. Alternatively, you can enter them manually.
9. If the policy includes fields for limiting it to servers, server groups, clients, or client groups (Application policies only), specify them in the **Servers** field or **Clients** field. You can use the Browse feature to select what you want to limit the policy to.
10. If the policy includes fields for limiting it to hosts or host groups (Link policies only), specify them in the **Hosts** field. You can use the Browse feature to select what you want to limit the policy to.
11. In the **Metrics being monitored** section, you can accept the default setting or modify them. The default settings have been found to be generally useful. If you have a good understanding of the behavior of your network, you might want to tune them to your network.
12. In the **Alerting and Notification** section, select the levels of alerts that the policy should generate and specify who is to be notified of low and high alert conditions. Recipients are specified on the Behavior Analysis > Notifications page Recipients tab.
13. Click **OK** to create the policy.
14. On the Behavior Analysis > Policies page Performance & Availability tab, observe that the policy is listed in the Configured Policies list. The Status column shows the policy as **Queued** or **Initializing Baseline** until it has collected enough data to begin operating, at which time the status is listed as **Ready**.

Tuning a policy

The general procedure for tuning an Availability or Performance policy is as follows:

1. On the Behavior Analysis > Policies page, go to the Performance & Availability tab and select the policy that you want to tune. Ensure that the policy is Ready and enabled.
2. Choose **Tune** from the Actions list for the selected policy to open the editing section of the page.
3. Before making any adjustments, examine the preview graph for each metric to see how the policy has been performing for the past week. In particular, consider how often and by how much the plot of actual traffic went beyond the tolerance range with the current tolerance settings.

Note that multiple excursions outside the tolerance range (“outliers”) may be determined to be part of the same event. Because of the number of factors analyzed in determining if a policy violation event has occurred, the number of outliers does not directly indicate how many events will be detected. However, looking at how many outliers would result from a particular tolerance setting can give you a good sense of whether that setting will produce many events or few events. In this way the graph can help you tune the tolerance settings to the characteristics that are typical for your network.

4. If there are no outliers, or if there are too many, adjust the tolerance slider for the metric until more or fewer points on the plot line of actual data lie outside the tolerance range. The graph will show you how the policy would have performed over the past week with different tolerance settings. Decreasing the tolerance reduces the width of the tolerance range and thereby results in more outliers. Having more outliers generally means having more policy violation events detected.
5. If applicable, specify the duration for which the outlier must be present before it an alert is reported.
6. If desirable, specify the **Noise floor** value as necessary to avoid having too small a change produce an alert.
7. When you are satisfied with the new tolerance settings, click **OK** in the editing section. The editing section becomes a viewing section, in which you can check the results of your editing.

If you want to check the actual performance of the policy for a period of longer than a week, run a Service Level Objective Report for the time frame of interest.

If you want to change what the policy is monitoring, select the **Show advanced settings** option in the Metrics being monitored section of the page.

Application Availability policies

Application Availability policies monitor:

- Number of clients per second that meet the criteria of the policy
- Average bytes per second of traffic that meet the criteria of the policy

A decrease in either value could indicate that the application is not as available for use as it normally is. The policy can be set to alert operators to this change and to notify those responsible for the application.

You can limit a policy to specific applications, protocols, ports, DSCP markings, servers, and clients. These can be entered manually or selected from lists using browse tools. You can also adjust the sensitivity of the policy to changes in the metrics.

Figure 8-2. Behavior Analysis > Policies page Performance & Availability tab - new Application Availability policy

Create New Application Availability Policy

Name:

OK

Cancel

Description:

Enabled:

☒

Applications:

Browse...

Protocols or ports:

Browse...

DSCP Marking (QoS):

Browse...

Servers:

Browse...

Clients:

Browse...

Metrics being monitored

☒ Show advanced settings

Number of Client Hosts

Status: Unknown (details...)

☐ Detect spikes

☒ Detect dips

Set Tolerance (sigmas)

2

3

4

5

6

Low

High

Duration intervals x 15 minutes

Noise floor hosts

Bandwidth

Status: Unknown (details...)

☐ Detect spikes

☒ Detect dips

Set Tolerance (sigmas)

2

3

4

5

6

Low

High

Duration intervals x 15 minutes

Noise floor bits/s

Alerting and Notification

Select who to notify for the following types of alerts

Enabled	Alert Level	Recipient
<input checked="" type="checkbox"/>	Low	Default
<input checked="" type="checkbox"/>	High	Default

OK

Cancel

SteelCentral™ NetProfiler and NetExpress User's Guide

179

Application Performance policies

Application Performance policies monitor specified traffic for:

- Decreases in the number of new connections to the application servers
- Increases in the average response time experienced by users of applications
- Increases in the number of TCP resets
- Increases in the number of TCP retransmissions
- Increases in the number of Active Connections
- Increases or Decreases in Connection Duration
- Decreases in Average Connection Application-level Throughput

Unusual changes in any of these measurements could indicate that the application is not performing normally.

You can limit a policy to specific applications, protocols, ports, DSCP markings, servers, and clients. These can be entered manually or selected from lists using browse tools. You can also adjust the sensitivity of the policy to changes in the metrics.

Link Congestion policies

Link congestion policies monitor traffic on a specified interface for:

- Abnormal increases in inbound or outbound bandwidth consumption
- Increases in inbound or outbound traffic that exceed a specified interface utilization level

Each link congestion policy applies to one interface. The sensitivity to changes in bandwidth usage and the allowable level of interface utilization are specified separately for inbound and outbound traffic.

You can limit a policy to specific applications, protocols, ports, DSCP markings, and hosts. These can be entered manually or selected from lists using browse tools.

Figure 8-3. Behavior Analysis > Policies page Performance & Availability tab, new Application Performance policy

Create New Application Performance Policy

Name: OK Cancel

Description:

Enabled: ☒

Applications: Browse...

Protocols or ports: Browse...

DSCP Marking (QoS): Browse...

Servers: Browse...

Clients: Browse...

Metrics being monitored

☒ Show advanced settings

New Connections Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: connections/s

Active Connections Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: connections/s

Average Connection Duration Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: s

Response Time Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: ms

Number of TCP Resets Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: resets/s

TCP Retransmissions Status: Unknown (details...)

☒ Detect spikes
☐ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: bits/s

Average Application Throughput Per Connection Status: Unknown (details...)

☐ Detect spikes
☒ Detect dips

Set Tolerance (sigmas)

Duration: intervals x 15 minutes

Noise floor: bits/s per conn

Alerting and Notification

Select who to notify for the following types of alerts

Enabled	Alert Level	Recipient
<input checked="" type="checkbox"/>	Low	Default
<input checked="" type="checkbox"/>	High	Default

OK Cancel

Figure 8-4. Behavior Analysis > Policies page Performance & Availability tab, new Link Congestion policy

Create New Link Congestion Policy

Name:

OK

Cancel

Description:

Enabled:

☒

Interface:

Browse...

DSCP Marking (QoS):

Browse...

Applications:

Browse...

Protocols or ports:

Browse...

Hosts:

Browse...

Metrics being monitored

☒ Show advanced settings

Inbound Bandwidth

Status: Unknown (details...)

☒ Detect spikes

Set Tolerance (sigmas)

Low

High

Duration intervals x 15 minutes

Noise floor bits/s

☐ Detect when interface utilization exceeds % Util.

Outbound Bandwidth

Status: Unknown (details...)

☒ Detect spikes

Set Tolerance (sigmas)

Low

2

3

4

5

6

High

Duration intervals x 15 minutes

Noise floor bits/s

☐ Detect when interface utilization exceeds % Util.

Alerting and Notification

Select who to notify for the following types of alerts

Enabled	Alert Level	Recipient
<input checked="" type="checkbox"/>	Low	Default
<input checked="" type="checkbox"/>	High	Default

OK

Cancel

Link Outage policies

Link outage policies monitor traffic on a specified interface for:

- Abnormal decreases in inbound or outbound bandwidth consumption
- Decreases in inbound or outbound traffic that drop below a specified interface utilization level

Each link outage policy applies to one interface. The sensitivity to changes in bandwidth usage and the minimum level of interface utilization are specified separately for inbound and outbound traffic.

You can limit a policy to specific applications, protocols, ports, DSCP markings, and hosts. These can be entered manually or selected from lists using browse tools.

Figure 8-5. Behavior Analysis > Policies page Performance & Availability tab, new Link Outage policy

Create New Link Outage Policy

Name:

OK

Cancel

Description:

Enabled:

☒

Interface:

Browse...

DSCP Marking (QoS):

Browse...

Applications:

Browse...

Protocols or ports:

Browse...

Hosts:

Browse...

Metrics being monitored

☒ Show advanced settings

Inbound Bandwidth

Status: Unknown (details...)

☒ Detect dips

Set Tolerance (sigmas)

2

3

4

5

6

Low

High

Duration intervals x 15 minutes

Noise floor bits/s

☐ Detect when interface utilization drops below % Util.

Outbound Bandwidth

Status: Unknown (details...)

☒ Detect dips

Set Tolerance (sigmas)

2

3

4

5

6

Low

High

Duration intervals x 15 minutes

Noise floor bits/s

☐ Detect when interface utilization drops below % Util.

Alerting and Notification

Select who to notify for the following types of alerts

Enabled	Alert Level	Recipient
<input checked="" type="checkbox"/>	Low	Default
<input checked="" type="checkbox"/>	High	Default

OK

Cancel

CHAPTER 9 User-defined Policies

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for monitoring violations of network usage policies. It includes the following sections:

- [“Overview,”](#) next
- [“Alerting”](#) on page 186
- [“Pre-defined policies”](#) on page 186
- [“Defining policies”](#) on page 187

Overview

User-defined policies can be created for monitoring and alerting on changes in metrics for hosts, interfaces, and response times. The appliance provides several pre-defined policies that have been found to be useful as starting points and examples. You can modify these and create additional policies to monitor for the occurrence or absence of activity of interest.

User-defined policies differ from performance and availability policies or security policies in that they compare traffic to absolute values that you specify, whereas the other policies compare current traffic to profiles of typical traffic or to combinations of profiles and user-defined settings. Additionally, the severity of a user-defined policy event remains as you assigned it; it is not adjusted upward or downward in response to traffic conditions.

If any measurement of network behavior meets the event detection conditions of the policy, the appliance determines that the event has occurred and assigns the event a severity number from 1 to 100.

The severities of events resulting from user-defined policies are compared to user-defined alerting thresholds to determine if the events should generate alerts and send notifications. If the severity of the event exceeds the Low, Medium, or High alerting threshold, then the appliance displays an alert message.

Common uses of user-defined policies include generating alerts when:

- Connections occur within specified time periods.
- Any connection using a specified port occurs (even if only one packet).
- Traffic volume of a specific type exceeds an upper or lower limit.
- Response time exceeds a specified limit.

A user-defined policy is defined on a worksheet page available from the Behavior Analysis > Policies page User-defined tab.

This page lists all user-defined policies. It provides Actions links for viewing, editing, deleting, copying, and enabling or disabling an existing policy.

Figure 9-1. Behavior Analysis > User-defined Policies page

Policies ?

Service
Performance & Availability
User-defined
Security
Health

Configured Policies
Show alert counts for the last day

Name	Low Alerts	Medium Alerts	High Alerts	Enabled	Actions
User-defined Policy	0	0	0	Yes	Advanced settings Disable

User-defined Policy Alerting Thresholds
Tuning Help
New...

Source	Destination	Protocols or Ports	Low	Med	High	Actions
Any	Any		60	75	90	Move up Move down Edit Analyze Delete

User Defined Policies
New...

Analytic	Name	Schedule	Severity	Enabled	Actions
Host	Compliance-RegulatedAccess	Daily 12:00 AM-11:59 PM	100	Yes	View Edit Delete Copy Disable
Host	Firewall Tunneling Activity	Daily 12:00 AM-11:59 PM	50	No	View Edit Delete Copy Enable
Host	P2P Application Activity	Daily 12:00 AM-11:59 PM	100	No	View Edit Delete Copy Enable
Host	P2P Port Activity	Daily 12:00 AM-11:59 PM	75	No	View Edit Delete Copy Enable
Interface	Service Assurance	Weekdays 8:00 AM-5:59 PM	100	No	View Edit Delete Copy Enable
Host	SpamBot Activity	Daily 12:00 AM-11:59 PM	100	No	View Edit Delete Copy Enable
Host	Tunneled Application Activity	Daily 12:00 AM-11:59 PM	75	No	View Edit Delete Copy Enable
Interface	VoIP is not tagged correctly	Daily 12:00 AM-11:59 PM	100	Yes	View Edit Delete Copy Disable

1 go to page 1 Show: 50 entries per page

Alerting

The level of alert that the event generates (High, Medium, Low) is determined by the:

- Severities you specify for the alert levels in the Threshold section of the New User-defined Policy page
- Alerting thresholds you have defined on the Behavior Analysis > Policies page User-defined tab.

You can specify multiple rules so different hosts or host groups trigger different levels of alerts.

Click **New** in the User-defined Policy Alerting Threshold section to open a page on which you can define a new alerting rule.

Pre-defined policies

The appliance is shipped with the following user-defined policies included but not enabled:

- Firewall Tunneling Activity - detects tunneling activity that may pass through common firewall holes.
- P2P Application Activity - detects P2P applications.
- P2P Port Activity - detects suspicious activity involving TCP and UDP ports commonly used by P2P networks.
- Spambot Activity - detects spam activity from your email servers to the external network.
- Tunneled Application Activity - detects suspicious application tunneling.

Figure 9-2. Behavior Analysis > User-defined Policies page Alerting Thresholds section

Threshold Settings for User-defined Policy

Thresholds

Low [Disable](#)

Medium [Disable](#)

High [Disable](#)

---select to populate src/dst---

ByLocation

Source [Syntax Help](#)

☒ **Hosts**

Any

☐ **Groups**

Austin
Columbus
DataCenter
Hartford
LosAngeles

Destination [Syntax Help](#)

☒ **Hosts**

Any

☐ **Groups**

Austin
Columbus
DataCenter
Hartford
LosAngeles

You can examine the definition of each of these by going to the Behavior Analysis > Policies page User-defined tab and clicking **View** in the entry for the rule of interest.

These pre-defined policies should not be enabled until host groups have been defined. (Refer to the Definitions chapter.)

Defining policies

User-defined policies are defined on the Behavior Analysis > Policies page User-defined tab. The **New** button in the User-defined Policies section displays a worksheet page on which you can limit the conditions for detecting an event to very specific combinations of hosts, host groups, ports, protocols, applications, interfaces, interface groups, DSCP markings, and response times. You can also set the severity of the event that is detected and who is to be notified for each level of alert the event triggers.

Click **New** in the User-defined Policies section, choose **Host Policy**, **Interface Policy**, or **Response Time Policy**, and fill in the required fields.

- **Host Policy** - Choose this to define a policy about traffic between hosts or host groups. If the detection criteria are met, the appliance assigns an event ID and saves a report listing the details of traffic over connections between host or host groups.
- **Interface Policy** - Choose this to define a policy about traffic volume or utilization percent for devices, interfaces or interface groups. If the detection criteria are met, the appliance assigns an event ID and saves a report listing the details of traffic over the interface. The interface policy applies to any or all interfaces on devices that send the appliance traffic information.

Figure 9-3. Behavior Analysis > User-defined Policies > New User-defined Policy page

New User-defined Policy

Host Policy

▼ Policy Identification / Schedule

Name:

Description:

☒ Enabled

Days to run rule: ☒ Mon ☒ Tue ☒ Wed ☒ Thu
☒ Fri ☒ Sat ☒ Sun

Start time:

End time:

Select Time Zone: ?

▼ Hosts / Groups

Host/Group A:

☒ Any ☐ Within ☐ Outside

Role: [Browse...](#)

Statistics:

Host/Group B:

☒ Any ☐ Within ☐ Outside

Role: [Browse...](#)

Statistics:

▼ Applications / Ports

Applications:

☒ Any ☐ Within ☐ Outside

[Browse...](#)

Protocols/Ports:

☒ Any ☐ Within ☐ Outside

[Browse...](#)

▼ Reporting Interfaces / DSCP Marking (QoS)

Reporting Devices/Interfaces:

☒ Any ☐ Includes ☐ Excludes

[Browse...](#)

DSCP Marking:

☒ Any ☐ Tagged ☐ Not tagged

[Browse...](#)

▼ Interfaces in Network Path

Devices/Interfaces in Network Path:

☒ Any ☐ Includes ☐ Excludes

[Browse...](#)

▼ Threshold

Trigger:

Direction:

Duration: hours minutes

Severity:

Notification: Low Medium High

- **Response Time Policy** - Choose this to define a policy about overall response time, server delay, or network response time. If the detection criteria are met, the appliance assigns an event ID and saves a report listing the performance details.

CHAPTER 10 Security Policies

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for monitoring violations of network security policies. It includes the following sections:

- [“Overview,”](#) next
- [“Security event detection”](#) on page 190
- [“Security profiles”](#) on page 192
- [“Tuning alerting”](#) on page 193
- [“Alerting thresholds”](#) on page 194
- [“Tools for managing alerts”](#) on page 195
- [“Notifications of security events”](#) on page 196

Overview

When the security analytics module is enabled, the appliance detects network security events by comparing current network behavior to mathematically-derived profiles of behavior that is typical for the current time of day and day of the week. The event detection analytics are controlled by a wide variety of traffic metrics settings. These are preset to values that have proven to be most widely useful, and they do not normally require adjustments. However, you can fine-tune them to your network.

A network event that violates a security policy is dynamically assigned a severity based on the set of metrics and parameters used by the analytic that detected the event. The severity number (1 to 100) is checked against a user-definable set of alerting thresholds to determine if the appliance should generate an alert. Events that have a severity that exceeds a High, Medium, or Low alerting threshold are logged and trigger alert indications and notifications.

The appliance includes the following policies for detecting and alerting on network security events:

- **DoS/Bandwidth Surge** - Significant increase of traffic that conforms to the characteristics of a Denial of Service attack.
- **Host Scan** - Hosts on the monitored network are being pinged.
- **New Host** - A host that has not been seen before has sent enough traffic to be regarded as having joined the network.
- **New Server Port** - The appliance has discovered that a host or an Automatic host group is providing or using a service over a new port.

- **Port Scan** - Ports of a host are being tested for running services or being in a “listening” or “accepting” state.
- **Suspicious Connection** - Communication between two hosts that have been on the monitored network for some period of time, but which do not normally communicate with one another (for example, a Maintenance department host connecting to a Finance department host).
- **Worm** - Increase in connections that typically results from the spread of a worm. The appliance traces these connections over time through the network to identify how the worm spreads from infected hosts to new hosts.

Security policies can be enabled, disabled, and tuned on the Behavior Analysis > Policies page Security tab. Also, alerting thresholds for events detected by each of these policies are edited using this page.

Figure 10-1. Behavior Analysis > Policies page Security tab

Policies




Service
Performance & Availability
User-defined
Security
Health

Configured Policies
☒ Show alert counts for the last day
Security Profiles
Global Policy Settings...

Name +	Low Alerts	Medium Alerts	High Alerts	Enabled	Actions
DoS/Bandwidth Surge	0	0	0	Yes	Advanced settings Disable
Host Scan	0	0	0	Yes	Advanced settings Disable
New Host	0	0	0	Yes	Advanced settings Disable
New Server Port	0	0	0	Yes	Advanced settings Disable
Port Scan	0	0	0	Yes	Advanced settings Disable
Suspicious Connection	0	0	0	Yes	Advanced settings Disable
Worm	0	0	0	Yes	Advanced settings Disable

* Security policies are only run on those hosts which are contained within Inside Addresses.

DoS/Bandwidth Surge Alerting Thresholds
Tuning Help
New...

Source	Destination	Protocols or Ports	 Low	 Med	 High	Actions
Any	Any	Any	N/A	75	90	Move up Move down Edit Analyze Delete

Security event detection

Security policy event detection can be enabled, disabled, and tuned using options on the Behavior Analysis > Policies page Security tab as follows:

- Event detection for each policy can be enabled or disabled individually by selecting the policy and clicking the **Enable** control.
- Settings that affect all security policy and user-defined policy event detection are available by clicking the **Global Policy Settings** button.

Figure 10-2. Behavior Analysis > Policies > Security > Global Policy Settings

Global settings for all Security Policies

Event detection delay

Global Event Delay	Generate events after the Profiler has collected data for	<input type="text" value="0"/> days
New Host Delay	For a new host, don't generate any events for	<input type="text" value="0"/> days

Mitigation settings

Plan generation threshold	Create plans for events with severity equal to or higher than	<input type="text" value="None"/>
----------------------------------	---	-----------------------------------

OK Cancel

- Settings that control security and user-defined policy event detection are available (where applicable) by selecting the policy and clicking the **Advanced settings** control.

Figure 10-3. Behavior Analysis > Policies > Security > Advanced Settings

Advanced settings for DoS/Bandwidth Surge

Criteria for reporting event

Bandwidth Threshold Ratio	Ratio of inbound traffic rate, in bytes per second, to historical average, that needs to be exceeded before it is reported.	<input type="text" value="1.2"/> ratio
PPS Threshold	Minimum inbound traffic rate required for the event to be reported.	<input type="text" value="250"/> pps
Maximum Severity Surge Ratio	Ratio of inbound attack traffic rate, in bytes per second, to historical average, that will be assigned a maximum severity as configured in Maximum Severity from Bandwidth.	<input type="text" value="20"/> ratio
Maximum Severity from Bandwidth	Maximum number of severity points that are added as a result of bandwidth surge.	<input type="text" value="40"/> points

Severity increase settings

Non-TCP Traffic Adjustment	Amount by which the severity is increased when the Non-TCP Traffic Ratio is exceeded.	<input type="text" value="20"/> points
Non-TCP Traffic Ratio	The maximum percent of the event traffic that can use non-TCP protocols before the Non-TCP Traffic Adjustment is applied.	<input type="text" value="90"/> %
Max Sources Adjustment	Amount by which the severity is increased if the number of source addresses exceeds the Max Sources Threshold setting.	<input type="text" value="20"/> points
Max Sources Threshold	The maximum number of source addresses that can be detected before the Max Sources Adjustment is applied.	<input type="text" value="256"/> addresses
New Hosts Adjustment	Amount by which the severity is increased when the percent of new hosts in the event exceeds the New Host Percent setting.	<input type="text" value="20"/> points
New Hosts Percent	The maximum percent of the event traffic that can be older than the New Hosts Age Threshold before the New Hosts Adjustment is applied.	<input type="text" value="90"/> %
New Host Age Threshold	Minimum time a host must have been sending or receiving packets for it to be excluded from the New Host Adjustment.	<input type="text" value="100"/> seconds

OK

Cancel

- Settings that control the profiles against which current network behavior is compared are set on the Security Profiles page. Click the **Security Profiles** button to open this page.

Security profiles

The security analytics compare current network behavior to typical network behavior. Typical network behavior is represented by a security profile. A security profile is a mathematically-derived abstraction of the network behavior that is typical for the time periods the profile represents. Recent statistics play a larger role in the profile than older statistics, with each previous time period having a successively smaller impact on the profile. This allows the NetProfiler or NetExpress to automatically adjust to changes in network traffic patterns over time. It is responsive to new conditions, yet retains a historical perspective of traffic patterns on the network.

The appliance collects traffic data from the monitored network and aggregates it into security profiles. A profile can be created for “business hours” or “weekends” or any other time periods you want to specify.

The security profile is available to the security analytics after the appliance has collected sufficient data and a user-definable delay time has ended. The appliance compares new traffic to the corresponding profile to detect security events. The definition of a security event can be tuned to accommodate a wide variety of considerations.

Types of security profiles

There are two types of security profiles:

- Recurring profiles
- Exception profiles

Recurring profiles are developed from traffic during times that occur every week, such as Monday from 8:00 AM to 4:59 PM. Exception profiles are developed from traffic collected during times that occur less frequently than a weekly schedule, such as ends of quarters or holidays.

Both types of profiles can comprise multiple time period specifications. For example, a recurring profile named “Business hours” might be specified to include traffic from 8:00 AM to 4:59 PM every weekday. An exception profile called “Ends of Quarters” might be specified to include traffic on March 31, June 30, and so forth.

Recurring profiles are useful for tailoring your system to accommodate known peaks and lulls in weekly traffic. Exception profiles allow you to treat holidays, quarterly events, or one-time promotional event surges differently from normal traffic. Using multiple configurable profiles allows you to set security alerting thresholds more closely without significantly increasing false positives.

Changing security profiles

You can create and reconfigure profile schemes on the Security Profiles page.

The appliance is shipped with default profiles for weekdays, weeknights, and weekends. The default weekdays profile, for example, instructs the appliance to compare weekday traffic to its computed profile for weekday traffic. Operators and Administrators can create other profile schemes. For example, you could define a recurring profile for days or times of day when traffic is significantly different from other times, such as Monday mornings. You can also specify exception profiles to be used on holidays or during anticipated surges.

Traffic data that is collected during an exception time period is used with the exception profile and not with the recurring profile. Although exception profiles and recurring profiles can have overlapping time periods, only one set of data is collected. Exception profile data collection takes precedence over recurring profile data collection.

Figure 10-4. Behavior Analysis > Policies > Security > Security Profiles

Security Profiles ⓘ

Current system time: **Sunday, June 12, 2016 3:04 PM EDT (America/New_York).**

Recurring Profiles

Exception Profiles

The appliance provides tools for replacing recurring and exception profiles. These are accessed by clicking **Reconfigure Weekly Scheme** or **Reconfigure Exception Scheme** respectively. Refer to the online help system for descriptions of these tools.

Tuning alerting

For any given set of network conditions, the number of alerts that the appliance generates depends upon the:

- Alerting thresholds for the event type
- Criteria used for recognizing anomalous behavior as an event
- Severity level assigned to that event

Adjusting the alerting thresholds is the basic and simple way to control the number of alerts generated. The lower you set the alerting thresholds, the more alerts the appliance will generate. The higher the thresholds, the fewer the alerts. However, there may be circumstances in which you want to consider modifying the event detection criteria and event severity as well.

For security policies, detection criteria are predefined to be values that have been found to be generally useful. Some analytics adjust the severity assigned to the event dynamically, based on a variety of parameters that represent current conditions on the network.

You can tune the event detection analytics by selecting a policy on the Behavior Analysis > Policies page Security tab and clicking **Advanced settings**. Only Administrators and Operators with a good understanding of the appliance should modify the heuristic-based event detection functions.

Alerting thresholds


Thresholds can be set for individual hosts, address ranges of hosts, host groups, ports, and interfaces. You can tailor the thresholds based on expected behavior.

You can also define multiple alerting rules for a policy so that the occurrence of an event in one group of addresses or ports produces a higher level of alert than the same type of event in another group. For example, you may want a higher level of alert for suspicious connections to your financial servers than for suspicious connections to your desktops.

There is a default alerting threshold rule for each policy that has adjustable severity levels. The default rule specifies the severity levels that must be reached or exceeded to trigger Low, Medium and High alerts. However, you can restrict particular alerting thresholds to specified source hosts or host groups, destination hosts or host groups, or both, depending on the type of event.

Select a policy in the Configured Policies section to display the Alerting Threshold section for that policy. You can add, modify, remove and reorder alerting threshold rules using links in this section. The page also links to pages for advanced tuning of the security analytics that detect events and assign severity levels to events.

Figure 10-5. Behavior Analysis > Policies > Security > Alerting Thresholds

Policies 




Service Performance & Availability User-defined **Security** Health

Configured Policies ☒ Show alert counts for the last day Security Profiles Global Policy Settings...

Name +	Low Alerts	Medium Alerts	High Alerts	Enabled	Actions
DoS/Bandwidth Surge	0	0	0	Yes	Advanced settings Disable
Host Scan	0	0	0	Yes	Advanced settings Disable
New Host	0	0	0	Yes	Advanced settings Disable
New Server Port	0	0	0	Yes	Advanced settings Disable
Port Scan	0	0	0	Yes	Advanced settings Disable
Suspicious Connection	0	0	0	Yes	Advanced settings Disable
Worm	0	0	0	Yes	Advanced settings Disable

* Security policies are only run on those hosts which are contained within Inside Addresses.

DoS/Bandwidth Surge Alerting Thresholds Tuning Help New...

Source	Destination	Protocols or Ports	 Low	 Med	 High	Actions
Any	Any	Any	N/A	75	90	Move up Move down Edit Analyze Delete

Specifying alerting thresholds

For each policy that has an alerting threshold, you can set Low, Medium, and High alerting thresholds for:

- Individual hosts
- CIDR blocks of hosts
- Host groups

Additionally, you can set alerting thresholds that are limited to hosts that use or provide services using specific protocols or ports. Protocol- and port-based alerting thresholds are available for the following event types:

- Denial of Service/Bandwidth Surge
- Worm
- Host Scan

- Port Scan
- Suspicious Connection

For each policy that supports alerting thresholds, you can set different alerting thresholds for different hosts or host groups. For example, assume that you set the default alerting threshold for an event type to trigger a low level alert when the severity of an event of that type reaches or exceeds 60. Then you add a rule specifying that, if any traffic involved in an event of that type is in the range of 10.0.0.0/16, the appliance should send a Low level alert when the event severity reaches 40.

The result of this will be that an event with the severity of, for example, 50 will trigger a Low level alert only if traffic in the range of 10.0.0.0/16 is involved. If all traffic involved in the event is outside this range, the appliance will not send an alert until the event severity is 60.

Requirements for matching an alerting rule

The following conditions are necessary for an event severity to match an alerting rule:

- If the alerting rule specifies source hosts, then all source hosts in the event must be within the source host specification of the alerting rule.
- If the alerting rule specifies destination hosts, then all destination hosts in the event must be within the destination host specification of the alerting rule.
- If the alerting rule specifies protocols or ports, then all protocols or ports in the event must be within the specification of the alerting rule.

If sources, destinations, protocols or ports are not applicable for the type of event for which the alerting rule is specified, they are treated as “Any.”

Precedence of alerting threshold rules

When you create multiple alerting threshold rules for policy, each rule appears in the Alerting Thresholds list on the page. The appliance checks the severity of events of that event type against each rule in the list in the order in which the rules appear in the list. When it finds a rule that meets the criteria for an alert, it uses that rule and ignores all subsequent rules in the list.

You can change the location of a rule in the list by selecting it, then using the up arrow or down arrow at the right of the list to move the rule up or down in the list. Moving a rule up gives it precedence over the rules that follow it in the list. An exception to this is the default rule of Any, which always appears last in the list. If none of the other rules in the list apply, then the appliance uses the default specification.

Tools for managing alerts

The appliance features two tools for helping you manage the number of alerts:

- **Threshold Advisor** - A quick way to deal with non-critical alerts that are appearing more often than is useful.
- **Event Tuning Analyzer** - A tool for getting a better understanding of how threshold settings are impacting the number of alerts being generated.

Refer to the online help system for descriptions of these tools.

Notifications of security events

You can specify who is to be notified when a security policy event triggers an alert. Specify recipients on the Behavior Analysis > Notifications page. See [“Notifications” on page 201](#).

CHAPTER 11 Health Policies

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for alerting users to problems with hardware, software and connectivity within or between SteelCentral products.

Overview

Health policies are defined on the Behavior Analysis > Policies page Health tab. A health policy violation is considered a high severity event and always triggers a High alert.

Health policy violation events can be reported on the Reports > Events page and in Event Detail reports. If notifications are configured on the Behavior Analysis > Notifications page, alerts are sent by email or SNMP notification to specified addresses.

Alerts are listed in the Current Events display on the Dashboard and also reported in the status section of the System > Information page.

When an ongoing event occurs, information about subsequent events of the same type is merged into the same report so that an Event Detail report includes all on-going events of the event type at the current moment.

There are health policies for four types of problems:

- Data Source Problem
- Hardware Problem
- Module Problem
- Storage Problem

Figure 11-1. Behavior Analysis > Policies page Health tab

Policies ?

Service	Performance & Availability	User-defined	Security	Health
Configured Policies				
<input checked="" type="checkbox"/> Show alert counts for the last day ▼				
Name ↑	High Alerts	Enabled	Actions	
Data Source Problem	0	Yes	Advanced settings	
Hardware Problem	2	Yes	Advanced settings	
Module Problem	0	Yes	Advanced settings	
Storage Problem	0	Yes		

Data Source Problem

Data Source problems include:

- **Disconnects** - A SteelCentral product that has been communicating with the NetProfiler or NetExpress is no longer reachable.
- **Protocol Violations** - The NetProfiler or NetExpress is attempting to communicate with another SteelCentral product but is not receiving data in the expected format (for example, not time synchronized).
- **Silent Interfaces** - An interface on a SteelCentral product that has been communicating with NetProfiler or NetExpress has stopped reporting traffic for longer than the number of minutes specified on the Advanced settings page.
- **Sensor Application Matching Problems** - A Cascade Sensor that has been reporting to NetProfiler or NetExpress has a problem with its application identification feature.
- Click the **Advanced settings** link to display a page on which you can enable or disable detection of each of these conditions and specify the number of minutes after which an interface is considered silent if it is not sending traffic information to NetProfiler or NetExpress.

Figure 11-2. Behavior Analysis > Policies > Health - Data Source problem

Advanced settings for Data Source Problem

Settings

Disconnects	Report data source disconnects.	<input checked="" type="checkbox"/>
Protocol Violations	Report data source protocol violations.	<input checked="" type="checkbox"/>
Silent Interfaces	Report silent interfaces.	<input checked="" type="checkbox"/>
Interface Silence Tolerance	Consider interface silent if it has reported traffic before, but does not report traffic for this period of time.	<input type="text" value="2"/> minutes
Sensor Application Matching Problems	Report problems with Sensor application identification feature.	<input checked="" type="checkbox"/>

OK Cancel

Hardware Problem

NetProfiler and NetExpress check their hardware status every minute. Hardware problems include:

- **Fan Failure** - a fan has failed or is missing.
- **Power Failure** - a power supply has failed or is not plugged in. Alerting for this is disabled by default.
- **High Temperature** - the temperature inside the chassis is critically high (above 100 degrees C).
- **CPU Issue** - a CPU is configured incorrectly or has failed.
- **Memory Issue** - memory is configured incorrectly or has failed.

Click the **Advanced settings** link to display a page on which you can enable or disable detection of each of these conditions individually.

Fan and power failures are not reported on virtual editions of the products. For virtual editions, CPU and memory issues are reported only if the virtual hardware does not meet the minimum specifications for the virtual product model and license level.

Figure 11-3. Behavior Analysis > Policies > Health - Hardware Problem

Advanced settings for Hardware Problem

Settings

Fan Failure	Report when a fan is missing or has failed.	<input checked="" type="checkbox"/>
Power Failure	Report when a power supply has failed or is not plugged in.	<input type="checkbox"/>
High Temperature	Report when the chassis temperature is critically high.	<input checked="" type="checkbox"/>
CPU Issue	Incorrect CPU configuration or CPU failure.	<input checked="" type="checkbox"/>
Memory Issue	Incorrect memory configuration or memory failure.	<input checked="" type="checkbox"/>

OK Cancel

Module Problem

A Module Problem event is detected if, for more than five minutes, any major software component is:

- Unreachable
- Not synchronized to the NTP source
- Stopped

Click the **Advanced settings** link to display a page on which you can enable or disable detection of each of these conditions individually

Figure 11-4. Behavior Analysis > Policies > Health - Module Problem

Advanced settings for Module Problem

Settings

Process Failure	Report when a system process has shut down.	<input checked="" type="checkbox"/>
Module Failure	Report when a module is not connected.	<input checked="" type="checkbox"/>
Time Unsynchronized	Report when NTP is not synchronized to server.	<input checked="" type="checkbox"/>
System Process Crashed	Report when a system process has crashed.	<input checked="" type="checkbox"/>
Flow Limit Breached	Report when the flow limit has been breached.	<input checked="" type="checkbox"/>

OK Cancel

Storage Problem

A Storage Problem event is detected if any of the following conditions or events occur:

- Disk failed
- RAID system is rebuilding
- RAID system is degraded
- Partition is full
- Partition is unmounted
- Partition failed

- Partition is mounted as read-only

The status of the storage system is displayed on the [System > Information](#) page.

CHAPTER 12 Notifications

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for notifying users or groups of users when network behavior triggers an alert. It includes the following sections:

- [“Overview,”](#) next
- [“Adding recipients”](#) on page 202
- [“Assigning notifications to recipients”](#) on page 203

Overview

The Behavior Analysis > Notifications page offers several options for notifying management systems or operations personnel of alert conditions. An alert notification can be delivered as follows:

- HTML message in email
- PDF message in email
- SNMP v1 and v2c trap messages
- SNMP v3 trap message
- SNMP v3 inform message

Alert notifications are delivered to recipients. A recipient is defined as one or more email addresses and/or one or more trap or inform addresses that are to receive alert notifications. Defining a recipient allows you to work with multiple SNMP destinations or email addresses as a single unit.

For security policies and user-defined policies, a recipient can be designated as an owner of one or more groups of one or more group types. Each level of alert for each type of event can be logged, delivered to a specified recipient, or delivered to all recipients who have been designated as owners of the groups involved in the event.

To enable the appliance to send notifications of alert conditions, start by completing the applicable fields on the Behavior Analysis > Notifications page Recipients tab for the Default recipient. This enables the appliance to send all notifications to the Default recipient. You can rename “Default” to a recipient label of your choosing. Beyond this minimum requirement, you can:

- Specify additional recipients for notifications.

- Specify that notifications resulting from particular alert levels (High, Medium, Low) for particular types of events (DoS, Host Scan, etc.) are to be sent to specific recipients or merely logged.

Note: If your network uses security policies that discard email from unknown sources, you may need to ensure that alert notification email from the appliance uses a “from” name that is known to your security devices. You can specify the email “from” name on the Configuration > General Settings page in the Outgoing Mail Server (SMTP) Settings section.

Until you provide specific notification assignments on the Policies tab, the appliance sends all notifications to the Default recipient or to the first recipient you create. If you do not set up recipients, the appliance logs events but does not send notifications.

Figure 12-1. Behavior Analysis > Notifications page Recipients tab

Notification delivery settings ?

Recipients			
Label	Email	SNMP	Actions
Default			Edit Delete

[New...](#)

Adding recipients

To add more notification recipients, go to the Behavior Analysis > Notifications page Recipients tab and click **New**.

This displays the New Recipient page. If you anticipate wanting to send notifications to this recipient on the basis of which groups it owns, click **Assign Group Ownership** and fill in the page. Note that owner-based notification is not available for service policies or performance and availability policies.

Figure 12-2. Behavior Analysis > Notifications > New Recipient page

New Recipient

New Recipient

Recipient label: [Assign Group Ownership...](#)

Email Recipient

Addresses: [Test Now...](#)

Format: ☐ PDF ☒ HTML

SNMP Trap Recipient

Destination IP 1: Port 1: [Test Now...](#)

Destination IP 2: Port 2:

SNMP Settings

SNMP Version: ☒ v1 ☐ v2c ☐ v3

SNMP Community (read):

[OK](#) [Cancel](#)

Assigning notifications to recipients

Each type of alert notification can be sent either to a recipient or to the owners of host groups involved in the alert. You can assign delivery destinations to alert notifications on the Policies tab of the Behavior Analysis > Notifications page.

Figure 12-3. Behavior Analysis > Notifications page Policies tab

Notification delivery settings ?

Policies

Recipients

Clear selection

Set Recipient ▼

To select a cell in the table, click it.
To select an entire row or column, click the label for that row or column.

	Low	Medium	High
Service:VoIP-Calls	* Log Only	n/a	* Log Only
Service:HR-Portal	Default	n/a	Default
Service:ERP	Default	n/a	Default
Service:Exchange	Default	n/a	Default
Service:Sharepoint	Default	n/a	Default
Service:FinancePortal	* Log Only	n/a	* Log Only
DoS/Bandwidth Surge	Default	Default	Default
Worm	Default	Default	Default
Host Scan	Default	Default	Default
Port Scan	Default	Default	Default
Suspicious Connection	Default	Default	Default
New Host	Default	Default	Default
New Server Port	Default	Default	Default
Data Source Problem	Default	Default	Default
LosAngeles-WAN	* Log Only	n/a	* Log Only
RTR-DataCenter:Ethernet11	* Log Only	n/a	* Log Only
Hartford-WAN	* Log Only	n/a	* Log Only
Storage Problem	Default	Default	Default
Module Problem	Default	Default	Default
Hardware Problem	Default	Default	Default
Compliance-RegulatedAccess	* Log Only	* Log Only	* Log Only
Firewall Tunneling Activity	Default	Default	Default
P2P Application Activity	Default	Default	Default
P2P Port Activity	Default	Default	Default
Service Assurance	* Log Only	* Log Only	* Log Only
SpamBot Activity	Default	Default	Default
Tunneled Application Activity	Default	Default	Default
VoIP is not tagged correctly	* Log Only	* Log Only	* Log Only

Apply

The **Set Recipient** drop-down list contains the recipients that you have defined on the Recipients tab. Select:

- **Log Only** - to record and display the alert on the appliance, but not send an alert notification. (This menu selection is prefixed with an asterisk to distinguish it from actual recipient names.)
- **Owner** - to send all the selected notification types to all recipients who are owners of any group involved in the alert. This menu selection is prefixed with an asterisk to distinguish it from actual recipient names. Note that owner-based notification is not available for service policies or performance and availability policies.
- **<recipient name>** - to send the selected notifications to a recipient you have defined. If you have not defined any recipients, notifications will be sent to the Default recipient (if it has been specified).

CHAPTER 13 Reporting

This chapter describes SteelCentral™ NetProfiler appliance and SteelCentral™ NetExpress appliance reporting features. It includes the following sections:

- [“Overview,” next](#)
- [“Report Layouts” on page 207](#)
- [“Quick reports” on page 214](#)
- [“Shortcuts to reports” on page 216](#)
- [“Service reports” on page 219](#)
- [“Traffic reports” on page 219](#)
- [“WAN Optimization reports” on page 223](#)
- [“Top Talkers” on page 224](#)
- [“Event reports” on page 225](#)
- [“Event Details reports” on page 228](#)
- [“SteelHead QoS shaping policy reports” on page 229](#)
- [“Active Directory Users reports” on page 240](#)
- [“Saved reports” on page 241](#)
- [“General Information reports” on page 242](#)
- [“Investigation reports” on page 253](#)
- [“SDN \(Software-defined Networks\) Reports” on page 256](#)
- [“VoIP reports” on page 265](#)
- [“Audit Trail reports” on page 267](#)
- [“Analyzing packet information with Packet Analyzer” on page 268](#)
- [“Packet reporting and export with Cascade Sensor” on page 270](#)

Overview

In addition to the displays on the Dashboard page, the appliance offers the following reporting features:

- **Quick reports** - creates a report on a selected subject; available at the top of every GUI page listed in the navigation bar.
- **Shortcuts** - links to pre-defined executive summary reports, service reports, general information reports, traffic reports, WAN optimization reports, investigation reports, VoIP reports and custom reports.
- **Service reports**
 - Overall Service Performance Report - presents a high-level view of how well all monitored services are performing.
 - Service Performance Report - reports how well a service or a sub-component of a service has performed. This shows the current trends of the service and provides historical information about how the service performed over a specified time such as a week, month, quarter or year.
 - Service Incident Report - shows the performance of a service or sub-component of a service over a short duration of time. This is useful for quickly determining why a dashboard health indicator is green or red.
 - Location Performance Report - shows the health of a location, the health of services that include the location, and the health of front end segments for these services. This report provides quick indications of why a traffic indicator is green or red, when problems occurred, and for which components.
 - Location Incident Report - indicates how well a location has performed across all services over a specific time range. This report shows current trends in the location as well as performance over time. This is useful for a high-level view, such as for end-of-quarter reports.
- **Traffic reports**
 - Hosts traffic reports - traffic of hosts, subnets, or groups reported by any tracked parameter.
 - Interfaces traffic reports - traffic over interfaces of devices that are providing traffic data to the appliance.
 - Applications traffic reports - traffic from applications that the appliance recognizes.
 - Advanced traffic reports - customized combinations of host, interface and application traffic.
- **WAN Optimization reports**
 - Site reports - report LAN traffic and WAN traffic for all connections that traverse the WAN between the specified WAN site and any other site.
 - Inter-site reports - report LAN and WAN traffic for connections that traverse the WAN between two specified WAN sites.
 - Overall reports - report LAN and WAN statistics for all interfaces in the default WAN interface group.
- **Top Talkers reports** - lists and displays most active members of each category of tracked traffic.
- **Event reports** - summary of events of a specified type.
- **Event Detail reports** - details of a selected event.
- **SteelHead QoS Shaping reports** - summary and detail information about the performance of SteelHead QoS shaping policies across the network.
- **Users reports** - record of network users.
- **Saved reports** - completed reports and templates for running reports.
- **Audit reports** - reports the appliance usage.

- **Packet reports** - the Packet Analyzer can be opened from the right-click menu to report packet-level detail.

Traffic monitoring and reporting tasks are assumed to be the responsibility of those with Operator or Monitor accounts. However, users with Administrator accounts can also perform all the tasks described in this section.

Report Layouts

All reports use the same basic layout and navigation features, regardless of their contents. You can run a report immediately, run it in the background, or schedule it for later. You can create reports from templates and save reports as templates. You can modify display formats, change parameters, and re-run them. You can display them in a new window. You can print, email and export reports.

Reports begin with a Report Criteria section in which you specify the content and format of the report. When you run the report, the results are organized into sections. There is a control menu for each section, as well as one for the overall report.

A typical report is described in paragraphs that follow. Following that, there is a section describing each individual type of report.

Report Criteria

Use this section to:

- Limit the report to traffic that meets specified criteria within a specified time frame
- Select the format of the report
- Save, schedule or run the report
- Load templates that have been previously saved

The Report Criteria section provides a text box or buttons for specifying the subject of the report. It may include an Additional Criteria section for further limiting the report to more specific criteria. Most traffic reports include the option for limiting the report to a specified virtual network. If no virtual network is specified, then the physical network traffic is reported.

Additionally, the Report Criteria box includes the following other controls:

- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Report by** - Specifies the category of data by which traffic is reported. This isn't present on all reports.
- **Report Format** - Specifies the graphical presentation to be used for reporting traffic information. (Options vary slightly from tab to tab where non-applicable items are omitted.) Individual displays of the completed report can be modified.
- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Figure 13-1. Typical Report Criteria section

☐ Report Criteria (default by Port)

▸ VXLAN

Hosts, subnets or groups: [Browse...](#)

Report by: [?](#)

▾ Additional Traffic Criteria

Peer hosts, subnets or groups: [Browse...](#)

Applications used: [Browse...](#)

Protocols or ports used: [Browse...](#)

DSCP Marking (QoS): [Browse...](#)

Time frame:

☒ Starting Hour(s) ago

☐ From:

To:

Data resolution: [?](#)

▾ Report Format

☒ Overall traffic graph

☒ Separate ports served from ports consumed

☒ Time chart

☒ Pie chart

☒ Bar chart

☒ Summary table

☒ Flow list

Reports contain multiple sections, depending on the reporting criteria. Each section has controls for modifying the display or closing the individual section. Tables have options for changing columns, changing the number of rows, and exporting the data in a Comma-Separated-Value (CSV) file. Many graphs can be zoomed for a quick view of what is happening on the network.

The report has a Report Options menu that enables you to save, schedule, print, email or export the report and to change the units of measure in the report. The Report-by selection, if present in the Report Criteria section, determines which options are available from the Report Options menu. It also determines which data columns are available in the Add/Remove Columns feature of the Options menu on a report table.

Report Format

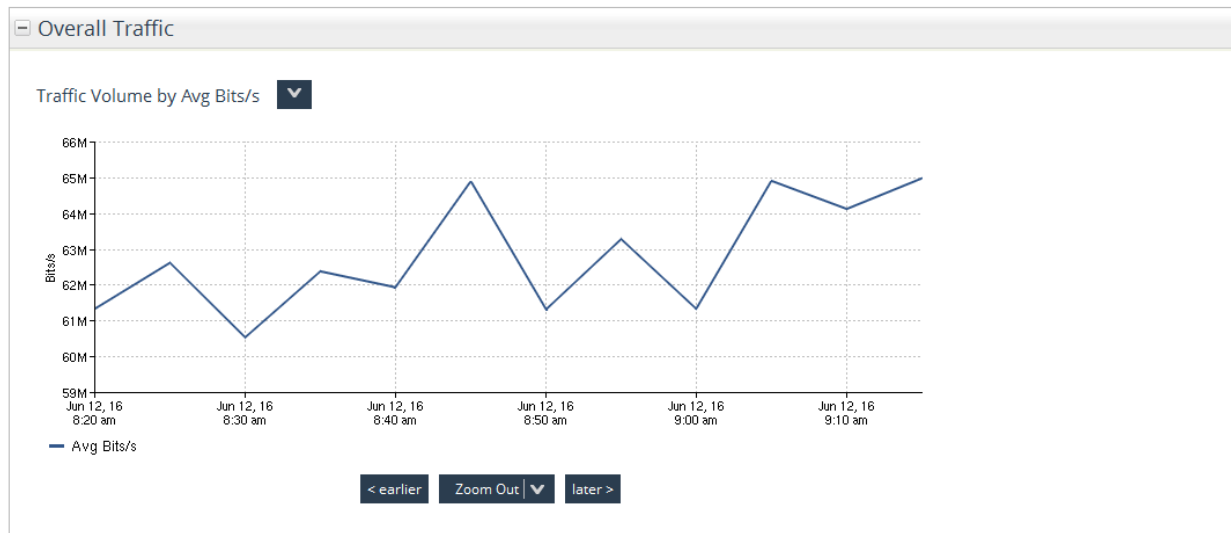
The Report Format options in the Report Criteria section offer a selection of charts and tables for displaying the results. These include:

- Graphs
- Time charts
- Pie charts
- Bar charts
- Summary tables
- Flow lists

Overall graphs

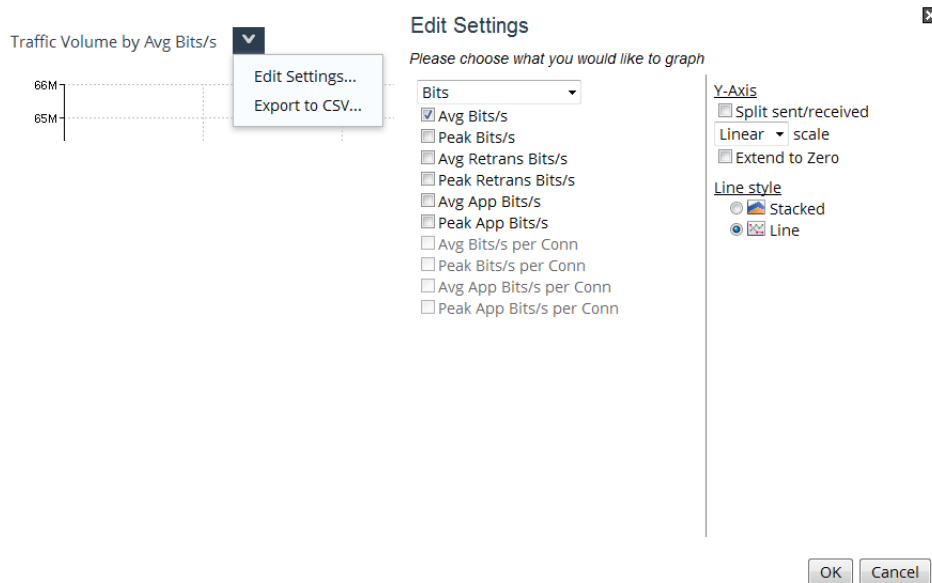
The down-arrow behind the graph title provides options for editing the format and exporting the data.

Figure 13-3. Overall graph



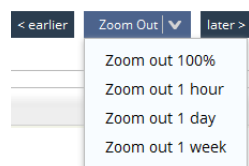
The Edit Settings page provides options for what is displayed on the graph and how the display is formatted.

Figure 13-5. Report graph format



The Zoom control at the bottom of a graph enables you to move the display forward and backward in time and zoom in and out in scale.

Figure 13-7. Report graph zoom controls



You can also use left-click-drag to select an area of the graph to zoom in on.

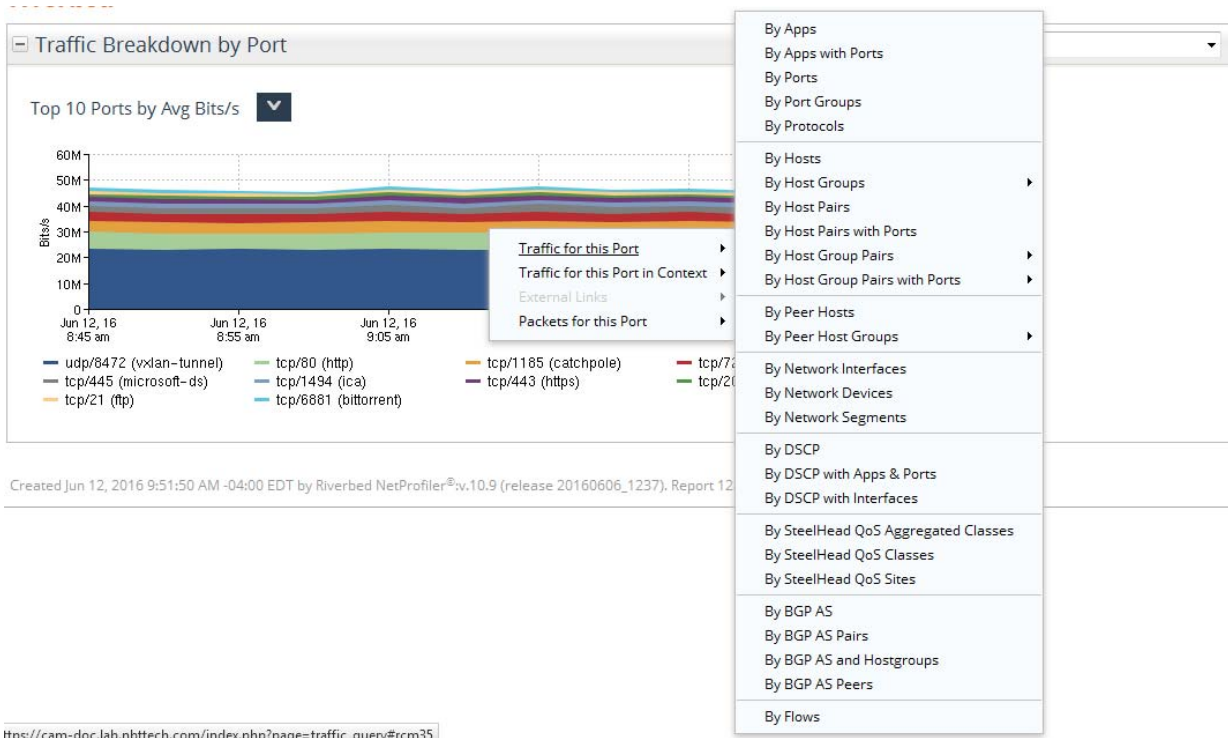
Figure 13-9. Zooming and re-running



Time charts

On a time chart, you can left-click a display to run a traffic report on a particular entity. You can right-click a display to display a shortcut menu of additional reports that are available for the item. The options on the shortcut menu are specific to the item you click.

Figure 13-11. Time chart

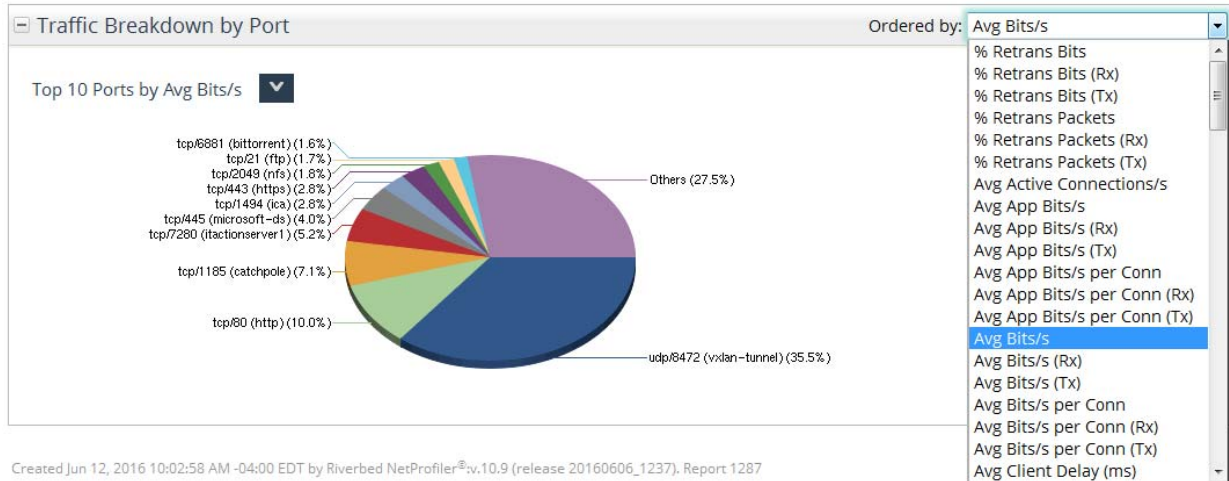


You can also use the section-level menu (the down-arrow button) to edit the format of the display and to export the time series to a comma-separated-value file for use with other programs.

Pie charts

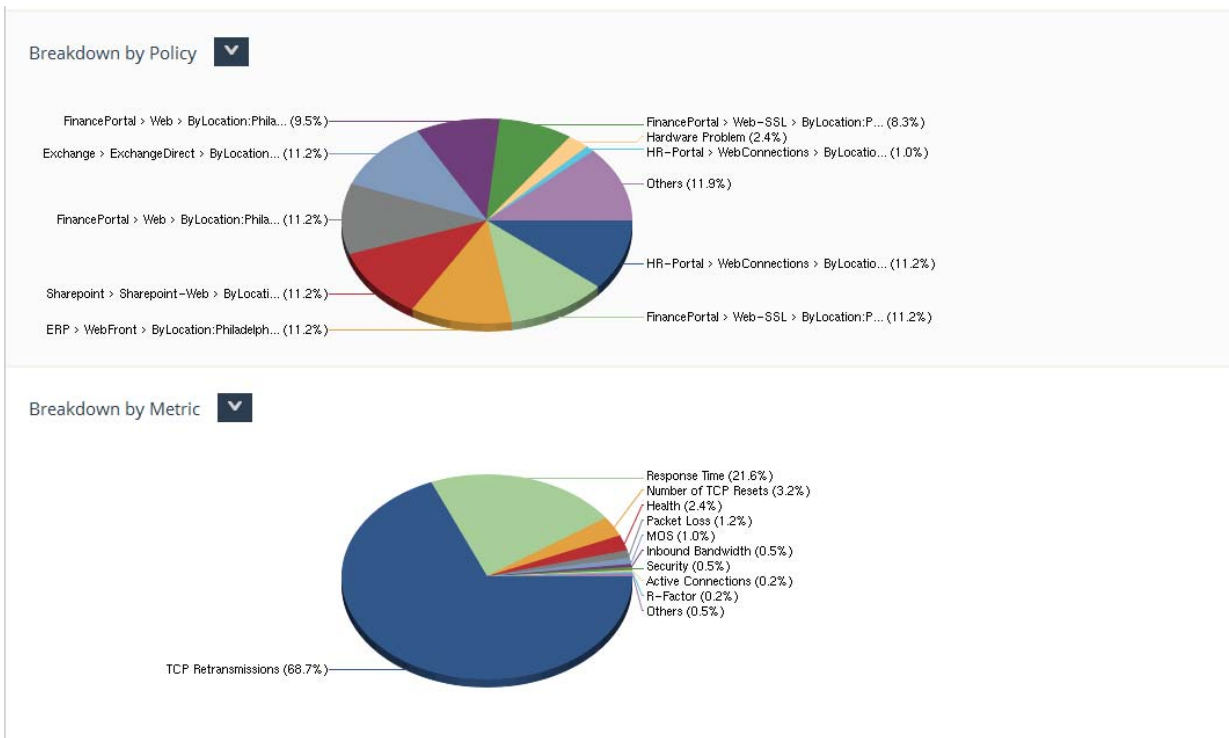
Pie charts for traffic can show the proportions of traffic as ordered by a metric selected from the “Ordered by” menu. The data can be exported as a CSV file.

Figure 13-13. Pie chart



Pie charts are also available for events that cause alert conditions.

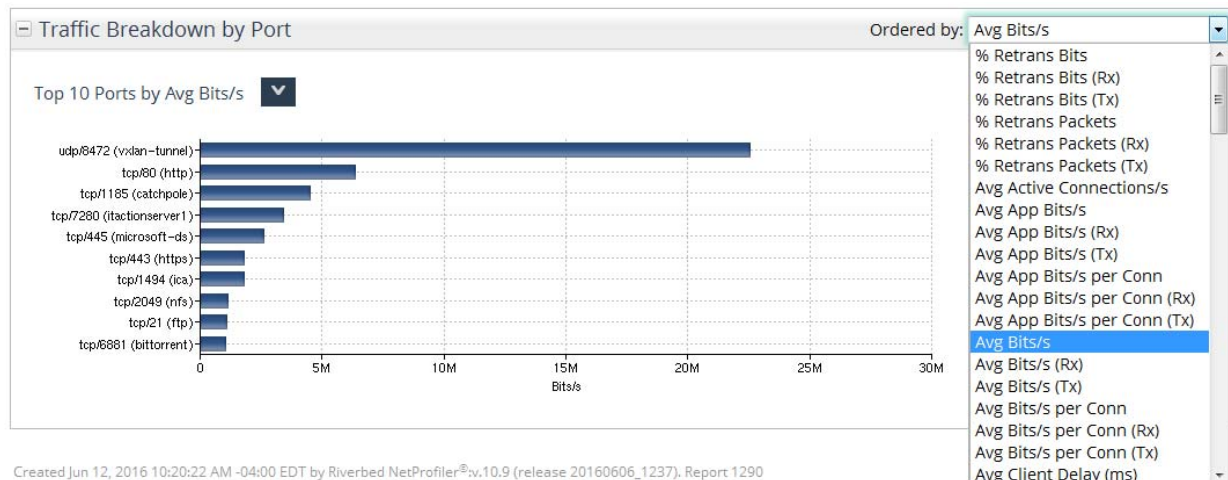
Figure 13-15. Pie chart - Events



Bar charts

Information can be presented in bar charts and ordered by a selected metric. The section-level menu provides options for editing the display settings and exporting the data.

Figure 13-17. Bar charts



Summary tables

Summary tables list values ordered by the metric selected from the “Ordered by” menu. The section-level options menu enables you to add and remove columns in the table, change the number of rows displayed on a page, filter the information for specific details, and export the data for the resulting table. Refer to the in-product help system for instructions on filtering column data.

Figure 13-19. Summary Tables

Traffic Breakdown by Port Ordered by: Avg Bits/s

Port	Count	%	Avg Packets/s	Avg Active Connections/s	Avg Net RTT (ms)	Avg Server Delay (ms)
udp/8472 (vxdm-tunnel)	3,963	(24%)	27.78	(34%)		
tcp/80 (http)	739.64	(4%)	7.26	(9%)	63	75
tcp/1185 (catchpole)	577.04	(3%)	3.84	(5%)	97	3
tcp/7280 (itactionserv1)	4,245	(26%)	4.26	(5%)	10	5
tcp/445 (microsoft-ds)	2,601,635	(4%)	310.47	(2%)	3.74	(5%)
tcp/443 (https)	1,804,310	(3%)	226.66	(1%)	3.22	(4%)
tcp/1494 (ica)	1,775,199	(3%)	679.29	(4%)	1.65	(2%)
tcp/2049 (nfs)	1,121,568	(2%)	131.94	(< 1%)	1.12	(1%)
tcp/21 (ftp)	1,112,909	(2%)	126.55	(< 1%)	< 1	(< 1%)
tcp/6881 (bittorrent)	1,052,842	(2%)	123.43	(1%)	1.21	(1%)
Others	17,289,303	(27%)	5,474	(33%)	26.03	(32%)
Total	63,579,541	(100%)	16,597	(100%)	80.87	(100%)

1 2 3 4 5 ... go to page 1

Flow lists

Flow lists display statistics for each traffic flow seen on the monitored network during the time frame of the report. A large number of metrics are available for being added to the table.

Flow lists can be filtered and their filtered contents used for defining host groups.

Figure 13-21. Flow List

Flow List

Flows 1 - 20 of 10000

Row	Start Time	End Time	Duration	Protocol	Client	Client Port	Server	Server Port	Total Bits (cli -> srv)
1	Jun 12, 2016 9:32:46			tcp	Desktop18-154	38045	65.99.105.102	6881	134,176
2	Jun 12, 2016 9:32:46			tcp	Desktop13-116	14735	CitrixServer-91	1494	18,600
3	Jun 12, 2016 9:32:46 AM	Jun 12, 2016 9:33:01 AM	15 seconds	tcp	Desktop18-172	16262	ExchangeServer-23	1185	2,632

Context menu options:

- Add/Remove Columns...
- Change Number of Rows...
- Show Filter
- Show All Topology
- Export to Host Group...
- Export to CSV...

Refer to the in-product help system for information about using the column chooser to add metrics to the table.

Figure 13-23. Column Chooser

Chooser

Search in column names:

Application	Avg Client Delay (ms)
Client IP	Avg Jitter (ms) (cli -> srv)
Client MAC	Avg Jitter (ms) (srv -> cli)
Client Switch Info	Avg MOS (cli -> srv)
Client Switch IP Info	Avg MOS (srv -> cli)
Server IP	Avg Net RTT (ms)
Server MAC	Avg R-Factor (cli -> srv)
Server Switch Info	Avg R-Factor (srv -> cli)
Server Switch IP Info	Avg Req Network Time (ms)
Virtual Network Tunnel	Avg Req Retrans Time (ms)
	Avg Resp Network Time (ms)
	Avg Resp Retrans Time (ms)

OK Cancel

Refer to the in-product help system for information about filtering metrics in the table.

Figure 13-25. Flow List filtering

Topology (cli -> srv)	Total Bits (srv -> cli)	Total Packets (srv -> cli)	Flags (srv -> cli)
shark-Hartford :mon0 [Default] WAN-RTR-Hartford:(lan [Default] → wan [Default])	145,544	9	FPA
AOL-ATDN:SH-Phoenix :lan0_0 [Default] → wan0_0 [Default:Realtime] shark-Phoenix :mon0 [Default] shark-DataCenter :mon0 [Default] SH-DataCenter :(wan0_0 [Default] → lan0_0 [Default]) AOL-ATDN:RTR-DataCenter:(vlan400 [Default] → vlan100 [Default])	152,296	69	FPA

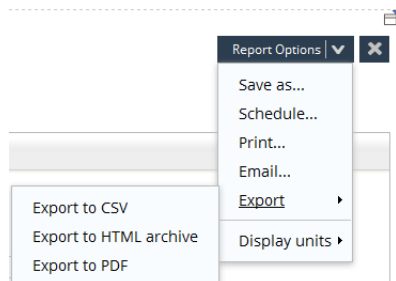
Filter dropdown options:

- >
- Empty
- Not Empty
- =
- Not=
- >
- <
- Range

Report menu

In addition to the menu for each section of the report, there is a menu for handling the entire report. It is located in the upper-right corner of the report. The report options are described later in this chapter.

Figure 13-27. Report options



There is also a small icon in the far upper-right corner of the report page that places the report on a separate page.

Figure 13-29. New page icon



The content options and display formats vary slightly by report types. Not all options are available on all report types. The sections that follow describe the information and formatting that are available for each type of report.

Quick reports

Each top-level GUI page includes two Quick report boxes for generating reports on specific entities.

Figure 13-31. Quick Report box



1. In the first of the two Quick report boxes, select the category of the item you want to query on from the drop-down list box.
2. In the second box, specify the item as listed in the table that follows.
3. Click **Go** to generate a report.

Category	Value
Host/Group	<p>Specify a host or a host group. Specify a host to generate a Host Information Report. Specify a host group to generate a Host Group Information report.</p> <p>Host - Specify a host by host name, IP address, MAC address, or an address range in CIDR format.</p> <p>Host Group - Specify a host group by name and group type, as defined on the Definitions > Host Groups page, separated by a colon, in the following format: group_name:group_type</p> <p>For example, email:application_servers</p>
User	Specify the user name under which the user is logged in.

Category	Value
Port	<p>Specify a port as:</p> <ul style="list-style-type: none"> • port number (e.g., 23) • protocol/port number combination (e.g., tcp/80) • protocol/port number range (e.g., tcp/1-100) • port name (e.g., smtp)
Application	Specify a built-in or custom application definition by application name. Enter this as it is listed on either tab of the Definitions > Applications page.
Protocol	<p>Specify a protocol either by name or by number. Refer to http://www.iana.org/assignments/service-names for protocol names.</p> <p>Refer to http://www.iana.org/assignments/protocol-numbers for protocol numbers.</p>
Interface/Device/ Group	<p>Specify an interface or interface group.</p> <p>Interface - Specify an interface by the host name or IP address of the network device being used as a data source, followed by a colon and an interface identifier in any of the following formats:</p> <ul style="list-style-type: none"> • <i>interface_device:interface_name</i> • <i>interface_device:interface_index</i> • <i>interface_device:interface_label</i> <p>For example, 10.0.0.1:1</p> <p>These values can be found by going to the System > Devices/Interfaces page and choosing the Device List view.</p> <p>Interface Group - Specify an interface group name as it is defined on the Definitions > Interface Groups page.</p> <p>Alternatively, specify the host name or IP address of a network device being used as a data source and click Go to generate a traffic report for that device.</p>
DSCP	Specify the decimal value, binary value, or name of a DSCP marking, as it is identified on the Definitions > DSCP page. This field is case sensitive.
Template	Specify a template for generating a report by entering its name. The field will auto-complete the template name. The template can be a built-in template or a custom template.
SH QoS Summary	Specify the name of a SteelHead appliance that is sending QoS configuration data to the NetProfiler or NetExpress appliance.
Switch	Specify the name or IP address of a switch that has been identified on the Configuration > Integration > Switch Port Discovery page.
BGP AS	Specify the BGP Autonomous System name or number.
VNI/VNI + Host	<p>VNI - Enter either the actual VNI or the name for the VNI, which is defined on the Definitions > Interface Groups page.</p> <p>VNI + Host - Specify a host by host name, IP address, MAC address, or an address range in CIDR format.</p> <p>Use a space to separate the VNI and the host: <VNI or VNI name> <space> <host name or address></p>
VTEP	Specify the host name or IP address of a network device that is hosting a VTEP (virtual tunnel endpoint).

Shortcuts to reports

The shortcuts listed on the Reports > Shortcuts page are links to predefined report templates. The templates have been predefined as far as practical and named in terms of common tasks to simplify running a report to answer a question about your network.

There are shortcuts to two types of reports:

- **Built-in** - Summaries of network activity. For Executive Summary reports, you choose a time frame (last day, week, month, year) for which you want to see a summary of network-wide traffic or security activity. For General Information reports, you enter identify the item to be reported on and a time frame for which you want to see summary data. For a software-defined network report, you choose or enter a VNI or VTEP. For WAN Optimization reports, you choose or enter a time frame for which you want to see how WAN optimization is benefiting or can benefit the network. For Investigation reports, you enter the time frame and attributes of interest. For SteelHead QoS shaping reports, you enter the SteelHead or SteelHead shaping policy.
- **Custom** - Reports that support investigating the traffic volumes, dependencies, or performance of specified hosts, groups of hosts, interfaces, or applications. Network elements can be specified using the same conventions as used with the Quick Reports tool or the Reports > Traffic pages. A variety of sample custom reports are predefined.

To run a shortcut,

1. Click the shortcut link. This opens the applicable report page.
2. Enter the information and time frame that are to be the subject of the report. (Executive Summary reports require only a time frame.)
3. At the bottom of the Report Criteria section, click **Run now**.

Built-in reports

The Executive Summary reports are network-wide in scope. They report traffic information or security information for the entire monitored network for the specified time frame.

The Executive Network Summary report requires the ByLocation host group to have been defined. Define this group on the Definitions > Host Groups page before running the Executive Network Summary report.

Service reports require at least one service to have been defined.

The General Information reports are designed for network administrators and other operations personnel. In addition to being accessible on the Reports > Shortcuts page, they can be accessed from the right-click menu on other pages. Position the cursor over an underlined host, host group, interface or application anywhere in the appliance GUI and right-click it to access one of these reports.

The WAN Optimization reports provide views into which applications are using the WAN, which sites (WAN interfaces) are the most active, and where there are potential response time or congestion problems.

The WAN Optimization reports require the WAN to have been defined. Define your WAN on the Definitions > WAN page before running the WAN Optimization reports.

Figure 13-33. Reports > Report Shortcuts page - Built-in reports tab

Report Shortcuts ?

Built-in Custom

- Executive Summary Reports
 - Executive Network Summary Day, Week, Month, Year
 - Executive Event Summary Day, Week, Month, Year
 - Executive DSCP Summary Day, Week, Month, Year
- General Information Reports
 - Application Information
 - Interface Information
 - Interface Capacity Planning
 - Device Information
 - Interface Group Information
 - Host Information
 - Host Group Information
 - Server Information
 - Switch Information
 - Network Segment Information
 - DSCP Information
 - BGP AS Information
- Investigation Reports
 - Audit Trail
 - Event
 - Active Directory User
 - Service Level Objective
 - Performance Investigation
 - 95th percentile
- SDN Reports
 - VXLAN Summary Day, Week, Month, Year
 - Virtual Network Information
 - Tunnel Endpoint Information
- Service Reports
 - Overall Service Performance
 - Service Performance
 - Service Incident
 - Location Performance
 - Location Incident
- Steelhead QoS Shaping Reports
 - Steelhead QoS Summary
 - Steelhead QoS Shaping
- Traffic Reports
 - Host
 - Interface
 - Application
 - Advanced
 - Top Talkers
- VoIP Reports
 - VoIP Performance Day, Week, Month, Year
 - VoIP Dependencies - Signaling Host, Site
 - VoIP Dependencies - Calls Host, Site
- WAN Optimization Reports
 - Overall WAN Analysis Day, Week, Month, Year
 - Optimization Benefit Analysis Day, Week, Month, Year
 - Optimization Candidate Analysis Day, Week, Month, Year
 - Site Capacity Analysis
 - WAN Site Optimization
 - WAN Intersite Optimization

Custom reports

The Type column identifies the tab of the traffic report page or WAN optimization report page to which the template applies. For example, Advanced means that the shortcut opens a pre-configured report on the Reports > Traffic page Advanced tab. WAN Site Optimization means that the shortcut opens a pre-configured report on the WAN Optimization page Site tab.

The Top Internet Applications report and Top Internet Destinations report require the ByInternalHosts host group to have been defined. The Application Performance Assessment report requires the ByLocation host group to have been defined. Define these groups on the Definitions > Host Groups page before running the reports.

You can modify the report specifications, save your modifications as a new template, schedule the running of the template, save the reports, and have them emailed.

Figure 13-34. Reports > Reports Shortcuts page - Custom tab

Report Shortcuts ?

Built-in Custom

Custom Reports (32) Refresh

Type ↑	Template name
Advanced	Top Internet Applications
Advanced	Top Internet Destinations
Advanced	d3-network segments w connection graph
Advanced	d5-server dependency mapping - AppServer-1 server
Advanced	d6-flow list - tcp for previous 5 min
Advanced	e1-three-tier-app performance
Advanced	e5-IPv6 VoIP host pair port report with DSCP list
Advanced	e6-IPv6 host pair report
Application	Application Dependency Graph
Application	Application Performance Assessment
Application	Email Dependency Graph
Application	VoIP Dependencies/Host (Calls)
Application	VoIP Dependencies/Host (Signaling)
Application	VoIP Dependencies/Site (Calls)
Application	VoIP Dependencies/Site (Signaling)
Application	d4-application dependency mapping - msexchange application
BGP AS Information	d9-BGP AS Info report for AS 1668 (AOL Transit Data Network)
Event	d7-analytic events
Host	Group/Subnet Inventory
Host	Host Dependency Graph
Host	Host Response Time Assessment
Interface	95th percentile
Interface	d1-interface reporting by utilization
Interface	d8-interface report with Shark SRT ports
Interface Capacity Planning	e3-WAN Interface Capacity Planing Report
VoIP Performance	e4-IPv6 VoIP Performance report with DSCP list
WAN Intersite Optimization	WAN Intersite Best Optimized Applications
WAN Intersite Optimization	WAN Intersite Best Optimized Hosts
WAN Site Optimization	WAN Site Best Optimized Applications
WAN Site Optimization	WAN Site Best Optimized Hosts
WAN Site Optimization	d2-wan optimization reporting by application - remote sites - 3days
WAN Site Optimization	e2-wan optimization reporting by application - remote sites - 3days

⏪ ⏩ 1 ⏪ ⏩ go to page Show: 50 entries per page

Service reports

Service reports are run from the Services > Reports menu or the right-click menu. They are described in [Chapter 3, “Monitoring Services.”](#)

Traffic reports

The Reports > Traffic page has four tabs for specifying reports:

- **Hosts** - Reports run from the Hosts tab provide data relative to hosts, subnets, and host groups. They report what is being served or consumed, or what is being transmitted or received.
- **Interfaces** - Reports run from the Interfaces tab provide data relative to devices (switches or routers), interfaces, or interface groups. They report traffic volumes or rates coming into or going out of a particular interface.
- **Applications** - Reports application traffic on networks monitored by one or more Sensor or NetShark appliances.
- **Advanced** - Reports traffic for any combination of hosts, interfaces, applications, ports, protocols, DSCP markings and BGP Autonomous Systems.

Each of these tabs has a Report Criteria section and a Traffic Report section.

Figure 13-35. Reports > Traffic page - Report Criteria section

Traffic ⓘ

Hosts Interfaces Applications Advanced

Report Criteria

Templates ▾

▸ VXLAN

Hosts, subnets or groups: Browse...

Report by: Ports ⓘ

▸ Additional Traffic Criteria

▸ Report Format

Time frame:

☒ Starting 1 Hour(s) ago ▾

☐ From: Jun 12, 2016 10:53 AM

To: Jun 12, 2016 11:53 AM

Data resolution: automatic ⓘ

Run now Run in background...

Report Criteria section

Use this section to:

- Limit the report to traffic that meets specified criteria within a specified time frame
- Select the format of the report
- Save, schedule or run the report
- Load templates that have been previously saved

The Report Criteria section provides a box for selecting the subject of the report. It includes an Additional Traffic Criteria section (except for the Advanced tab) for further limiting the report to more specific criteria. Most traffic reports include the option for limiting the report to a specified virtual network. If no virtual network is specified, then the physical network traffic is reported.

Additionally, the Report Criteria box includes the following other controls:

- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Report by** - Specifies the category of data by which traffic is reported. (See description below.)
- **Report Format** - Specifies the graphical presentation to be used for reporting traffic information. (Options vary slightly from tab to tab where non-applicable items are omitted.) Individual displays of the completed report can be modified.
- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Traffic reports contain multiple sections, depending on the reporting criteria. Each section has controls for modifying the display or closing the individual section. Tables have options for changing columns, changing the number of rows, and exporting the data in a Comma-Separated-Value (CSV) file. The Overall Traffic graph can be zoomed for a quick view of what is happening on the network.

The traffic report has a Report Options menu that enables you to save, schedule, print, email or export the report and to change the units of measure in the report. The Report-by selection in the Report Criteria section determines which options are available from the Report Options menu. It also determines which data columns are available in the Add/Remove Columns feature of the Options menu on a report table.

“Report by” options

The Report by option organizes the report in terms of the information you are most interested in seeing, such as:

- Applications
- Hosts (IP addresses or resolvable DNS names of all devices accessible on the network)
- Peers (what specified machines are connecting to)
- Network interfaces and the network segments between them
- BGP Autonomous Systems and the segments between them
- DSCP markings
- SteelHead QoS sites and classes

When you select a category in the “Report by” list, the report criteria and display format automatically change to the settings of the default template for the selection. Also, the Templates menu lists any other templates that are available for that Report by selection.

When you specify a host traffic report with the “Report by” option set to any of the following values, it causes the Report Format section to include a “Separate <reported_entity> served from < reported_entity > consumed” option.

- Applications
- Applications with Ports
- Ports
- Protocols

Both the “served” and “consumed” applications, ports or protocols are reported in reference to the host that is acting in the server role in a client-server connection. For example, if you set the “Report by” option to Ports, then:

- For hosts that were acting in the role of a server, the “Ports Served” table lists the server ports they used for serving application data to hosts that were acting in the role of a client.
- For hosts that were acting in the role of a client, the “Ports Consumed” table lists the ports they accessed on hosts that were acting in the role of a server.

Applications

To view traffic volumes and performance metrics for applications across your network, choose one of the following Report by options:

- Applications - Which applications are consuming the most bandwidth.
- Application with Ports - Which server ports are in use by which applications.
- Ports - Which server ports are carrying the most traffic.
- Protocols - Which protocols are in use and how much traffic volume they account for.

Hosts

To view traffic volumes and performance metrics for hosts on your network, choose one of the following Report by options:

- Hosts - Which hosts are consuming the most bandwidth.
- Host Groups - Which host groups are consuming the most bandwidth.
- Host Pairs - Which hosts are providing services and which are consuming those services.
- Host Pairs with Ports - Which ports are being used for connections between servers and clients.
- Host Group Pairs - Which host groups are providing services and which are consuming those services.
- Host Group Pairs with Ports - Which ports are being used for connections between host groups.

Peers

To view traffic volumes and performance metrics for hosts that connect to hosts whose addresses you specify, choose one of the following Report by options:

- Peer Hosts - Which hosts are the specified hosts connecting to, whether they are clients or servers, and how much bandwidth is being consumed by the connections.
- Peer Host Groups - Which hosts are the specified hosts or host groups connecting to, whether they are client groups or server groups, and how much bandwidth is being consumed by the connections.

Network Interfaces and Network Segments

To view traffic volumes for network interfaces and the network segments between them, choose one of the following Report by options:

- Network Interfaces - Which interfaces have the highest traffic volume and the highest or lowest percent of utilization.
- Network Devices - Which network devices (which may have one or more interfaces) have the highest traffic volume and the highest or lowest percent of utilization.

- Network Segments - Which network segment has the highest traffic volume and how it compares with other network segments.

BGP Autonomous Systems

To view traffic volumes organized by BGP Autonomous Systems, choose one of the following Report by options:

- BGP AS - Traffic volumes by Autonomous System.
- BGP AS Pairs - traffic volumes between two specified Autonomous Systems.
- BGP AS Peers - organized by Autonomous Systems that are peers with the Autonomous Systems that are carrying the highest traffic volumes.
- BGP AS and Host Groups - traffic volumes listed by the top Autonomous Systems and the top host groups.

DSCP markings

To view information about the usage of DSCP markings in your network, choose one of the following Report by options:

- DSCP - Which DSCP markings are in use; how much traffic is being tagged for each.
- DSCP with Applications and Ports - Which DSCP markings are your applications receiving; which applications are being tagged with more than one DSCP markings; how are they performing; which ports are associated with particular DSCP markings.
- DSCP with Interfaces - Which DSCP markings are in use on which interfaces; how much traffic is the interface carrying for each DSCP marking.

SteelHead QoS Shaping configuration

- SteelHead Aggregated Classes - Each aggregated class represents the aggregation of all traffic in that class for all sites defined on the SteelHead.
- SteelHead Classes - As defined on the SteelHead.
- SteelHead Sites - As defined on the SteelHead.

The item you choose is displayed as the first column of the summary table in the report. You can change or rearrange the columns on the summary table by using the Column Chooser tool.

Traffic report section

Traffic reports contain multiple sections. The contents of a report depend on the tab from which it was run, and the Report by and Report Format settings in the Report Criteria section. The report has a Report Options menu at the top for options that act on the entire report, such as saving, scheduling, printing, exporting, emailing, exporting or changing display units.

There are also controls in each section of each report, which apply to only the individual section. These provide options for editing graphing options, changing table columns, changing the number of rows in a table, and exporting data from tables and charts into a Comma-Separated-Value (CSV) files.

Refer to the online help system for detailed descriptions of the formatting requirements for entering report criteria.

WAN Optimization reports

The WAN Optimization page displays traffic volume data for WANs and LANs so that you can see the effects of the current WAN optimization and identify opportunities for further WAN optimization. Your WAN must be defined on the Definitions > WAN page before you can run the WAN Optimization reports.

The Reports > WAN Optimization page has three tabs for specifying reports:

- **Site** - Reports run from the Site tab provide data relative to a specified site on the WAN. They report LAN traffic and WAN traffic for all connections that traverse the WAN between the specified site and any other site.
- **Intersite** - Reports run from the Intersite tab display LAN and WAN traffic for connections that traverse the WAN between two specified WAN sites.
- **Overall** - Reports run from the Overall tab provide LAN and WAN statistics for all interfaces in the WAN interface group that has the default name WAN-All. If you have created additional WAN interface groups on the Definitions > Interface Groups page, then you can select one of them as the subject of the Overall report in the Additional Traffic Criteria section.

Each of these tabs has a Report Criteria section and a Report section. The text fields and lookup tools for limiting the report to specific applications, protocols, ports, hosts, subnets, and host groups have the same labels and functions as for the traffic reports described in the previous section. Refer to the online help system for detailed descriptions of the formatting requirements for entering report criteria.

Site reports

Site reports provide data relative to a specified site on the WAN. They report LAN traffic and WAN traffic for all connections that traverse the WAN between the specified site and any other site.

The Reports > WAN Optimization page Site tab includes a Report Criteria section for specifying traffic criteria for the report and a Report section, which displays the report after it is run.

The criteria in the Site box limit the report to traffic that is associated with a list of WAN interfaces, WAN interface groups, or devices that have at least one WAN interface in a WAN interface group. You can specify these either by browsing a list or by entering them manually.

Intersite reports

Intersite reports display LAN and WAN traffic for connections that traverse the WAN between two specified WAN sites.

The Reports > WAN Optimization page Intersite tab includes a Report Criteria section for specifying traffic criteria for the report and a Report section for displaying the report.

The labels and controls for the Intersite report are the same as those for the Site report except that there are two specifications for WAN sites:

- **Primary Site** - The criteria in the Primary Site box limit the inter-site report to traffic for which one end of the connection is associated with the specified primary WAN site. Traffic is always reported relative to the primary site.

You can specify the primary site either by browsing a list or by manually entering a list of WAN interfaces, WAN interface groups, or devices that have at least one WAN interface in a WAN interface group.

- **Secondary Site** - The criteria in the Secondary Site box limit the inter-site report to traffic for which the other (non-Primary) end of the connection is associated with the specified secondary WAN site.

You can specify the secondary site either by browsing a list or by manually entering a list of WAN interfaces, WAN interface groups, or devices that have at least one WAN interface in a WAN interface group.

Overall reports

Overall reports provide LAN and WAN statistics for all interfaces in the WAN interface group that has the default name WAN. The Reports > WAN Optimization page Overall tab includes a Report Criteria section for specifying traffic criteria for the report and a Report section for displaying the report.

The labels and functions of the Report Criteria section are the same as for the Site report except that you do not need to provide a WAN site specification. By default, the report includes all WAN interfaces that are members of the WAN group indicated in the WAN Group box, except as limited by the other criteria of the report.

If you have created additional WAN interface groups on the Definitions > Interface Groups page, then you can select one of them as the subject of the Overall report by selecting the desired WAN interface group in the Additional Traffic Criteria section. The report will use the group you select instead of the default group.

Top Talkers

The Top Talkers page displays traffic volume data for the most active:

- Hosts
- Host Pairs
- Host Pairs with Ports (can be broken out into MAC-IP assignments)
- Host Groups
- Host Group Pairs
- Host Group Pairs with Ports
- Applications
- Application with Ports
- Ports
- Protocols
- Network Interfaces
- Network Devices

The Reports > Top Talkers page has a Report Criteria section and a Traffic Report section.

Report Criteria section

In the Report Criteria section, you can select the category of traffic to be reported. When reporting on host groups, use the drop-down list box to choose the group type to be included in the report.

In addition to the traffic category selection, the Report Criteria section includes:

- **Templates** - a menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template. You can also load an existing template for the selected reporting category, if one has been saved.

- **Time frame** - the length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Group type** - the host group type, as defined on the Definitions > Hosts Groups pages, that is to be included in the report.
- **Run now** - runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Traffic Report section

When the report is completed and displayed, you can use the Report Options menu to:

- Save the report on the Reports > Saved Reports page.
- Print the report to a printer or file.
- Email the report.
- Export the data in a Comma-Separated-Value (CSV) file, HTML archive file, or PDF file.
- Display a different unit of measure for traffic volume.
- Choose a different Group Type by which to display the report.

You can use Options menu on the table to:

- Change the columns included in the report and change their order.
- Change the number of rows in the report.

Event reports

Use the Reports > Events page to generate Event Reports. The Event Report displays graphs and a list of events that have triggered alerts. You can limit the displays to events detected by specific policies or analytics and to events associated with specific hosts, protocols, ports, or interfaces.

Each item in the event list provides an Event ID and basic information about the event. The Event ID links to an Event Detail page that provides detailed information about the event. You can specify the time span of the report and how many events are displayed on one page.

The report includes a Report Criteria section for specifying what is to be reported and an Event Report section for displaying the graphs and event list.

Report Criteria section

In the Report Criteria section, Operators, Administrators and Monitors can specify the events to be listed in the report by specifying either the event properties or the event IDs.

Search by Properties

In the Triggering policies section, expand and navigate as necessary to select policies from the Service, Performance & Availability, User-defined, Security or Health categories, as necessary. (The Security category of events is not available if the security analytics module is disabled.)

You can specify additional criteria to further limit the report to hosts, protocols, ports, or interfaces in the Additional Criteria section. These can be entered by browsing and clicking, or by entering them manually.

Search by Event IDs

The report can be limited to a list or range of event ID numbers. When you specify event IDs, the event properties criteria are ignored.

Report Format

The report can display pie charts of events reported by:

- **Alert level** - High, Medium, Low
- **Analytic category** - Performance & Availability, User-defined, Security
- **Analytic** - displays events for each type of analytic, such as Link Congestion, Interface, Host Scan.
- **Policy** - displays events by individual policies, as they are identified by name on the Behavior Analysis > Policies pages.
- **Metric** - displays events by the monitored metrics that caused alerts.

Additionally, the report can display a list of events. Each event listed has a summary of event information and a link to an Event Detail report. The detail report displays a summary of the anomalies identified as part of the event and provides links to additional details.

Additional controls

In addition to the policies, hosts, protocols, ports and interfaces specifications, the Report Criteria section includes:

- **Time frame** - the length of time (ending now) or the interval of time (from x to y) that the report is to cover
- **Time frame behavior** - select among showing events that started within the time frame, events that started before the time frame, or events that are on-going
- **Templates** - a menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template. You can also load an existing template for the selected reporting category, if one has been saved.
- **Run now** - runs the report and displays the results as soon as they are available
- **Run in background** - opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Event Report section

The Event Report section displays the event list and the pie charts that you selected from the Report Format options in the Report Criteria section.

The title bar of the Event Report section includes a Report Options control. This enables you to save, print or email the report.

The title bar of the event list has a menu that enables you to change the columns on the table, change the number of rows displayed per page, and export the table contents.

Pie charts

The pie charts display events by alert level (High, Medium, or Low) or by the analytic that detected them.

Event list

The event list provides a summary of events, listed by event ID. The list is sortable by column. Additionally, you can use the Options menu to add, remove or rearrange the columns included in the report. The following columns are available:

- **Actions taken** - identifies actions that have been taken on this event, including:
 - Email-notified - Email has been sent to the specified recipients.
 - Trap-notified - An SNMP trap has been sent to the designated management system.
 - Vscan-run - A vulnerability scan has been started.
- **Alert Level** - the level of alert the event triggered: High, Medium, or Low.
- **Analytic** - the name of the analytic that detected the event, such as Application Availability, Host Scan, etc.
- **Analytic Category** - the category of the analytic that detected the event: Health, Performance & Availability, Security, Service, User-defined
- **Destination** - host name of the destination device associated with the event. If the name cannot be resolved, the IP address is displayed.
- **Destination IP** - the IP address of the destination device associated with the event. You can right-click individual host listings for a list of optional actions.
- **Destination MAC** - the MAC address of the destination device associated with the event. This is available if the appliance is integrated with DHCP. You can right-click individual host listings for a list of optional actions.
- **Duration**
- **End Time**
- **Event ID** - Each event listed has a link to an Event Details report that displays a summary of the anomalies identified as part of the event and provides links to additional details.
- **Interface** - the interface in the format of device name:label. If the device name is not available, then the device IP address is displayed. If the interface label is not available, then the index number is displayed. These are the interfaces listed on the System > Devices/Interfaces pages.
- **Interface IP** - the IP address of the interface, if it has one. Otherwise, the IP address of the device.
- **Mitigation plan** - If a Mitigation Plan has been generated, the number of the plan is displayed.
- **On going** - Yes or No to indicate if the event was ongoing at the time that the report was run.
- **Policy** - the name of the policy as it appears on the Behavior Analysis > Policies pages.
- **Port/App name** - the port name (e.g., tcp/80) followed by the service name in parentheses, followed by the application name, if available. Application names are listed on the Definitions > Applications pages.
- **Severity** - the severity, on a scale of 1 to 100, of the threat posed by the event.
- **Source** - the host name of the source device associated with the event. If the name cannot be resolved, the IP address is displayed.

- **Source IP** - the IP address of the source device associated with the event. You can right-click individual host listings for a list of optional actions.
- **Source MAC** - the MAC address of the source device associated with the event. This is available if the appliance is integrated with DHCP.
- **Start Time**

Event Details reports

An Event Details report is created and saved for each event that triggers an alert. There are several ways to view the Event Detail report:

- Click the event ID on the Dashboard page.
- Go to the Reports > Events page, generate an event report, then click the event ID on the report.
- If an event report has already been run and saved, go to the Saved Reports page, view the event report, and click the event ID on the Event report.
- If you are on a remote management system and receive an email or SNMP notification from the appliance, view the URL included with the message. This requires an Event Viewer account.

The Event Detail report displays detailed information about the event. The details depend on the type of event. The report provides options to:

- Snooze alerts caused by the event - “Snoozing” suppresses the reporting of alerts for the type of event for a time period that you specify. Snoozed events continue to be reported on the events lists the same way that other events are.
- Learn the event - the appliance “learns” an event by checking the alerting threshold that the event is exceeding and calculating what the alerting thresholds should be to avoid triggering alerts under the current conditions.
- Mitigate the event - If you have configured the appliance for mitigation, you can initiate mitigation by starting from an event listed in the events list on the Dashboard page.
- ACL - If a User-defined policy triggers an alert because an upper limit was exceeded, the Event Details report provides an ACL button. This opens a dialog box in which you can generate access control list entries. The appliance generates these by converting host-pair-port information into Cisco ACL syntax. These are compatible with access list numbers 101 - 199 in most Cisco IOS releases. You can examine the list and determine which entries to roll up, group, or cut and paste into a router. You can export the list to a file for further analysis.

Additionally, you can print or email the Event Details report.

Viewing with an Event Viewer account

An Event Detail page can be viewed by a user with an Event Viewer account as follows:

- Open the email notification of the alert condition (if using email) or use your network management system to view the URL contained in the SNMP trap message that reported the event.
- Click the link in the email message or trap message.
- When prompted, enter your user name and password. The appliance displays the Event Detail report.

Event Viewers cannot log in to the GUI or view anything other than the Event Detail report.

Event Detail reports are specific to the type of event that they are reporting. If a vulnerability scan report that includes the event has been created or is in the process of running, this is noted on the Event Detail report.

SteelHead QoS shaping policy reports

The NetProfiler and NetExpress appliances report statistics for outbound SteelHead traffic that has been shaped by SteelHead QoS shaping policies. They report statistics by SteelHead appliances, by SteelHead sites, and by SteelHead QoS shaping policies. This enables you to gain both an overall view and detailed views of how your SteelHead QoS shaping policies are performing across your network.

The Reports > SteelHead QoS Shaping page is the primary source of these reports. This page opens with a navigation pane on the left displaying SteelHead appliances, SteelHead sites, and SteelHead QoS shaping classes. Select a SteelHead from the SteelHeads drop down list to see which sites and classes you can run reports for.

The navigation pane shows an Aggregated Classes folder and a Sites folder. These can be expanded and collapsed.

The Aggregated Classes folder expands to list the SteelHead basic QoS shaping classes. Each class entry in this folder represents the aggregation of all traffic in that class for all sites defined on the selected SteelHead.

The Sites folder expands to display a list of all sites that have been properly defined on the selected SteelHead. You can run a report for each QoS class of each site.

The Sites folder has a subfolder named Global. Classes appear in this folder if:

- They are not defined in the site\$\$class format.
- The site component of their class name does not match the name of a valid SteelHead site.

Classes that are listed in the Global folder are not included in the Aggregated Classes folder.

Running a report

There are two type of SteelHead QoS shaping reports available from the Reports > SteelHead QoS Shaping page:

- Summary report, available by clicking the name of the SteelHead.
- Detail report, available by clicking the name of a SteelHead site or QoS class.

If you use a left-click, the report runs for a time frame starting 1 hour ago. If you right-click, you can choose a different time frame. The right-click menu also offers other reports.

To run a report, left-click or right-click an entry in the navigation pane as follows:

- SteelHead name - Left-click to run the SteelHead QoS Shaping Summary report for the SteelHead, or right-click to see a menu of other reports that you can run for the SteelHead.
- Class name in the Aggregated Classes folder - Left-click to run a detailed report on outbound traffic for the class across all sites defined for this SteelHead, or right-click to see a menu of other reports that you can run for the SteelHead.
- SteelHead site name in the Sites folder - Left-click to run a report on outbound traffic for all QoS classes on this site, or right-click to see a menu of other reports that you can run for the site.
- Class name listed under a site in the Sites folder - Left-click run a detailed report on outbound traffic for this class at this site, or right-click to see a menu of other reports that you can run for the class.

SteelHead QoS Summary reports

The SteelHead QoS Summary report is run by left-clicking a SteelHead entry in the navigation pane of the Reports > SteelHead QoS Shaping page. It can also be run from the Reports > Shortcuts page. When running it from the Shortcuts page, you must specify the SteelHead in the Report Criteria section. When running it from the Reports > SteelHead QoS Shaping page, the SteelHead you left-click is automatically selected, so the report results are displayed without the Report Criteria section. The report results include the following sections:

- Summary
- Traffic by Aggregated SteelHead QoS Classes
- Traffic by Sites (Host Groups)
- Traffic by WAN Interface
- Traffic by Application

You can expand the Report Criteria section, specify a different time frame, and re-run the report.

The report contains multiple sections, depending on the report formats selected in the Report Criteria section. Each section has controls for modifying the display or closing the individual section. Tables have options for changing columns, changing the number of rows, filtering, and exporting the data in a Comma-Separated-Value (CSV) file.

The report has a Report Options menu at the top. This enables you to save, schedule, print, email or export the report and to change the units of measure in the report. You can export the table as a CSV, HTML archive or PDF file.

Report Criteria section

The Report Criteria section specifies the SteelHead that is the subject of the report. A browse feature enables you to search for and select a different SteelHead appliance.

The Report Criteria section includes the following controls:

- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Report Format** - The Report Format section allows you to show or hide sections for:
 - QoS Class Details
 - QoS Site Details
 - Interface Details
 - Application Details
- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Summary section

The Summary section lists the following SteelHead QoS configuration settings:

- Configuration Mode

- QoS and Application Statistics Export
- QoS Shaping
- QoS Marking
- QoS WAN Oversubscription
- QoS Class Mode
- Last Configuration Synchronization date and time - The last time that the NetProfiler or NetExpress successfully polled the SteelHead to obtain QoS configuration information.

The Summary section also reports the QoS status of the SteelHead WAN interfaces.

Traffic by Aggregated SteelHead QoS Classes section

The Top 10 SteelHead QoS Aggregated Classes graph shows the classes of the heaviest outbound traffic flows. For each QoS shaping class, the graph shows the aggregation of traffic on all the SteelHead sites. Left-click and drag over an area to zoom in. Left-click a class display to run a shaping report for that class. Right-click a class display to see additional reports available for the class.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Traffic by SteelHead QoS Aggregated Classes table lists the QoS shaping classes in order of outbound traffic volume. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Sites (Host Groups) section

The Top 10 SteelHead QoS Sites graph displays the SteelHead sites that have the most outbound traffic on QoS-enabled interfaces. The report name says Host Group parenthetically because a SteelHead site is treated like a host group. The NetProfiler and NetExpress automatically define a host group type for each SteelHead appliance from which they receive information. Within that host group type, each SteelHead site is treated as a host group. Within the host group for each site, traffic between hosts is reported just as traffic between hosts that are not associated with a SteelHead.

Left-click and drag over an area to zoom in. Left-click a site display to run a shaping report for that site. Right-click a site display to see additional reports available for the site.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Traffic by QoS Site table lists the SteelHead sites with the highest traffic volumes. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by WAN Interface section

The Traffic by WAN Interface graph displays the outbound traffic volumes of the busiest QoS-enabled WAN interfaces of the SteelHead in terms of the percentage of utilization of each.

Left-click and drag over an area to zoom in. Left-click a site display to run a shaping report for that interface. Right-click an interface display to see additional reports available for the interface.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The WAN Interfaces table lists the SteelHead QoS-enabled WAN interfaces with the highest outbound traffic volumes. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Application section

The Top 10 Applications graph lists the applications that are responsible for the most outbound traffic on the SteelHead QoS-enabled WAN interfaces.

Left-click and drag over an area to zoom in. Left-click an application display to run a shaping report for that application. Right-click an application display to see additional reports available for the application.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Traffic Breakdown by Application section lists the busiest applications and their main statistics. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

SteelHead QoS Shaping reports

SteelHead QoS Shaping reports show how SteelHead QoS shaping policies are performing across the network. They can be run from the Reports > SteelHead QoS Shaping page, the Reports > Shortcuts page, and the right-click menu in reports that display SteelHead sites or QoS shaping classes.

When you run the report by left-clicking a SteelHead site or QoS shaping class in the navigation pane of the Reports > SteelHead QoS Shaping page, the site or class you click is the subject of the report. When you run the report from the Reports > Shortcuts page, the report first displays the Report Criteria section for you to specify the site and class information.

There are three variations of the report based on what you click in the navigation pane of the Reports > SteelHead QoS Shaping page:

- Aggregated Class - When you click an aggregated class under the Aggregated Classes folder.
- Site - When you click a SteelHead site under the Sites folder.
- Unaggregated Class - When you click a class listed under one of the sites in the Sites folder or in the Global folder.

SteelHead QoS Shaping report for an aggregated class

The SteelHead QoS Shaping report for an aggregated class is run by left-clicking a class entry in the Aggregated Classes folder in the navigation pane of the Reports > SteelHead QoS Shaping page. The report includes the following sections:

- Report Criteria
- SteelHead QoS Aggregated Class Summary
- Traffic by QoS Shaping Class
- Traffic by Application
- Traffic by Site (Host Group)
- Traffic by Interface
- Traffic by Host

- **Traffic by Host Pair**

The report has a Report Options menu at the top. This enables you to save, schedule, print, email or export the report and to change the units of measure in the report. You can export the table as a CSV, HTML archive or PDF file.

Report Criteria section

The Report Criteria section specifies the SteelHead and QoS class that are the subject of the report. This is specified in the form of the full path of the SteelHead QoS shaping policy except that the path includes the term “Aggregated_Classes” instead of a site name because it is the aggregation of the traffic for all the sites using this class. A browse feature enables you to search for and select a different shaping policy.

The Report Criteria section includes the following controls:

- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Additional Traffic Criteria** - You can limit the report to specified interfaces and applications.
 - **Interfaces** - A browse tool enables you to look up and select the interfaces you want to investigate. The others are filtered out. Leave this field blank to include all device interfaces.
 - **Applications** - A browse tool enables you to look up and select the applications you want to investigate. The others are filtered out. Leave this field blank to include all applications.
- **Report Format** - The Report Format section allows you to show or hide sections for:
 - SteelHead QoS Class Traffic
 - SteelHead QoS Site Traffic
 - Interface Traffic
 - Application Analysis
 - Host Analysis
 - Host Pair Analysis
- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

SteelHead QoS Aggregated Class Summary section

The SteelHead QoS Aggregated Class Summary section displays the average minimum bandwidth utilization for the aggregation of all outbound traffic in the class at all SteelHead sites. It also displays the QoS configuration settings.

Traffic by QoS Shaping Class section

The Top 10 SteelHead QoS Shaping Class graph shows the classes of the heaviest outbound traffic flows. For each QoS shaping class, the graph shows the aggregation of outbound traffic on all the SteelHead sites. Left-click and drag over an area to zoom in. Left-click a class display to run a shaping report for that class. Right-click a class display to see additional reports available for the class.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Traffic by SteelHead QoS Shaping Class table lists the QoS shaping classes in order of outbound traffic volume. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Application section

The Top 10 Applications graph lists the applications that are responsible for the most outbound traffic on the SteelHead QoS-enabled WAN interfaces.

Left-click and drag over an area to zoom in. Left-click an application display to run a shaping report for that application. Right-click an application display to see additional reports available for the application.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Applications table lists the busiest applications seen on the QoS-enabled outbound WAN interfaces and their main statistics. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by QoS Site (Host Group) section

The Top 10 SteelHead QoS Sites graph displays the QoS-enabled SteelHead sites that have the most outbound traffic. The report name says Host Group parenthetically because a SteelHead site is treated like a host group. The NetProfiler and NetExpress automatically define a host group type for each individual SteelHead appliance from which they receive information. Within that host group type, each SteelHead site is treated as a host group. Within the host group for each site, traffic between hosts is reported just as traffic between hosts that are not associated with a SteelHead.

Left-click and drag over an area to zoom in. Left-click a site display to run a shaping report for that site. Right-click a site display to see additional reports available for the site.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The SteelHead QoS Site table lists the QoS-enabled SteelHead sites with the highest outbound traffic volumes. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Interface section

The Top 10 Network Interfaces graph displays the outbound traffic volumes of the busiest QoS-enabled WAN interfaces of the SteelHead in terms of the percentage of utilization of each.

Left-click and drag over an area to zoom in. Left-click a site display to run a shaping report for that interface. Right-click an interface display to see additional reports available for the interface.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Network Interfaces table lists the QoS-enabled SteelHead WAN interfaces with the highest outbound traffic volumes. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host section

The Top 10 Hosts graph lists the hosts that are responsible for the most outbound traffic on the QoS-enabled WAN interfaces.

Left-click and drag over an area to zoom in. Left-click a host display to run a host information report for that host. Right-click a host display to see additional reports available for the host.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Hosts section lists the busiest hosts and their main statistics. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host Pair section

The Top 10 Hosts Pairs graph lists the host pairs that are responsible for the most outbound traffic on the QoS-enabled SteelHead WAN interfaces.

Left-click and drag over an area to zoom in. Left-click a host pair display to run a host information report for that host pair. Right-click a host pair display to see additional reports available for the host pair.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Host Pairs section lists the busiest host pairs and their main statistics. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

SteelHead QoS Shaping report for a site

The SteelHead QoS Shaping report for a SteelHead site is run by left-clicking a site entry in the Sites folder in the navigation pane of the Reports > SteelHead QoS Shaping page. The report includes the following sections:

- Report Criteria
- SteelHead QoS Site Summary
- Traffic by QoS Shaping Class
- Traffic by Application
- Traffic by Interface
- Traffic by Host
- Traffic by Host Pair

The report has a Report Options menu at the top. This enables you to save, schedule, print, email or export the report and to change the units of measure in the report. You can export the table as a CSV, HTML archive or PDF file.

Report Criteria section

The Report Criteria section specifies the SteelHead and site that are the subject of the report. This is specified in the form of the path of the SteelHead QoS shaping policy. A browse feature enables you to search for and select a different shaping policy.

The Report Criteria section includes the following controls:

- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Additional Traffic Criteria** - You can limit the report to specified interfaces and applications.
 - **Interfaces** - A browse tool enables you to look up and select the interfaces you want to investigate. The others are filtered out. Leave this field blank to include all device interfaces.

- **Applications** - A browse tool enables you to look up and select the applications you want to investigate. The others are filtered out. Leave this field blank to include all applications.
- **Report Format** - The Report Format section allows you to show or hide sections for:
 - SteelHead QoS Class Traffic
 - SteelHead QoS Site Traffic
 - Interface Traffic
 - Application Analysis
 - Host Analysis
 - Host Pair Analysis
- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can reopen the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

SteelHead QoS Site Summary section

The SteelHead QoS Site Summary section displays the bandwidth and average outbound traffic volume for the site. It also displays the QoS configuration settings for the site.

Traffic by QoS Shaping Class section

The Top 10 SteelHead QoS Shaping Classes graph shows the classes of the heaviest outbound traffic flows for the site. Left-click and drag over an area to zoom in. Left-click a class display to run a shaping report for that class. Right-click a class display to see additional reports available for the class.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Traffic by SteelHead QoS Shaping Class table lists the QoS shaping classes in order of outbound traffic volume for the site. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Application section

The Top 10 Applications graph lists the applications that are responsible for the most outbound traffic for the site.

Left-click and drag over an area to zoom in. Left-click an application display to run a shaping report for that application. Right-click an application display to see additional reports available for the application.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Applications table lists the busiest applications seen on the QoS-enabled outbound WAN interfaces and their main statistics. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Interface section

The Top 10 Network Interfaces graph displays the outbound traffic volumes of the busiest QoS-enabled WAN interfaces for the site in terms of the percentage of utilization of each.

Left-click and drag over an area to zoom in. Left-click a site display to run a shaping report for that interface. Right-click an interface display to see additional reports available for the interface.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Network Interfaces table lists the QoS-enabled SteelHead WAN interfaces with the highest outbound traffic volumes for the site. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host section

The Top 10 Hosts graph lists the hosts that are responsible for the most outbound traffic on the QoS-enabled WAN interfaces for this site.

Left-click and drag over an area to zoom in. Left-click a host display to run a host information report for that host. Right-click a host display to see additional reports available for the host.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Hosts section lists the busiest hosts and their main statistics. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host Pair section

The Top 10 Hosts Pairs graph lists the host pairs that are responsible for the most outbound traffic on the QoS-enabled SteelHead WAN interfaces.

Left-click and drag over an area to zoom in. Left-click a host pair display to run a host information report for that host pair. Right-click a host pair display to see additional reports available for the host pair.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Host Pairs section lists the busiest host pairs and their main statistics. You can use the menu for the graph to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

SteelHead QoS Shaping report for a class at a specified site

The SteelHead QoS Shaping report can report on outbound traffic for a class at an individual SteelHead site (in contrast to reporting on an aggregation of the traffic for the class at all sites, as described earlier). You can do this by left-clicking a class name entry under the site name in the Sites folder in the navigation pane of the Reports > SteelHead QoS Shaping page. The report includes the following sections:

- Report Criteria
- SteelHead QoS Class Summary
- SteelHead QoS Class Details
- Traffic by Application
- Traffic by Interface
- Traffic by Host

- **Traffic by Host Pair**

The report has a Report Options menu at the top. This enables you to save, schedule, print, email or export the report and to change the units of measure in the report. You can export the table as a CSV, HTML archive or PDF file.

Report Criteria section

The Report Criteria section specifies the SteelHead, the SteelHead site and QoS class that are the subject of the report. This is specified in the form of the full path of the SteelHead QoS shaping policy. A browse feature enables you to search for and select a different shaping policy.

The Report Criteria section includes the following controls:

- **Time frame** - The length of time (ending now) or the interval of time (from x to y) that the report is to cover.
- **Data resolution** - The period of time represented by each data point on the report.
- **Additional Traffic Criteria** - You can limit the report to specified interfaces and applications.
 - **Interfaces** - A browse tool enables you to look up and select the interfaces you want to investigate. The others are filtered out. Leave this field blank to include all device interfaces.
 - **Applications** - A browse tool enables you to look up and select the applications you want to investigate. The others are filtered out. Leave this field blank to include all applications.
- **Report Format** - The Report Format section allows you to show or hide sections for:
 - SteelHead QoS Class Traffic
 - SteelHead QoS Site Traffic
 - Interface Traffic
 - Application Analysis
 - Host Analysis
 - Host Pair Analysis
- **Templates** - A menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template.
- **Run now** - Runs the report and displays the results as soon as they are available. When you run the report using the Run now control, the Report Criteria section is collapsed to present a better display of the report. You can re-open the Report Criteria, change the settings and run a new report.
- **Run in background** - Opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

SteelHead QoS Class Summary section

The SteelHead QoS Class Summary section displays the average minimum bandwidth utilization for outbound traffic in the class at the SteelHead site. It also displays the QoS configuration settings.

SteelHead QoS Class Details section

The SteelHead QoS Class Details graph shows the outbound traffic volume for the class at the site. It also shows the bandwidth limit. Left-click and drag over an area to zoom in.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

Traffic by Application section

The Top 10 Applications graph lists the applications that are responsible for the most outbound traffic to the SteelHead site. Left-click and drag over an area to zoom in. Left-click an application display to run a shaping report that is limited to that application. Right-click an application display to see additional reports available for the application.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Applications table lists the busiest applications seen on the QoS-enabled outbound WAN interfaces for the site and their main statistics. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Interface section

The Top 10 Network Interfaces graph displays the outbound traffic volumes of the busiest QoS-enabled WAN interfaces for the SteelHead site in terms of the percentage of utilization of each.

Left-click and drag over an area to zoom in. Left-click an interface display to run a shaping report for that interface. Right-click an interface display to see additional reports available for the interface.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Network Interfaces table lists the QoS-enabled SteelHead WAN interfaces with the highest outbound traffic volumes. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host section

The Top 10 Hosts graph lists the hosts that are responsible for the most outbound traffic on the QoS-enabled WAN interfaces. Left-click and drag over an area to zoom in. Left-click a host display to run a host information report for that host. Right-click a host display to see additional reports available for the host.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Hosts table lists the busiest hosts and their main statistics. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Traffic by Host Pair section

The Top 10 Hosts Pairs graph lists the host pairs that are responsible for the most outbound traffic on the QoS-enabled SteelHead WAN interfaces.

Left-click and drag over an area to zoom in. Left-click a host pair display to run a host information report for that host pair. Right-click a host pair display to see additional reports available for the host pair.

You can use the menu for the graph to change this display between a stacked area graph and a line graph or to export the data to a CSV file.

The Host Pairs table lists the busiest host pairs and their main statistics. You can use the menu for the table to add or remove columns, limit the number of rows, filter the data being displayed, or export the data to a CSV file.

Active Directory Users reports

User accounts that have permission can generate reports of user logins and login attempts on the network. This report requires a source of user identity information to be integrated with the appliance. You can confirm the availability of an identity information source on the Integration > Identity Sources page.

The user identity reporting feature supports several approaches to creating reports:

- Active Directory Users Report page
- Quick report box in header
- Left-clicking a user name on an Event Report, Host Information Report, or another Active Directory Users Report
- Right-clicking a host or host group to get a shortcut menu

Active Directory Users Reports provide user identification and login information. They can be limited to specified time spans, users, hosts, or CIDR blocks of hosts.

The page includes a Report Criteria section for specifying user criteria for the report and a results section for displaying the report.

Report Criteria section

Use the Report Criteria section to:

- Limit the report to a comma-separated list of users.
- Limit the report to a comma-separated list of hosts.
- Include or exclude successful or failed login attempts.

In addition to user and host criteria, the Report Criteria section includes:

- **Time frame** - the length of time (ending now) or the interval of time (from x to y) that the report is to cover
- **Templates** - a menu of options for using the current Report Criteria settings. You can use the current settings as a template and schedule future reports to be automatically generated using the template. You can also load an existing template for the selected reporting category, if one has been saved.
- **Run now** - runs the report and displays the results as soon as they are available

Run in background - opens a window for you to specify the title of the report and the option for saving the report. It then runs the report in the background. When the report is ready, it is saved and listed on the Reports > Saved Reports page.

Report section

When the report is completed and displayed, you can use the Report Options menu to:

- Save the report. It will be listed on the Reports > Saved Reports page.
- Print the report to a printer or file.
- Email the report in HTML, Comma-Separated-Value (CSV), or PDF format.

On the Users List, you can use the Options menu to:

- Change Columns using the column chooser.

- Change Number of Rows reported on a page.
- Export to export the report data in a Comma-Separated-Value (CSV) file, HTML archive file, or PDF file.

Saved reports

The Reports > Saved Reports page lists completed reports and report templates that were saved on the Traffic Report page. It also lists event reports, users reports, and vulnerability scan reports.

Operators, Administrators and Monitors can:

- View completed reports.
- Create new reports from saved templates, either immediately or in the background.
- Reschedule the running of a report template to produce new reports and save the new schedule as a revision to the original template or as part of a new template.
- Delete saved reports and templates.

Reports section

The Reports section lists the reports that have been completed, are running, or are waiting to run. Click Refresh to view the latest status of the reports listed. Click the name of a completed report to view the report.

In the Reports section, you can choose report storage options, and you can sort the list by owner, report name, run time, status, and size. You can mark a report to keep indefinitely or you can delete it.

The Reports section options menu allows you to filter the list of reports. Also, the option menu allows you to limit the list to your own reports and to just the most recent days, weeks or months. Additionally, the option menu provides a feature for pruning the list by deleting reports that are older than a specified date.

Templates section

The Templates section lists templates; their owners, types and names; and their schedule and next run time. You can sort the templates by any of these attributes. The Templates section options menu allows you to filter the list of templates to limit the list to your own templates. Additionally, you can prune reports that are older than a specified date.

In the Templates section, you can select a template and do one of the following:

- **Load** - Load the template so that you can modify the reporting criteria and then run it in the foreground or background.
- **Run in Background** - Run a report using the selected template, save it in the Completed Reports section, and distribute it as configured with the Save as/Reschedule feature.
- **Save as/Reschedule** - Open a page on which you can edit the specifications for how reports that are run using the selected template are scheduled, saved, and distributed. Each template can be scheduled to generate reports according to the time in a different time zone.
- **Delete** - Delete the selected template.

Up to 500 report templates can be saved. Templates are not automatically deleted.

General Information reports

Detailed information about a specific host, host group, interface, application, DSCP marking, or network segment is available by right-clicking the name wherever it is displayed as a link (underlined). These reports are also available from the Reports > Shortcuts page Built-in tab. Clicking a report shortcut in the General Information Reports section of this tab prompts you to identify what is to be reported.

The following types of information reports are available:

- [“Application Information reports” on page 242](#) - detailed information about the activity of one of more applications
- [“Interface Information reports” on page 243](#) - detailed information about a selected interface
- [“Device Information reports” on page 246](#) – detailed information about the traffic volumes and utilization of selected devices
- [“Interface Group Information reports” on page 246](#) – detailed information about the traffic volumes and average performance of interface groups
- [“Host Information reports” on page 247](#) - detailed information about an individual host
- [“Host Group Information reports” on page 248](#) - detailed information about a selected host group
- [“Network Segment Information reports” on page 250](#) - statistics for traffic between two specified interfaces
- [“DSCP Information reports” on page 251](#) - information about traffic that is tagged for a specified DSCP marking
- [“BGP AS Information reports” on page 252](#) - information about BGP Autonomous Systems
- [“Server Information reports” on page 249](#) - detailed information about a specified server
- [“Switch Information reports” on page 249](#) - information about a switch and an inventory of its physical ports
- [“Analyzing packet information with Packet Analyzer” on page 268](#)
- [“Packet reporting and export with Cascade Sensor” on page 270](#)

Information reports include report-level and section-level option menus. Report options allow you to save, print or email the report. You can also change the display units and, where applicable, change the group type by which host groups are reported.

Section-level options allow you to modify graphical displays, filter table columns, and export data.

Refer to the on line help system for detailed descriptions of the report contents.

Application Information reports

Application Information reports provide multiple perspectives on the activity of one of more applications. When you run it from the Shortcuts page, you can limit the report to a list of applications. When you run the report from the right-click menu, it reports on the application you right-clicked.

The report includes statistics about total application traffic volume, server hosts, client host groups, host pairs and ports, DSCP markings, and network segments. Overall traffic volume is reported as sent or received relative to the application servers.

The report provides the following information for the specified applications and time frame:

Summary

This section reports the peak and average transmitted and received traffic for the specified application. It also reports the peak and average connections per second.

Details

This section graphs the average traffic volume that was transmitted and received by the specified applications over the selected time frame.

Servers

This section provides the following performance information about the specified applications:

- Average server delay for the top ten application servers
- Average number of retransmissions by the top ten application servers
- Average number of Resets by the top ten application servers
- Breakdown of traffic volume by application server

A dashed line in a graph indicates that the plot is missing data points.

Clients

This section provides information by host groups. The information is presented by host group because there are usually a large number of individual clients. The section includes:

- Average response time experienced by the top ten host groups that are clients of the specified application
- Breakdown of application traffic by client host group
- Host pair connections (click and zoom for details)

Delivery Path

This section provides information about the application delivery path, including:

- Server-client host pairs, the ports over which they are communicating, and performance statistics
- Breakdown of application traffic by DSCP markings
- Connections by network segments

Interface Information reports

The Interface Information report is useful for seeing average and peak percent utilization of an interface over the past hour or the required time frame. Data is reported as inbound (In) or outbound (Out) relative to the interface. The report also provides interface configuration information.

When you run the report from the Shortcuts page, you can limit the report to a list of interfaces. You can use the browser tool to select interfaces or enter them manually using the *device:interface* format.

You can also run the report by right-clicking an interface name or index number. Interface names are available on traffic reports when you select Network Interfaces for the “Report by” criteria on the Reports > Traffic pages. Names and index numbers are also available on the System > Devices/Interfaces pages.

Right-click the interface name anywhere it is displayed and select Interface Information Report. This runs the report for the interface you right-click for the time frame you select from the menu.

The report can include comparisons of information in the specified time frame with the same information in an earlier time frame. Tables list the percentage of increase or decrease from the earlier time frame if data is available.

Report options allow you to save, schedule, print or email the report. You can also change the display units and change the group type by which host groups are reported. Section-level options allow you to modify graphical displays, filter tables, and export data.

The report lists the following information for the selected time frame.

Summary section

- Interface Information - identifies the interface by its name, type, MTU, speed, and MAC address.
- Traffic Summary - lists peak traffic, average traffic and percent of capacity utilization for input and output.
- Interface Groups - If the interface has been assigned to one or more interface groups on the Definitions > Interface Groups page, then the groups it belongs to are listed.

Details section

- Traffic Volume by Peak % Utilization - Mirror graph showing transmit and receive percent utilization over the selected time frame. Choose Edit Settings from the menu for this section to add Average % Utilization to the display.

Activity section

- Top Inbound Applications with Ports by Average Bits/s - graphs the traffic volumes of the applications and ports with the top inbound traffic seen on the interface within the specified time frame.
- Inbound Traffic by Application with Port - lists the average and total inbound traffic volumes of applications and ports seen on the interface.
- Top Outbound Applications with Ports - graphs the traffic volumes of the applications and ports with the top outbound traffic seen on the interface within the specified time frame.
- Outbound Traffic by Application with Port - lists the average and total outbound traffic volumes of applications and ports seen on the interface.

Quality of Service (DSCP) section

- Top Inbound DSCPs by Average Bits/s - graphs the volumes of inbound traffic with the DSCP markings seen most often on the interface.
- Inbound Traffic by DSCP - lists inbound traffic volumes seen on the interface ordered by DSCP markings.
- Top Outbound DSCPs by Average Bits/s - graphs the volumes of outbound traffic with the DSCP markings seen most often on the interface.
- Outbound Traffic by DSCP - lists outbound traffic volumes on the interface ordered by DSCP markings.

Quality of Service (CBQoS Inbound) section

When a Cisco router is configured to send NetProfiler class-based Quality of Service information, this section displays pre-policy and post-policy inbound traffic volumes by the classes defined on the router.

- Top Classes by Average Pre-policy Bits/s - graphs the traffic classes that have the most traffic before the router's inbound QoS policies are applied.
- Top Classes by Average Post-policy Bits/s - graphs the traffic classes that have the most traffic after the router's inbound QoS policies are applied.

- Top Classes by Average Dropped Bits/s - graphs the traffic classes for which the router's inbound QoS policies have discarded the most incoming traffic.
- Summary - lists peak and average values for the traffic classes displayed on the graphs. The class names are fully qualified except for the top-level policy names.

The status of CBQoS polling is displayed on System > Devices/Interfaces page Synchronization tab when you select CBQoS Devices as the Device type. See [“Devices supporting Class-based QoS” on page 145](#).

Quality of Service (CBQoS Outbound) section

When a Cisco router is configured to send NetProfiler class-based Quality of Service information, this section displays pre-policy and post-policy outbound traffic volumes by the classes defined on the router.

- Top Classes by Average Pre-policy Bits/s - graphs the traffic classes that have the most outbound traffic before the router's outbound QoS policies are applied.
- Top Classes by Average Post-policy Bits/s - graphs the traffic classes that have the most traffic after the router's outbound QoS policies are applied.
- Top Classes by Average Dropped Bits/s - graphs the traffic classes for which the router's QoS policies have discarded the most outbound traffic.
- Summary - lists peak and average values for the traffic classes displayed on the graphs. The class names are fully qualified except for the top-level policy names.

Virtual Networks section

- Top Virtual Networks by Average Bits/s - graphs the traffic volumes of the virtual networks with the top traffic seen on the interface within the specified time frame.
- Virtual Networks by Average Bits/s - lists the traffic volumes of the virtual networks seen on the interface within the specified time frame.

Conversations section

This section lists the traffic volumes of host pairs and the ports over which they are communicating. The DSCP list column shows all the DSCP markings seen in the conversation between the hosts. This makes it easy to identify interfaces that have multiple DSCP markings.

Event Activity section

- Alert Level Summary chart – pie chart showing proportions of High, Medium, and Low alerts.
- Alert Level Summary table – lists High, Medium, and Low alerts by number and by percent of total.

Notes on alert reporting

The Interface Information Report includes alerts that were triggered by User-defined policies of the Interface Policy type. This includes alerts triggered by Interface Policies that are limited to specific hosts. The Interface Information Report does not include alerts that were triggered by User-defined policies of the Host Policy type, even if the Host Policy was limited to a specific interface. That is, running an Interface Information Report on an interface will not show a Host Policy alert associated with the interface.

Use an Interface Information Report to see alerts triggered by the Interface Policy type of User-defined policy. Use a Host Information Report to see alerts triggered by the Host Policy type of User-defined policy.

Device Information reports

The Device Information report provides summary and detail information about a specified device. When you run it from the Shortcuts page, you must specify the device. When you run the report from the right-click menu, it reports on the device you right-clicked.

The device can be specified by its name or IP address. You can use the Browse feature to search for a device in an interface group.

Summary section

The Summary section lists:

- Device name
- Device IP address
- Device type
- Device version (if applicable)
- Number of interfaces in the device
- Interface Group to which the device belongs
- Description of the device

Details section

The Details section lists or displays:

- Traffic volume - displayed as average bits per second
- Top 10 network interfaces - displayed as average percent of utilization
- Network interfaces - list of the device's network interfaces with percent utilization and traffic volume

Activity section

The Activity section lists or displays:

- Top 10 applications with ports - displayed as average bits per second
- Applications with ports - traffic volume and active connections

DSCP Markings section

The DSCP Markings section lists or displays:

- Top 10 DSCP markings - traffic volume displayed as average bits per second
- Traffic by DSCP markings - volumes and active connections

Interface Group Information reports

The Interface Group Information report provides summary and detail information about a specified interface group or subgroup and all the interfaces contained within it.

The interface groups are specified by name. Subgroups are specified by path and name. You can use the Browse feature to search for an interface group or subgroup. The report includes a Summary section, Details section, Activity section and DSCP markings section.

Summary section

The Summary section lists:

- Interface Group name
- Interface Group description
- Number of interfaces in the group

Details section

The Details section lists or displays:

- Traffic volume - displayed as average bits per second
- Top 10 network interfaces - displayed as average percent of utilization
- Network interfaces - list of the device's network interfaces with percent utilization and traffic volume

Activity section

The Activity section lists or displays:

- Top 10 applications with ports - displayed as average bits per second
- Applications with ports - traffic volume and active connections

DSCP Markings section

The DSCP markings section lists or displays:

- Top 10 DSCP markings - traffic volume displayed as average bits per second
- Traffic by DSCP markings - volumes and active connections

Host Information reports

The Host Information report provides summarized information for a specified host. When you run it from the Shortcuts page, you must specify the host. When you run the report from the right-click menu, it reports on the host you right-clicked.

The report includes the name, IP address, and group membership of the host; traffic volumes, client-server connections, users, and alerts for the past hour. Overall traffic volume is reported as sent or received relative to the hosts.

The report lists the following information for the selected time frame:

- **Host Information** - the name, address, date first seen on the network, and the switch port. (To obtain the switch port, the switch must have been added on the Integration > Switch Port Discovery page.)
- **Traffic Summary** - average and peak transmitted and received traffic volumes.
- **Host Groups** - If the host has been assigned to one or more host groups on the Definitions > Host Groups page, then the groups it belongs to are listed.
- **Traffic Volume by Average Bytes per Second** - mirror graph showing transmit and receive time series data.
- **Top 10 Applications and Ports Served** - pie chart of applications and ports served by the hosts.
- **Traffic Breakdown by Application and Port Served** - list of traffic volumes, connections, and response times by application and port.

- **Top 10 Applications and Ports Connected To** - pie chart of applications and ports that the host has connected to.
- **Applications and Ports Connected To** - list of applications and ports that the host has connected to.
- **Host Pair and Port** - list of servers and clients that the host being reported is connecting to and the port numbers over it is connecting.
- **Peers Summary** - list of hosts that are having conversations with host being reported. The peer host's group is listed. Traffic volumes are listed in descending order.
- **Traffic by DSCP marking** - pie chart and table listing DSCP markings in use by traffic volume.
- **Users** - list of users of the host being reported, including time and identity information.
- **Alert Level Summary** chart - pie chart showing proportions of High, Medium, and Low alerts on this host for the selected time frame.
- **Alert Level Summary** table - lists High, Medium, and Low alerts by number and by percent of total.

Host Group Information reports

The Host Group Information report provides summarized information for a host group. When you run it from the Shortcuts page, you can limit the report to a list of hosts, subnets, or host groups. You can also limit it to a selected host group type.

When you run the report from the right-click menu, it reports on the host group you right-clicked.

The report includes traffic volume for the group, applications or ports served or connected to, group pairs, and alerts that have occurred within the group during the last hour.

Overall traffic volume is reported as sent or received relative to the hosts. Sections of the report that list what group a host belongs to identify group membership in terms of group type.

The report lists the following information for the selected time frame:

- **Host Group Information** - total number of hosts and the average and peak transmitted and received bytes per second.
- **Traffic Volume by Average Bytes per Second** - mirror graph showing transmit and receive time series data.
- **Hosts Seen Over Time** - line graph of number of hosts over time.
- **Top 10 Applications and Ports Served** - pie chart of applications and ports served by hosts in the host group.
- **Traffic Breakdown by Application and Port Served** - list of traffic volumes, connections, and response times by application and port.
- **Top 10 Applications and Ports Connected To** - pie chart of applications and ports that hosts in the host group have connected to.
- **Host Pair and Port** - list of hosts within the group that are connecting to other hosts inside or outside of the group, and the port number over which they are connecting.
- **Host Group Pair Summary** - list of host groups that the selected host group is having conversations with.
- **Top Peers Summary** - list of hosts that are having conversations with hosts in the selected host group. The peer host's group is listed. Traffic volumes are listed in descending order.
- **Traffic by DSCP Marking** - pie chart and table listing DSCP markings in use by traffic volume.
- **Alert Level Summary** chart - pie chart showing proportions of High, Medium, and Low alerts.
- **Alert Level Summary** table - lists High, Medium, and Low alerts by number and by percent of total.

Server Information reports

The Server Information report provides a comprehensive view of the operation of a specified server. When you run it from the Shortcuts page, you must specify the server. When you run the report from the right-click menu, it reports on the server you right-clicked. You can run the report by right-clicking a server name anywhere it is displayed and selecting Server Information Report from the shortcut menu.

The report provides the following information for the specified server and time frame.

Summary

This section reports:

- **Host Information** - the name, address, date first seen on the network, and the switch port. (To obtain the switch port, the switch must have been added on the Integration > Switch Port Discovery page.)
- **Traffic Summary** - average and peak transmitted and received traffic volumes.
- **Host Groups** - If the server has been assigned to one or more host groups on the Definitions > Host Groups page, then the groups it belongs to are listed.

Applications

This section reports:

- Average traffic volumes of the top ten applications served by the specified server.
- Average response time of the top ten applications served by the specified server.
- Breakdown of traffic volumes by application and port served.

Clients

This section reports:

- Average response time of the top ten peer groups (host groups containing clients of the server).
- List of host groups containing clients of the server.

DSCP Marking

- Pie chart showing the traffic of each DSCP marking as a percent of total traffic being reported.
- Table listing DSCP markings in use by traffic volume.

Events

This section reports:

- Pie chart showing proportions of High, Medium, and Low alerts on this server for the selected time frame.
- Table listing High, Medium, and Low alerts by level and number.

Switch Information reports

The Switch Information report provides information about a specified switch and an inventory of its physical ports. This report is helpful anytime you want to know basic information about a switch, such as model or serial number, software version and physical connections. For example, the inventory of switch port connections could help identify which devices will be affected during a switch maintenance window or other downtime event.

There are several ways to run the report:

- In the Quick report box at the top of the page, select **Switch** from the drop down list, enter the IP address of a switch, and click **Go**.
- Click the address of a switch in a traffic report.
- Right-click the address of a switch in a traffic report and choose Switch Info Report from the shortcut menu.
- On the Reports > Shortcuts page Built-in tab, go to the General Information Reports section and click the Switch Information link.

Note that the switch must be identified on the Configuration > Integration > Switch Port Discovery page before you can run this report.

Report Criteria

The results of the report are limited to information meeting the following criteria:

- Switch - Name or IP address of the switch to be inventoried.
- “Include switch ports without a MAC address” - Select this option to also return switch ports that do not have any devices attached.
- “Use only switch port polling for ARP Bindings” - Do not use DHCP import information to resolve MAC address to IP Address of attached devices.
- Switch Ports - Return information for only switch ports specified in a comma-separated list.
- Host MACs - Limit the switch port inventory to switch ports that are attached to hosts that have MAC addresses in a comma-separated list.

Report results

The results of the report are displayed in a Summary section and a Details section. The Summary section lists information that has been collected from the switch by SNMP polling. The Details section lists the ports of the switch and what is attached to them. If a switch is configured as “Lookup Router” only, the Switch Inventory table will be empty unless you enable “Include switch ports without a MAC address.”

You can use the menu in the Switch Inventory table to:

- Add or remove columns to the table.
- Change the number of rows displayed.
- Specify a filter to reduce the number of entries in the list.
- Export the list to a host group.
- Export the list to a comma-separated-value (CSV) file.

If you want to collect more information about a switch from an external system, you can pass the switch name and IP address to the external system by right-clicking the switch IP address in a report and choosing External link from the shortcut menu. This requires first defining a device link on the Configuration > Integration > External Links page.

Network Segment Information reports

The Network Segment Information report provides a view of the operation of a specified network segment. When you run it from the Shortcuts page, you must specify the network segment interfaces. When you run the report from the right-click menu, it reports on the segment you right-clicked.

The report includes statistics about the interfaces that are the endpoints of the segment, traffic volumes over the segment by application and port, and alerts occurring on the segment.

The report provides the following information for the specified network segment and time frame:

Summary

This section reports:

- **Segment Information** - the addresses of the transmitting interface and receiving interfaces comprising the two endpoints of the segment; the name, description (if available), index, MTU, type, speed, and MAC address.
- **Traffic Summary** - average and peak traffic volumes across the segment.

Details

This section graphs the average traffic volume that was carried by the specified segment over the selected time frame.

Applications

This section includes:

- Graph of average traffic volumes of the top ten applications and ports that have been seen on the segment.
- Table listing traffic on the segment by application and port and providing performance statistics, such as connections, retransmissions, and the percent of total traffic that is retransmissions.

Events

This section includes:

- Pie chart showing proportions of High, Medium, and Low alerts on this server for the selected time frame.
- Table listing High, Medium, and Low alerts by level and number.

DSCP Information reports

The DSCP Information reports provide information about the usage of a specified DSCP marking. When you run the report from the Shortcuts page, you must specify the DSCP markings of traffic to be reported. When you run it from the right-click menu, it reports on the DSCP markings you right-clicked.

The report includes the DSCP marking definition, a summary of traffic tagged with the specified DSCP markings and information about this traffic for by interface, application, and server host.

The report lists the following information for the selected time frame:

- **DSCP Marking Definition** - the DSCP markings name, decimal value, binary value, and description. You can modify the standard definitions of DSCP markings and add new definitions on the Definitions > DSCP page.
- **Traffic Summary** - traffic volumes are listed for all traffic in the network sent with the specified DSCP marking and all traffic received with the specified DSCP marking.
- **Interfaces** - the table lists the interfaces on which the specified DSCP marking was seen. It lists the descriptions of the interfaces, sorts them by traffic volume, and provides performance statistics.
- **Applications** - graphs traffic volumes for the top ten applications that use the specified DSCP markings. It also lists all applications and ports using the specified DSCP marking. It sorts them by traffic volume and provides performance statistics.

- **Server** - graphs traffic volumes for the top ten servers that use the specified DSCP marking. It also lists all hosts using the specified DSCP markings. It sorts them by traffic volume and provides performance statistics.

BGP AS Information reports

The BGP AS Information report provides information about BGP (Border Gateway Protocol) Autonomous Systems. This report requires SNMP polling to be enabled on the System > Devices/Interfaces page. (Select Global SNMP Settings from the Options menu on the Devices & Interfaces tab.)

Report Criteria

The results of the report are limited to information meeting the following criteria:

- BGP AS - Specify an AS number or name, or use the Browse tool to select one from a list.
- Scope - The Scope criteria limit the report to:
 - Public & Private - Only traffic flows that have gone through an Autonomous System, whether public or private.
 - Public - Only traffic flows that have gone through at least one public Autonomous System and are not known to have gone through any private Autonomous Systems. The report excludes flows that are known to have gone through a private Autonomous System. However, because the full AS paths may not be known to NetProfiler, such flows may have also gone through private Autonomous Systems.
 - Private - Only traffic flows that have gone through at least one private Autonomous System and are not known to have gone through any public Autonomous Systems. The report excludes flows that are known to have gone through a public Autonomous System. However, because the full AS paths may not be known to NetProfiler, such flows may have also gone through public Autonomous Systems.
- Group type - Choose the host group type by which traffic is reported in the Traffic by Host Groups section of the report results.

Report results

The results of the report are displayed in the following sections:

- Summary - AS number, active connections, hosts and traffic volume, and a connection graph showing all known AS paths.
- Traffic by Peers - Line graph showing the traffic volume of the top 10 peers of the AS and a table listing all peers of the AS sorted by traffic volume.
- Traffic by Public Peers - Line graph and table showing traffic volumes of peers of the AS. The graph shows volumes for the top 10 peers of the AS. The table lists traffic volumes for all peers of the AS sorted by volume. Both the graph and table are limited to traffic that has been carried over a public AS.
- Traffic by Private Peers - Line graph and table showing traffic volumes of peers of the AS. The graph shows volumes for the top 10 peers of the AS. The table lists traffic volumes for all peers of the AS sorted by volume. Both the graph and table are limited to traffic that has been carried over a private AS.
- Traffic by Host Groups - Line graph showing the top host groups (that is, the host groups with the highest traffic volume) that are connecting with hosts in the Autonomous System, and a table, sorted by traffic volume, listing all host groups that are connecting with hosts in the Autonomous System.

Investigation reports

Investigation reports include:

- [“Audit trail” on page 146](#) - available from the System > Audit Trail page
- [“Event reports” on page 225](#) - available from both the Reports > Shortcuts page and the Reports > Events menu
- [“Active Directory Users reports” on page 240](#) - available from both the Reports > Shortcuts page and the Reports > Users menu
- [“Service Level Objective reports” on page 253](#) - information about the operation of a Performance & Availability policy over time
- [“Performance Investigation reports” on page 254](#) - visual indications of the performance of an application delivery path
- [“95th Percentile report” on page 255](#) - shows the 95th percentile level on a graph of interface utilization

Service Level Objective reports

The Service Level Objective Report displays information about the operation of a policy over time. It provides qualitative graphical feedback on the frequency and magnitude of policy violations that are being detected. Additionally, it displays typical and actual values of the traffic attributes that the policy is monitoring. It uses the default time frame of the last week.

The report can be run from:

- Reports > Shortcuts page Built-in tab Service Level Objective link.
- Behavior Analysis > Policies page, Service tab or Performance & Availability tab, Configured Policies section.
- Right-click menu displayed by right-clicking a service policy or a performance and availability policy.

It can be printed, saved, scheduled and emailed. Scheduling the report to be routinely run and emailed can be a useful way of monitoring on-going traffic behavior as well as policy performance.

The report options and report section options offer the same functions as other reports for saving, printing, emailing and exporting the report, and for editing the graphical displays.

The report has a Report Criteria section and a Report section.

Report Criteria section

The Report Criteria section includes the following controls:

Select Policy

This box displays an expandable and collapsible tree listing service policies and performance and availability policies. Expand the tree as necessary to select the service segment or service location policy, or the performance and availability policy, that you want the report run for.

Time frame

Specify the time frame of the report as relative to the current time or as an absolute time interval:

Relative to the current time can be:

- **Starting** - Specify the most recent number of minutes, hours, days, weeks, months or years that the report is to cover, ending now. For example, if you specify the Starting value as 1 week ago, then the time frame of the report will start at this time last week and end now. If you specify 1 year ago, the time frame will start at this time on this date last year and end now.
- **Previous** - Specify the most recently ended full minute, hour, day, week, month or year before the current minute, hour, day, week, month or year, respectively. For example, if the current time is 10:17 AM Wednesday and you specify the Previous value as 1 hour, then the time frame of the report will start at 9:00 AM and end at 10:00 AM today. If you specify the previous 1 week, the time frame will start at 12:00 AM Monday of last week and end at 12:00 AM Monday of this week. If you specify the previous year, then the time frame will start at 12:00 AM, January 1st of last year and end at 12:00 AM, January 1st of this year.

For an absolute time interval, use the **From/To** field. Specify the time frame either by entering dates and times manually or by:

- Clicking the date to display a calendar tool, then choosing a date from the calendar.
- Clicking a time to display a list box of times, then choosing a time from the list.

The time frame starts at the “From” time and ends at the “To” time.

Report section

Graphs show the performance of each metric in the policy that has been selected and initialized. Each graph shows the:

- Current value of the traffic attribute being monitored.
- Typical value of the attribute for this time of the day and day of the week.
- Range of variations from the typical value that are tolerated as being normal for the current sensitivity setting. The solid light green area displays the tolerance range.
- Zone where the value of the attribute exceeded the tolerance range. A point outside the tolerance range is referred to as an “outlier.” The time frame in which an outlier occurred is displayed in yellow or red. Click in the yellow or red area to run an Event Report for the time frame.

Metric values that lie within the green tolerance range are treated as normal. Those within the yellow tolerance range indicate a low alert condition. Each instance of the plot of actual traffic behavior going outside the tolerance range is regarded as an “outlier.” That is, an outlier is a point where actual traffic behavior differs from typical behavior by more than the amount that you have specified as being within the tolerance of the policy. Values exceeding the green tolerance range cause a yellow outlier indication. Values exceeding the yellow tolerance range cause a red outlier indication. The NetProfiler uses outliers to determine if a policy violation has occurred.

Multiple outliers may be determined to be part of the same event. Because of the number of factors analyzed in determining if a policy violation event has occurred, the number of outliers does not directly indicate how many events will be detected.

Performance Investigation reports

Performance Investigation Reports provide visual indications of the performance of an application delivery path. You specify the application delivery path in terms of one or more attributes, such as application, ports, protocols, servers, clients, and DSCP markings. The report displays traffic volumes and performance metrics so that you can visually correlate changes on multiple aspects of the delivery path performance.

Performance Investigation Reports are available from the Investigation Reports section of the Reports > Shortcuts page **Built-in** tab. When you run the report from the Shortcuts page, you must specify the reporting criteria. That is, you use the Report Criteria section to limit the report to the applications, ports, protocols, servers, clients, and DSCP markings that are of interest. Empty fields are interpreted as meaning “all.”

Report-level options allow you to save, print or email the report. You can also change the display units and change the group type by which host groups are reported.

Section-level options allow you to modify graphical displays, change table columns, filter content, and export data.

The report provides the following information for the specified delivery path elements and time frame:

- Application Analysis section – graphs displaying timing metrics in milliseconds, traffic volumes, connections, resets and DSCP usage.
- Client Analysis section – graphs displaying the number of clients and the transaction times and traffic volumes for the top 10 client groups that are peers of the specified client's host group.
- Server Analysis section – graphs displaying timing metrics and traffic volumes for the top 10 server hosts.
- Details section – tables listing traffic volumes by application with port and by host pair with port.

Timing Metrics

The timing metrics available in this report include the peak and average times in milliseconds for the following:

- **Net RTT** - Network Round Trip Time; estimated during the 3-stage handshake for connection setup and then updated thereafter.
- **Resp Time** - Response Time; time from when the client sends a request to when the client receives the response.
- **Server Delay** - the time between the last client request packet and the first server response packet.
- **Client Delay** - the time from when a client sends a connection setup acknowledgment to a server to when the client sends a request to the server.
- **Req Network Time** - Request Network Time; the time difference between the arrival time of the last data segment sent by the client during the request and the departure time of the first data segment sent by the client during the request.
- **Resp Network Time** - Response Network Time; the time difference between the arrival time of the last data segment sent by the server during the response and the departure time of the first data segment sent by the server during the response.
- **Transaction Time** - the time, from the client perspective, between the last data segment sent by the server and the first data segment sent by the client during the same transaction.
- **Req Retrans Time** - Request Retransmission Time; the estimated time caused by TCP retransmission during the client request.
- **Resp Retrans Time** - Response Retransmission Time; the estimated time caused by TCP retransmission during the server response.

Where applicable, these can be added to a display. To add or remove metrics from a chart, pull down the menu in the upper right corner of the chart and click **Edit**. This opens a window in which you can select additional metrics for display and modify the display format.

95th Percentile report

The 95th Percentile report is run from the Investigation Reports section of the Reports > Shortcuts page Built-in tab. It is a network interface report that displays the 95th percentile of interface usage. By eliminating the high outliers, the 95th percentile display provides a graphical indication of the “water level” and “head room” of your bandwidth utilization.

By default the report displays peak and average inbound and outbound traffic volumes for the most recent hour and indicates the 95th percentile level of traffic volume. Just click **Run now**.

After you have run the report, you can choose **Edit Settings** from the Overall Traffic graph menu and select the 80th or 90th percentiles for display. You can also use settings in the Report Criteria section to limit the report to traffic on specific interfaces or with specific DSCP markings, applications, protocols or ports. Additionally, you can use the Time Frame control to specify the time the report covers.

By default the report uses 1-minute data resolution and combines five 1-minute records into one 5-minute record. The graph plots the values of the 5-minute intervals over time. Switching to a longer data resolution interval decreases the accuracy of the percentile calculations. For data resolution intervals of longer than one minute, 1-minute records are not combined into 5-minute records.

The menu for the Overall Traffic graph section of the report allows you to export the graph data as a comma-separated value (CSV) file. The Report Options menu at the upper right side of the page allows you to save, schedule, print, email or export the entire report.

SDN (Software-defined Networks) Reports

The NetProfiler and NetExpress support software-defined networks based on the IETF Internet Draft titled “VXLAN: A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks.” The appliances monitor traffic carried by virtual networks in a VXLAN environment and provides the following reports:

- [“VXLAN Summary Report” on page 257](#)
- [“Virtual Network Information Report” on page 259](#)
- [“Tunnel Endpoint Information Report” on page 261](#)

VXLAN technology

VXLAN (Virtual Extensible LAN) technology enables multiple virtual networks to coexist as overlays on the same physical network. Each virtual network is independent of all other virtual networks and of the physical network. Each can have its own IP address space.

Each virtual network is identified by a VNI, which is a “VXLAN network [segment] identifier” or simply a “virtual network identifier.” On the NetProfiler or NetExpress, VNIs can be assigned names and descriptions for convenience.

A hypervisor runs a VXLAN software environment in which a large number of virtual machines serve as virtual hosts for end users. The virtual hosts can connect to one another within that hypervisor. The hypervisor also runs a tunnel endpoint, which allows its virtual hosts to connect to virtual hosts running in VXLAN software hosted by other hypervisors. This is made possible by a UDP tunneling protocol that encapsulates the Ethernet frames of the virtual traffic in UDP datagrams for transport over the physical network from one tunnel endpoint to another tunnel endpoint. Additionally, VXLAN-enabled gateway devices enable connections between virtual hosts and hosts on other networks.

If your organization uses VXLAN virtualization technology internally, then you can set up virtual networks for different departments so that the network for one department is logically isolated from the network for another department.

If your organization provides network services to outside customers, then you can set up a virtual network for each customer to ensure that no customer can access another customer's network.

The customer (virtual network user) is considered a tenant. The customer's traffic is referred to as tenant traffic. Tenant traffic flows between virtual hosts running on the same hypervisor and also, by way of UDP datagrams being tunneled between hypervisors, to virtual hosts running on other hypervisors. The appliance reports how much tenant traffic is flowing between virtual hosts on the same hypervisor (intra-machine traffic) and how much traffic is being tunneled over the physical network between hypervisors (inter-machine traffic).

You can use the Virtual Network Information report to monitor how virtual hosts are communicating over a virtual network and use the Tunnel Endpoint Information report to monitor how much of a load they are placing on the physical network.

The VXLAN administrator may be able to reduce the load on your physical network by moving related virtual hosts to the hypervisor that they would otherwise be tunneling to.

The NetProfiler also reports the traffic across the physical and virtual interfaces of the hypervisors. The physical interfaces that a hypervisor uses to communicate with other endpoints are referred to as uplink interfaces. The interfaces that the virtual hosts use when they need to access virtual hosts on other hypervisors are referred to as access interfaces.

Consult with your VXLAN administrator or designer if you need more information about how virtual machines within a VXLAN environment communicate with one another and how they might possibly be moved to reduce the load on the physical network.

VXLAN Summary Report

The VXLAN Summary report can be run from the Reports > Shortcuts page. It provides an overview of the entire VXLAN environment including tenant traffic and tunneled traffic. It is a good starting point for identifying VXLAN configuration problems.

The VXLAN Summary report page has four sections:

- Report Criteria
- Summary of VXLAN Environment
- Virtual Network Details: Tenant Traffic
- Physical Network Details: Tunnel Traffic

All sections have menus for actions that can be performed on the section.

Report Criteria

Expand the Report Criteria section to specify if the report format is to include the virtual network and physical network details sections. You can also choose a time frame for the report.

Summary of VXLAN Environment

The Summary section displays:

Virtual Network Summary

- Total Virtual Networks – number of virtual networks seen during the specified time frame
- Total Virtual Network <units> – all tenant traffic, whether occurring only between virtual machines on a hypervisor or being tunneled between virtual machines on different hypervisors
- Total Tunnel <units> – traffic on the physical network that is tunneling virtual traffic between hypervisors
- % of Virtual-only Traffic – the percent of the traffic in all virtual networks that is intra-machine traffic

Breakdown of Virtual Network Traffic

A pie chart shows the percentages of inter-machine traffic and intra-machine traffic. The larger the percentage of intra-machine traffic, the less of a load the virtual network is placing on the physical network. The larger the percentage of inter-machine traffic (virtual traffic being tunneled between hypervisors), the greater a load the virtual network is placing on the physical network.

Virtual Traffic Volume by Avg Inter-machine Bytes/s, Avg Intra-machine Bytes/s

A line chart displays the amount of traffic between virtual hosts located on the same hypervisors and traffic between virtual hosts located on different hypervisors.

Virtual Network Details: Tenant Traffic

A tenant is the organization using a virtual network in a VXLAN environment. Virtual hosts are implemented on virtual machines in the tenant's virtual network. Traffic between the tenant's virtual hosts is tenant traffic.

Tenant traffic may be between virtual hosts running on the same hypervisor (intra-machine traffic) or it may be between virtual hosts running on different hypervisors (inter-machine traffic). Inter-machine connections require tunneling the tenant traffic over the physical network.

A VXLAN environment can support many virtual networks. Each is an independent overlay on the physical network. That is, one tenant has no knowledge of other tenants or of the physical network.

This section of the report lists the average traffic volumes for the report time frame for:

- Top 10 virtual networks
- All virtual networks
- Top 10 tunnel endpoints
- All tunnel endpoints

The Top 10 lists can be exported to CSV (comma-separated value) files. On the other tables you can:

- Add or remove columns. For additional detail, choose Add/Remove Columns from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table.
- Change the number of rows displayed in the table.
- Show a filter that allows you to limit the table to virtual networks meeting specific criteria.
- Export the table to a CSV file.

Physical Network Details: Tunnel Traffic

This section of the report displays traffic on the physical network that is transporting tunneled virtual traffic from one tunnel endpoint to another. It indicates the load that each individual virtual network is placing on the physical network. It reports traffic volumes of the physical network for:

- Top 10 virtual networks being tunneled over the physical network
- All virtual networks being tunneled over the physical network
- Tunnel endpoint pairs - graphical representations of the tunnel endpoints at each end of connections that are tunneling tenant traffic

The Top 10 lists can be exported to CSV (comma-separated value) files. On the table listing all virtual networks you can:

- Add or remove columns. For additional detail, choose Add/Remove Columns from the menu for the section. This opens the column chooser. Double-click a metric in the column chooser to add it to the table.

- Change the number of rows displayed in the table.
- Show a filter that allows you to limit the table to virtual networks meeting specific criteria.
- Export the table to a CSV file.

The menu in the title bar of the connection graph enables you to:

- Edit settings – control the size and layout format for displaying the network components
- Export to CSV – export the data from the display to a file in comma-separated value format
- Export to PDF – export the display to an PDF file
- Export to SVG – export the display to a file that can be opened and edited by Microsoft Visio
- Reroute Edges – clean up the diagram after you have made layout adjustments. This improves the display of connections between network components without moving the network component displays.

Virtual Network Information Report

The Virtual Network Information report provides detailed information about a specified virtual network. You must specify the name or VNI of the virtual network to be reported. You can enter it manually or use the Browse feature to locate the virtual network.

The report has four sections:

- Report Criteria
- Summary
- Virtual Network Details: Tenant Traffic
- Physical Network Details: Tunnel Traffic
- All sections have menus for actions that can be performed on the section.

Report Criteria

Use the Report Criteria section to specify the virtual network and if the report format is to include the virtual network and physical network details sections. You can also choose a time frame for the report.

Summary

The Summary section displays the following.

Virtual Network Summary

- Virtual Network – name of the virtual network (as defined on the Definitions > Interface Groups page)
- VNI Description – description of the virtual network (as defined on the Definitions > Interface Groups page)
- Total Tunnel Endpoints – number of tunnel endpoints used by the virtual network
- Hosts seen – number of virtual hosts seen on the network during the report time frame
- Total Virtual Network <units> – all tenant traffic, whether occurring only between virtual machines on a hypervisor or being tunneled between virtual machines on different hypervisors
- Total Tunnel <units> – traffic on the physical network that was tunneling virtual traffic between hypervisors
- % of Virtual-only Traffic – the percent of the traffic in this virtual network that was intra-machine traffic

Virtual Network Traffic Summary

This section lists the total and average traffic statistics for this virtual network for the time frame of the report.

Breakdown of Virtual Network Traffic

A pie chart shows the percentages of inter-machine traffic and intra-machine traffic. The larger the percentage of intra-machine traffic, the less of a load the virtual network is placing on the physical network. The larger the percentage of inter-machine traffic (virtual traffic being tunneled between hypervisors), the greater a load the virtual network is placing on the physical network.

Virtual Traffic Volume by Avg Inter-machine Bytes/s, Avg Intra-machine Bytes/s

A line chart displays the amount of traffic between virtual hosts located on the same hypervisors and traffic between virtual hosts located on different hypervisors.

Virtual Network Details: Tenant Traffic

A tenant is the organization using a virtual network in a VXLAN environment. Virtual hosts are implemented on virtual machines in the tenant's virtual network. Traffic between the tenant's virtual hosts is tenant traffic.

This section of the report lists the average tenant traffic volumes for the report time frame as follows.

- Traffic Volume line graph – displays tenant traffic volume for the virtual network. Tenant traffic may be between virtual hosts running on the same hypervisor (intra-machine traffic) or it may be between virtual hosts running on different hypervisors (inter-machine traffic). Inter-machine connections require tunneling the tenant traffic over the physical network.

The menu for the graph section enables you to export the data as a comma-separated value (CSV) file. It also has an Edit Settings option for modifying the display.

Additionally, you can use the zoom controls to modify the display.

- Top 10 Hosts pie chart – displays the percentage of the virtual network traffic attributable to each of the top 10 busiest virtual hosts.
- Top 10 Hosts line graph – displays the percentage of the virtual network traffic attributable to each of the top 10 busiest virtual hosts. The menu for this section includes options for exporting the data to a CSV file and editing the display settings. The Edit Settings option allows you to:
 - Switch between a stacked display and a line display.
 - Switch between linear and logarithmic display scales.
 - Extend the Y-axis to zero. This is useful for retaining perspective when two plots differ by a relatively small amount.
- Hosts table – lists the average traffic volumes for all the virtual hosts seen on the virtual network during the time frame of the report.
- Top 10 Applications with Ports pie chart – displays the percentage of the virtual network traffic attributable to each of the top 10 busiest applications on the virtual network.
- Applications with Ports table – lists the average traffic volumes for all the applications seen on the virtual network during the time frame of the report.
- Top 10 Host Pairs pie chart – displays the percentage of the virtual network traffic attributable to each of the top 10 busiest virtual host pairs on the virtual network.
- Host Pairs table – lists the average traffic volumes for all the virtual host pairs seen on the virtual network during the time frame of the report.

- Virtual Network Host Pairs connection graph – displays connections between virtual hosts on the virtual network.
- Virtual Network Flows table – lists all flows seen in the virtual network during the time frame of the report. When a virtual host connects to a physical host, there are two flows. The first flow is between the virtual host and the VXLAN-enabled gateway that serves as a proxy for connecting to the physical network. This flow is included in the Virtual Network Flows table. The second flow is between the gateway and the host in the physical network. That flow is not included in the Virtual Network Flows table.

This table could be large, so it is deselected in the Report Criteria section by default.

Physical Network Details: Tunnel Traffic

This section of the report displays traffic on the physical network that is transporting tunneled virtual traffic from one tunnel endpoint to another. It indicates the load that the specified virtual network is placing on the physical network, as follows:

- Traffic Volume line graph – lists traffic on the physical network that is tunneling virtual traffic for the specified virtual network.
The menu for the graph section enables you to export the data as a comma-separated value (CSV) file. It also has an Edit Settings option for modifying the display.
Additionally, you can use the zoom controls to modify the display.
- Top 10 Tunnel Endpoint pie chart – displays the percentage of the physical network traffic attributable to each of the top 10 busiest tunnel endpoints.
- Top 10 Tunnel Endpoint line graph – displays the percentage of the physical network traffic attributable to each of the top 10 busiest tunnel endpoints. The menu for this section includes options for exporting the data to a CSV file and editing the display settings. The Edit Settings option allows you to:
 - Select which tunnel endpoints to include in the graph.
 - Switch between a stacked display and a line display.
 - Switch between linear and logarithmic display scales.
 - Extend the Y-axis to zero. This is useful for retaining perspective when two plots differ by a relatively small amount.
- Tunnel Endpoints table – lists the average traffic volumes for all tunnel endpoints seen on the virtual network during the time frame of the report.
- Tunnel Endpoint Pairs connection table – displays graphical representations of the tunnel endpoints at each end of connections that are tunneling tenant traffic.
- Tunnel Flows table – lists all flows that were tunneling tenant traffic across the physical network during the time frame of the report. This table could be large, so it is deselected in the Report Criteria section by default.

Tunnel Endpoint Information Report

The Tunnel Endpoint Information report provides detailed information about a specified tunnel endpoint.

The report has four sections:

- Report Criteria
- Summary
- Virtual Network Details: Tenant Traffic
- Physical Network Details: Tunnel Traffic

All sections have menus for actions that can be performed on the section.

Report Criteria

In this section you must specify the tunnel endpoint to be reported. You can optionally limit the report to traffic for a specified virtual network. Except for requiring the tunnel endpoint, the report runs using default settings unless you modify the settings in this section.

The Report Criteria section includes the following settings:

- **VXLAN (Optional)** – To limit the report to a specified virtual network, open the VXLAN section and browse to a virtual network.
- **Tunnel Endpoint** – This is a required field. Click Browse to open the lookup tool and search for tunnel endpoints. In the list of tunnel endpoints, you can mouse over the Details icon to identify the tunnel endpoint you want to report on. The Paths section of the Details popup identifies the virtual networks that are using the tunnel endpoint.

If you use the Virtual Network field to limit the report to a virtual network, ensure that the selected tunnel endpoint includes that virtual network.
- **Report Format** – Select which sections of the report to include. The report always includes the Summary section. It must also include at least one of the following Report Format selections:
- **Show Virtual Network Traffic Details** – Select this to include the Virtual Network Details: Tenant Traffic section in the report. This requires that you specify a virtual network. If you leave the Virtual Network field empty, then the Virtual Network Details: Tenant Traffic section does not appear.
- **Show Tunnel Traffic Details** – Select this to include the Physical Network Details: Tunnel Traffic section.
- **Show Flow List** – Select this to include a virtual network flow list in the Virtual Network Details: Tenant Traffic section and a tunnel flow list in the Physical Network Details: Tunnel Traffic section. This option is deselected by default because the flow lists may be quite long.
- **Time Frame** – Specify the time frame for the information reported.
- **Data Resolution** – The data resolution determines the granularity of the data points on the graphs. By default it is set to automatic to optimize the display for the selected time frame.

Summary

The Summary section includes the following:

Tunnel Endpoint Summary

The Tunnel Endpoint Summary section includes:

- **Tunnel Endpoint** – the IP address of the tunnel endpoint being reported
- **Total Virtual Networks** – the number of virtual networks using the specified tunnel endpoint
- **Total Physical Switch Ports** – the number of physical switch ports used by the tunnel endpoint. The tunnel endpoints uses these switch ports to communicate with other tunnel endpoints. These are referred to as uplink ports.
- **Total Virtual Switch Ports** – the number of virtual switch ports in use by the tunnel endpoint. These are referred to as access ports.
- **Total Tunnel Endpoints** – the number of peer tunnel endpoints this tunnel endpoint communicates with

- Total Virtual Network <units> – the total amount of virtual network traffic seen by this tunnel endpoint. This includes all tenant traffic for the virtual network, whether occurring only between virtual machines on the hypervisor or being tunneled between virtual machines on different hypervisors. If no virtual network was specified, then this figure includes the traffic of all virtual networks that used this tunnel endpoint during the time frame of the report.
- Total Tunnel <units> – traffic on the physical network that was tunneling virtual traffic between hypervisors
- % of Virtual-only Traffic – the amount of virtual network traffic, expressed as a percent of total virtual network traffic, that used this tunnel endpoint for intra-machine conversations.

Breakdown of Virtual Network Traffic

A pie chart shows the percentages of inter-machine traffic and intra-machine traffic for this tunnel endpoint. The larger the percentage of intra-machine traffic, the less of a load the virtual network is placing on the physical network. The larger the percentage of inter-machine traffic (virtual traffic being tunneled between physical machines), the greater a load the virtual network is placing on the physical network.

Virtual Network Details: Tenant Traffic

A tenant is the organization using a virtual network in a VXLAN environment. Virtual hosts are implemented on virtual machines in the tenant's virtual network. Traffic between the tenant's virtual hosts is tenant traffic.

Because this is a tunnel endpoint report, the information in this section is limited to tenant traffic that uses the specified tunnel endpoint. For that traffic, this section reports information about virtual hosts rather than about tunnel endpoints. It lists the average tenant traffic volumes for the report time frame as follows.

- Traffic Volume line graph – displays tenant traffic volume for the tunnel endpoint. Tenant traffic may be between virtual hosts running on the same hypervisor (intra-machine traffic) or it may be between virtual hosts running on different hypervisors (inter-machine traffic), which the specified tunnel endpoint is tunneling.

The menu for the graph section enables you to export the data as a comma-separated value (CSV) file. It also has an Edit Settings option for modifying the display.

Additionally, you can use the zoom controls to modify the display.

- Top 10 Hosts pie chart – displays the percentage of the total tenant traffic generated by the top 10 virtual hosts that are using this tunnel endpoint.
- Hosts table – lists the average tenant traffic volumes seen during the time frame of the report. If no virtual network is specified, then this includes tenant traffic for all virtual networks that include this tunnel endpoint.
- Top 10 Applications with Ports pie chart – displays the percentage of the tenant traffic attributable to each of the top 10 busiest applications seen by the tunnel endpoint.
- Applications with Ports table – lists the average traffic volumes for all the applications seen by the tunnel endpoint during the time frame of the report.
- Top 10 Host Pairs pie chart – displays the percentage of the virtual network traffic attributable to each of the top 10 busiest virtual host pairs on the virtual network. If no virtual network is specified, then this includes tenant traffic for all virtual networks that include this tunnel endpoint.
- Host Pairs table – lists the average traffic volumes for all the virtual host pairs seen on the virtual network during the time frame of the report.
- Tunnel Endpoint and Host Pairs connection graph – displays connections between virtual hosts and this tunnel endpoint.
- Virtual Network Flows table – lists flows between entities on the virtual network seen during the time frame of the report. This table could be large, so it is deselected in the Report Criteria section by default.

Physical Network Details: Tunnel Traffic

This section of the report displays traffic on the physical network that is transporting tunneled virtual traffic from this tunnel endpoint to other tunnel endpoints, as follows:

- **Traffic Volume line graph** – lists traffic on the physical network over which this tunnel endpoint is tunneling virtual traffic. This is inter-machine traffic and does not include intra-machine traffic.

The menu for the graph section enables you to export the data as a comma-separated value (CSV) file. It also has an Edit Settings option for modifying the display.

Additionally, you can use the zoom controls to modify the display.

- **Top 10 Virtual Networks pie chart** – displays the percentage of the total tenant traffic carried by each virtual network that includes this tunnel endpoint. If the report is limited to a virtual network (specified in the Report Criteria section), then this chart will show that virtual network as generating 100% of the virtual traffic seen by the tunnel endpoint.
- **Top 10 Virtual Networks line graph** – displays the percentage of the total virtual network traffic that is attributable to each of the top 10 busiest virtual networks that include this tunnel endpoint. The menu for this section includes options for exporting the data to a CSV file and editing the display settings. The Edit Settings option allows you to:
 - Switch between a stacked display and a line display.
 - Switch between linear and logarithmic display scales.
 - Extend the Y-axis to zero. This is useful for retaining perspective when two plots differ by a relatively small amount.
- **Virtual Networks table** – lists traffic statistics for the virtual networks that include this tunnel endpoint.
- **Top 10 Tunnel Endpoint Peers pie chart** – displays the percentage of the total physical network traffic attributable to each of the top 10 tunnel endpoint peers of this tunnel endpoint.
- **Top 10 Tunnel Endpoint Peers line graph** – displays the percentage of the total physical network traffic attributable to each of the top 10 tunnel endpoint peers of this tunnel endpoint. The menu for this section includes options for exporting the data to a CSV file and editing the display settings. The Edit Settings option allows you to:
 - Switch between a stacked display and a line display.
 - Switch between linear and logarithmic display scales.
 - Extend the Y-axis to zero. This is useful for retaining perspective when two plots differ by a relatively small amount.
- **Tunnel Endpoints Peers table** – lists the average traffic volumes for connections between this tunnel endpoint and all peer tunnel endpoints during the time frame of the report.
- **Tunnel Endpoint Pairs connection graph** – displays graphical representations of the tunnel endpoints at each end of connections over which this tunnel endpoint is tunneling tenant traffic.
- **Tunnel Flows table** – lists all flows that this tunnel endpoint was using to tunnel tenant traffic across the physical network during the time frame of the report. This table could be large, so it is deselected in the Report Criteria section by default.

VoIP reports

The following pre-defined VoIP reports are available from the Reports > Shortcuts page.

- [“VoIP Performance report”](#)
- [“VoIP Dependencies - Signaling report”](#)
- [“VoIP Dependencies - Calls report”](#)

VoIP Performance report

The VoIP Performance report runs on a NetExpress appliance or on a NetProfiler or NetExpress appliance that is receiving VoIP metrics from a NetShark appliance or another NetExpress appliance. It is set by default to report on traffic that is identified as VoIP and RTP.

Although the Sensor appliance can report VoIP traffic statistics to a NetProfiler or NetExpress, the NetShark appliance or NetExpress appliance is required for reporting voice quality metrics, such as MOS, R-factor, Jitter and RTP packet loss.

Report Criteria section

The Report Criteria section enables you to limit the report to:

- **Hosts** - IP addresses or resolvable DNS names of all devices accessible on the network. Click **Browse** to search for hosts by host group type and host group.
- **Peers** - Peer hosts, subnets or host groups; what specified hosts are connecting to
- **Applications** - For the VoIP Performance report, this field is pre-populated to VoIP-RTP. The dash means “AND” (VoIP and RTP) while a comma delimiter means “OR.” Limiting the report to VoIP traffic that uses the RTP protocol excludes control plane traffic and includes only data plane traffic. You can click Browse and search for other VoIP protocols if necessary.
- **Protocols or ports used** - Limit the report to specified port numbers or port names for TCP or UDP protocols
- **DSCP markings** - Click Browse to search for Differentiated Services Code Point markings.
- **Group types** - Limit the report to traffic involving hosts in host groups of a specified type.
- **Time frame** - Time frame of the report. Specify a period of time ending in the present or a From/To time span.

Leaving an attribute field blank means “all.”

The Report Criteria section enables you to select or deselect the display of sections of the report. The Report Format options are:

- Show Network Usage Section
- Show Call Quality Section
- Show DSCP marking Section

Traffic report section

Traffic reports contain multiple sections. The contents of a report depend on the tab from which it was run, and the Report by and Report Format settings in the Report Criteria section. The report has a Report Options menu at the top for options that act on the entire report, such as saving, scheduling, printing, exporting, emailing, exporting or changing display units.

There are also controls in each section of each report, which apply to only the individual section. These provide options for editing graphing options, changing table columns, changing the number of rows in a table, and exporting data from tables and charts into a Comma-Separated-Value (CSV) files.

Refer to the on line help system for detailed descriptions of the formatting requirements for entering report criteria.

Network Usage section

The Network Usage section includes:

- Traffic Volume by Avg Bits/s
- Traffic by Application
- Top 10 Host Groups by Avg Bits/s

Call Quality section

The Call Quality section includes:

Traffic Quality by Average MOS

- Traffic Quality by Average Jitter (milliseconds)
- Traffic Quality by % RTP Loss Packets
- Worst 10 Host Groups by Minimum MOS
- Traffic by Host Group
- Host Group Pair by Average MOS
- Traffic by Host Group Pair

DSCP Marking section

The DSCP marking section includes:

- Top 10 DSCP markings by Average Bits/s
- Traffic by DSCP markings

VoIP Dependencies - Signaling report

The VoIP Dependencies - Signaling report is an application report. It reports traffic for connections between all clients and servers within the monitored network that are made over ports typically used for Voice over IP. These are listed by host pairs with ports or by host group pairs with ports. They are also displayed on a zoomable graph to indicate dependencies. Additionally, the report includes a connection graph that illustrates dependencies between clients and servers using VoIP ports.

If you are using the standard VoIP ports, then no inputs are needed to run this report.

- Click **Host** to run the report for host pairs with ports, or
- Click **Site** to run the report for host group pairs with ports.

Report Criteria

The Protocols or ports field of the Report Criteria section is pre-populated with the standard VoIP ports: tcp/1718, tcp/1719, tcp/1720, tcp/2000, tcp/5060, tcp/5660, udp/1720, udp/2517 and udp/5060.

You can modify the Report Criteria section to further limit the report, as follows.

- **VXLAN** - Limit the report to a virtual network.
- **Applications** - Click **Browse** to search for applications
- **Protocols or ports used** - The Protocols or ports field of the Report Criteria section is pre-populated with the standard VoIP ports: tcp/1718, tcp/1719, tcp/1720, tcp/2000, tcp/5060, tcp/5660, udp/1720, udp/2517. If your network uses different ports for Voice over IP, you can modify this the report criteria before running the report and save your modified version as a report template.
- **Servers, subnets or groups** - addresses or address ranges of servers or names of host groups
- **Clients, subnets or groups** - addresses or address ranges of clients or names of host groups
- **DSCP markings** - Click Browse to search for DSCP markings.
- **Time frame** - Time frame of the report. Specify a period of time ending in the present or a From/To time span.

Leaving an attribute field blank means “all.”

The Report Format section enables you to select additional displays.

Overall Traffic section

The Overall Traffic section displays the average VoIP traffic volume over time. The graph can be shifted forward or backward in time and zoomed to rerun the report on a narrower time frame.

Traffic Breakdown section

The Traffic Breakdown section displays the average volume of VoIP traffic and average number of connections between clients and servers. It displays these in both a table and a connection graph.

VoIP Dependencies - Calls report

The VoIP Dependencies - Calls report is an application report. It reports traffic for connections between clients and servers within the monitored network using Voice over IP applications. These are listed by host pairs with ports or by host group pairs with ports. They are also displayed on a zoomable graph to indicate dependencies.

Additionally, the report includes a connection graph that illustrates dependencies between clients and servers using VoIP applications.

The Applications field of the Report Criteria section is pre-populated with the VOIP-RTP application. If your network uses different a different application for Voice over IP, you can modify this filed before running report and save your modified version as a report template.

You can further limit the report by specifying other criteria.

Audit Trail reports

Audit Trail reports are described in [Chapter 6, “System Verification.”](#)

Analyzing packet information with Packet Analyzer

If a NetShark is sending packet information to a NetProfiler or NetExpress, then the NetProfiler or NetExpress can provide packet capture information to the Packet Analyzer either by sending it directly to Packet Analyzer or by exporting it as a packet capture (pcap) file. You can right-click any host, host pair, port, protocol, or flow wherever it is reported and send packet-level information about the reported item directly to Packet Analyzer for analysis or export it to a pcap file for later analysis. In both cases, the packet information is limited to the selected item and the time frame of the report.

The NetExpress appliance performs packet capture itself, so you can export packet capture files or send packet information to Packet Analyzer from the right-click menu without requiring a NetShark appliance. Also, you can define packet capture jobs and export full packet capture information as pcap files.

Additionally, the NetExpress allows Packet Analyzer users to connect to it just as they would connect to a NetShark. A Packet Analyzer user can request packet-level information from the NetExpress just as they would from a NetShark, although Packet Analyzer cannot log in to the NetExpress web interface to set up capture jobs. NetExpress capture jobs must be defined on the NetExpress Configuration > Packet Capture page. Refer to [“Packet capture \(NetExpress only\)” on page 40](#).

The use of Packet Analyzer packet analysis tool is described in the Packet Analyzer reference manual and in the product itself. Refer to the reference manual, the training videos, and the help topics in Packet Analyzer for instructions on analyzing traffic at the packet level.

This section describes accessing Packet Analyzer from within the NetProfiler. The advantage of this approach is that the NetProfiler automatically provides Packet Analyzer with the context for the item that you want to investigate. That is, Packet Analyzer opens with the information it needs to analyze the item that you right-clicked on in a NetProfiler or NetExpress report. It uses this information to obtain a packet trace from a NetShark or NetExpress. The packet information can be exported as a packet capture file or analyzed and displayed by Packet Analyzer.

Prerequisites

There are several prerequisites for using Packet Analyzer from the NetProfiler:

- **User account** - When you open Packet Analyzer from within the NetProfiler or NetExpress to analyze packet data, it must connect to the NetShark or NetExpress to obtain the data. So you must provide login credentials if you are connecting to a NetShark.
- **NetShark data export to NetProfiler** - The NetProfiler or NetExpress presents a menu of NetShark appliances that you can select as the source of the packet data you want to analyze with Packet Analyzer. The NetProfiler identifies all NetShark appliances that are sending the selected data to it. The NetShark web interface allows the NetShark administrator to set the NetProfiler configuration on the Settings > NetProfiler Settings page to export the data seen on one or more NetShark capture interfaces to one or two NetProfiler or NetExpress appliances. The NetShark exports data about all traffic flows that it sees, without any filtering.
- **NetShark capture job** - The NetProfiler and NetExpress can display traffic information seen by the NetShark whether or not a capture job is configured on the NetShark. However, a capture job is required in order to analyze the data in Packet Analyzer. One or more capture jobs can be defined for each capture interface. A capture job can filter the data according to a specification. When you use Packet Analyzer, you must specify which capture job it is to analyze. Note that catch and drop filters specified for capture jobs have no effect on the data being sent directly to the NetProfiler or NetExpress. They affect only the data being sent to Packet Analyzer.
- **Packet capture on NetExpress** - The NetExpress can be configured to capture packet data itself. It can also receive data from NetShark appliances. When exporting a packet capture file, you can select the NetExpress itself as the source of the packet capture data or select any NetShark that is sending data to the NetExpress. This feature is not available on the CAX360 model.

Analyzing NetShark or NetExpress packet information

To use Packet Analyzer to analyze packet-level data for a host, host pair, port, protocol, or flow,

1. Right-click the item to display the shortcut menu.
2. Select **Packets for this <selection>** to display the submenu.
3. Select **Analyze in Packet Analyzer**.
This opens the “Analyze in Packet Analyzer” popup window. This window has a drop-down list of NetShark appliances. It also lists the capture jobs that are running on the selected NetShark.
4. Select the NetShark appliance that you want to use as the source of the packet details you want to analyze. If you are using a NetExpress, it will be listed here along with the NetShark appliances as the source of the packet information.
5. Click the link for the capture job that you want Packet Analyzer to analyze.
6. The NetProfiler or NetExpress generates a Packet Analyzer script file based on the report criteria and the NetShark capture job parameters. Click the link to launch Packet Analyzer with the script file.
7. If required, Packet Analyzer displays a popup for you to enter the login credentials for the NetShark that you have selected.
8. Enter the login credentials and click **OK**. This opens main window of Packet Analyzer. The capture job you specified is listed in both the **Devices** and **Files** panels. In the **Files** panel you can use the trace clip created for the selection in the NetProfiler report. You can then apply views to the trace clip as necessary to analyze traffic at the packet level.

Refer to the Packet Analyzer documentation for descriptions of the features available for analyzing the traffic.

Traffic flow analysis shortcut

The right-click procedure for packet analysis allows you to analyze packet-level information for a host, host pair, port, protocol, or flow reported anywhere in the NetProfiler user interface. However, an additional shortcut is provided for analyzing traffic flows at the packet level. The Reports > Traffic pages have a report format option for displaying a flow list. The first column in the table listing traffic flows displays a row number for each flow listed. This can be clicked to analyze a traffic flow using the Packet Analyzer.

1. Left-click the flow list row number to display the “Analyze in Packet Analyzer” popup window. This window has a drop-down list of NetShark appliances classified as relevant and not relevant to the selected flow.
The window also lists the capture jobs that are running on the selected NetShark.
2. Choose the NetShark appliance that you want to use as the source of the packet details you want to analyze. (The relevant NetShark appliance is pre-selected.)
3. Click the link for the capture job on that NetShark appliance that you want Packet Analyzer to analyze.
4. The NetProfiler or NetExpress generates a Packet Analyzer script file based on the NetProfiler report criteria and the NetShark capture job parameters. Click the link to launch Packet Analyzer with the script file.
5. If required, Packet Analyzer displays a popup for you to enter the login credentials for the NetShark that you have selected.

6. Enter the login credentials and click **OK**. This opens main window of Packet Analyzer. The capture job you specified is listed in both the **Devices** and **Files** panels. In the **Files** panel you can use the trace clip created for the selection in the NetProfiler report. You can then apply views to the trace clip as necessary to analyze traffic at the packet level.

Refer to the Packet Analyzer documentation for descriptions of the features available for analyzing the traffic.

Exporting NetShark packet information

To use the NetShark appliance to export a trace file for packets associated with a host, host pair, port, protocol, or flow reported on the NetProfiler,

1. Right-click the item to display the shortcut menu.
2. Select **Packets for this <selection>** to display a submenu.
3. Select **Export to PCAP file**. This displays another submenu.
4. Choose **From NetShark** on the submenu. If there is only one NetShark appliance sending data to the NetProfiler, and if that one appliance has only one capture job, then this choice exports the PCAP file from that appliance. Otherwise, the NetProfiler or NetExpress displays the “Export a PCAP file” popup window and identifies the NetShark appliance that will be used.
5. Select the NetShark appliance that you want to use as the source of the packet details you want to export. With a NetExpress, you can select the NetExpress itself as the source, if capture jobs are defined.
6. Click the link for the capture job that you want to export data from.
7. If you are exporting from a NetShark, the NetProfiler or NetExpress connects to the NetShark. The first time you connect to the NetShark you are prompted to approve the NetShark certificate.
8. When your browser displays a download popup, choose the options necessary for saving the file. The NetShark Web Interface displays a popup for you to enter the login credentials for the NetShark that you have selected.
9. Enter the login credentials and click **OK**. This gives you a link to download the trace file. The download may start automatically, depending on the browser and its settings.

Packet reporting and export with Cascade Sensor

The Cascade Sensor monitors the network through taps or mirror ports. It sends traffic information to the NetProfiler for display, reporting and alerting. However, the Sensor also has traffic analysis features of its own. These are described in the *Cascade Sensor User's Guide* and in the Sensor online help system.

You can use the Sensor to view information about packets associated with traffic flows reported on the NetProfiler. From within the NetProfiler or NetExpress, right-click on any host, host pair, port, protocol, or flow, wherever it is reported. This displays a menu with an option to use the Sensor to view packet data collected by any Sensor that is sending information to the NetProfiler.

Additionally, you can use the NetProfiler to connect directly to the Sensor and export a packet trace file corresponding to the NetProfiler report criteria.

This section describes accessing the Sensor from within the NetProfiler. The advantage of this approach is that the NetProfiler automatically provides the Sensor with the context for the item that you want to investigate. That is, the Sensor GUI opens with the information it needs to view packets for the item that you right-clicked on a NetProfiler report.

Viewing Sensor packet information

To use the Sensor to analyze packet-level data for a host, host pair, port, protocol, or flow reported on the NetProfiler,

1. Right-click the item to display the shortcut menu.
2. Select **Packets for this <selection>** to display the submenu.
3. Select **View in Cascade Sensor**. This displays a submenu of Sensors that are sending data to the NetProfiler.
4. Choose the Sensor that you want to use as the source of the packet details you want to view.
5. The first time you choose a Sensor as the source of the data for analysis, you will be prompted to approve the connection to the Sensor. This may also happen on subsequent uses, depending on your browser settings.
6. Approve the connection, if necessary. The browser displays the login page for the Sensor that you have selected.
7. Enter the login credentials and click **OK**. This opens Sensor Traffic Analysis > Packet View page. This page displays information about packets associated with the host, host pair, port, protocol, or flow that you right-clicked on the NetProfiler report.

Exporting Sensor packet information

To use the Sensor to export a packet trace file for packets associated with a host, host pair, port, protocol, or flow reported on the NetProfiler,

1. Right-click the item to display the shortcut menu.
2. Select **Packets for this <selection>** to display the submenu.
3. Select **Export to PCAP file**. This displays a submenu of Sensor appliances that are sending data to the NetProfiler.
4. Choose the Sensor that you want to use as the source of the packet details you want to export.
5. The first time you choose a Sensor as the source of the data for analysis, you may be prompted to approve the connection to the Sensor. This may also happen on subsequent uses, depending on your browser settings.
6. The NetProfiler connects to the Sensor. You are prompted to approve the connection and to log in to the Sensor. Enter the login credentials for the Sensor that you have selected.
7. When the Sensor displays the Packet Export Download page, click the link to initiate the download. Your browser will prompt you for a location on your local machine to save the packet trace file.

CHAPTER 14 Mitigation

This chapter describes SteelCentral™ NetProfiler and SteelCentral™ NetExpress capabilities for mitigating the affects of malicious or misconfigured traffic. It includes the following sections:

- [“Introduction,”](#) next
- [“Trusted hosts setup”](#) on page 276
- [“Switch mitigation setup”](#) on page 277
- [“Router mitigation setup”](#) on page 279
- [“Enabling mitigation plan generation”](#) on page 280
- [“Managing mitigation actions”](#) on page 281
- [“Managing mitigation plans”](#) on page 283

Introduction

The mitigation feature enables you to reduce or eliminate traffic to and from specified hosts by using the appliance to reconfigure switches and routers in your network. This feature is available when the security analytics module is enabled.

The appliance automatically generates a mitigation plan for blocking traffic by switching off switch ports or by instructing routers to discard traffic. It reports the anticipated impact of mitigation actions and allows you to select which mitigation actions are taken.

Once you set up the mitigation feature, you can view and create mitigation plans, tailor them to your network, activate them, deactivate them, and delete or save them for reuse.

The setup of the mitigation feature involves specifying:

- Trusted hosts (hosts whose traffic will not be blocked)
- Mitigation switch information
- Mitigation router information

The use of the configured mitigation feature includes managing mitigation plans and individual mitigation actions. This chapter discusses each of these topics.

Switch Mitigation

The appliance supports the use of switches for blocking traffic. It uses SNMP polling to obtain:

- MAC address-to-switch port bindings from switches
- MAC address-to-IP address bindings from routers

The appliance uses this information to determine which switch port an offending host uses. It can then use SNMP to shut down the switch port and isolate the offending host.

Switch mitigation is appropriate for situations in which you would otherwise shut down switch ports manually by disconnecting cables or by sending commands to the switch. To minimize the impact on non-offending hosts, you should use switch mitigation on access switches where practical instead of distribution switches. Generally speaking, the closer in the network topology the mitigation switch is to the offending host, the fewer other hosts will be affected by the switch port being shut down.

Router Mitigation

The appliance supports the use of routers for blocking traffic by provisioning designated routers with black hole routing instructions. These work in conjunction with the unicast Reverse Path Forwarding (uRPF) router feature to isolate specified hosts from the routed network.

What uRPF does

uRPF prevents hosts from receiving traffic from IP addresses that it cannot verify. The feature assumes that a valid packet will be received on the same interface that the router uses to return a packet to the source address. It checks the packets it receives on a uRPF-enabled interface to determine if the interface and the source address of the packet match a best return path (reverse path) in its routing table. If they match, it forwards the packet. But if the return path specifies a different interface than the interface on which the packet was received, the router discards the packet. This prevents the destination host from receiving traffic from unverifiable IP addresses on the routed network.

What black hole routing does

A black hole route prevents a host from receiving any routed traffic. When you identify a host that is sending traffic that you want to block, you can use the appliance to publish a black hole route to a mitigation router. The black hole route appears to be the best path to the offending host because it is the most specific (/32).

When the appliance publishes such a route on a designated mitigation router, the routing protocol advertises the route to other routers on the network. The other routers add it to their routing tables as the best path to the offending host.

When a router that has the black hole route receives a packet having the destination address of the offending host, it forwards the packet to the mitigation router, as instructed in the black hole route. But instead of forwarding the packet to the offending host, the mitigation router forwards it to a null interface. That is, it discards the packet so that it never reaches the offending host. This prevents the offending host from receiving any traffic (except from hosts on the same subnetwork, which are not routed).

How uRPF and black hole routing work together

The uRPF feature discards traffic that has unverifiable source IP addresses. The black hole routing technique makes the IP address of an offending host unverifiable by uRPF. This blocks the offending host from sending traffic on the routed network.

The black hole routing technique also prevents an offending host from receiving any routed traffic, whether or not the source addresses are verifiable. The combination of the two techniques completely isolates an offending host from the routed network.

Example 1: Black hole routing without uRPF enabled

1. The appliance publishes a static route on the mitigation router. On the GUI, you can specify individual host addresses or ranges of addresses to be covered by different mitigation routers. However, each route the appliance publishes on a mitigation router is a /32 route.
2. The mitigation router uses a routing protocol (e.g., OSPF) to distribute the route to other routers on the network.
3. Host A sends traffic to the offending host. The first router to receive the traffic uses the black hole route to forward the traffic to the mitigation router. The mitigation router discards the traffic.
4. The offending host sends traffic to Host A. The traffic is routed to Host A. However, the offending host cannot receive information from Host A or engage in any two-way communication.

Example 2: Black hole routing working with uRPF

1. As in Example 1, the appliance publishes a static route on the mitigation router, and the mitigation router distributes the route to other routers on the network.
2. Also as in Example 1, Host A sends traffic to the offending host. The first router to receive the traffic uses the black hole route to forward the traffic to the mitigation router, where it is discarded.
3. The offending host sends traffic to Host A.
4. When a uRPF-enabled router with the black hole route pertaining to the offending host receives the traffic, it assumes that any traffic from the offending host should use the same route as traffic back to that host. But for most network topologies, the traffic from the offending host will not match the router's reverse path to the host, because the reverse path is the black hole route. So the uRPF-enabled router discards all traffic from the offending host.

There are uncommon network topologies in which the traffic from the offending host can arrive on the port specified by the reverse path to the mitigation router and therefore be forwarded despite uRPF. For example, if there is a switch or non-uRPF-enabled router between the mitigation router and the uRPF-enabled router, and if the traffic from the offending host enters the network through that device, then the traffic can enter the uRPF-enabled router through the port specified in its reverse path route to the mitigation router. The uRPF-enabled router will forward the traffic in this case.

Configuration notes on uRPF

The uRPF feature does not have to be enabled on every router, but mitigation is more effective when uRPF is enabled on more routers. Additionally, enabling uRPF on routers near the edge of the protected network is usually more effective than on routers closer to the core.

Configuration notes on the mitigation router

You can use the appliance to publish a black hole route on a router that you designate as a mitigation router. You must enter the name and passwords of this router on the Configuration > Mitigation > Add Router page so that the appliance can publish the route.

The mitigation router must use a routing protocol such as OSPF to distribute the route to other routers. Usually, the mitigation router must be explicitly configured to redistribute static routes.

The mitigation router does not need to run uRPF, and the uRPF-enabled routers do not need to be configured to redistribute static routes. Refer to your router documentation for guidance on redistributing static routes.

Using the mitigation feature

The general procedure for using the mitigation feature is:

1. **Specify trusted hosts.** This is traffic that is to be excluded from mitigation actions, such as trusted infrastructure devices.
2. **Specify the switch mitigation setup.** This involves identifying one or more lookup routers and one or more switches. The lookup routers must have SNMP enabled.
3. **Specify the router mitigation setup.** This involves designating one or more mitigation routers and ensuring that each is set up for redistribution of static routes. The appliance must be given the names and passwords of the mitigation routers so that it can publish null routes for offending hosts on them.
4. **Enable or disable automatic mitigation plan generation.** By default, the appliance does not automatically generate mitigation plans. You can set it to generate mitigation plans for events that cause Low, Medium, or High alerts. Alternatively, you can leave automatic mitigation plan generation disabled and generate plans only when you choose to. If you typically do not take mitigation action when you receive alerts, then Riverbed recommends leaving automatic plan generation off.
5. **Work with mitigation plans and actions.** You can activate, deactivate, modify, create and delete mitigation actions and mitigation plans.

These steps are discussed in more detail in the sections that follow.

Trusted hosts setup

The appliance does not take mitigation actions against devices that you designate as trusted hosts. Trusted hosts are typically critical infrastructure devices, which you add to the appliance trusted host list on the Configuration > Mitigation > Trusted Hosts page.

The appliance automatically adds the following devices to its trusted hosts list:

- all the appliance modules and storage devices
- mitigation switches and the lookup router for switch mitigation
- mitigation routers

You can add a trusted host either by specifying it in the GUI or by importing a list of IP addresses and comments.

To add devices to the trusted hosts list

1. Go to the Configuration > Mitigation > Trusted Hosts page.
2. Click **Add....** This displays the Add Trusted Host page.
3. Enter the IP address of a host or a range of trusted hosts in CIDR format.
4. Optionally, enter a comment for future reference.
5. Click **Add** to add the host or range of hosts to the trusted hosts list.

Figure 14-1. Configuration > Mitigation > Trusted hosts page

Trusted Hosts

Trusted hosts are hosts that are exempt from mitigation.

Trusted Hosts			Add...	Import...
Host/CIDR 	Comments	Actions		
10.100.100.251	mitigation device	Edit	Delete	
10.99.18.251	mitigation device	Edit	Delete	
10.99.17.251	mitigation device	Edit	Delete	
10.99.16.251	mitigation device	Edit	Delete	
10.99.15.251	mitigation device	Edit	Delete	
10.99.14.251	mitigation device	Edit	Delete	
10.99.13.251	mitigation device	Edit	Delete	
10.99.12.251	mitigation device	Edit	Delete	
10.99.11.251	mitigation device	Edit	Delete	
10.38.129.70	profiler component	Edit	Delete	

To import a trusted hosts list

1. Create a file specifying the trusted hosts. The file must specify one IP address or CIDR block of IP addresses per line, with a comma separating the IP address from the optional comment. For example:

```
ip_address,comment
ip_address/24,comment
ip_address,comment
```

2. Go to the Configuration > Mitigation > Trusted Hosts page.
3. Click **Import....** This displays the Import Trusted Host page.
4. Enter or browse to the path to the file containing your trusted hosts list.
5. Click **Import** to add the hosts to the trusted hosts list.

Switch mitigation setup

Switch mitigation requires a lookup router and one or more mitigation switches. Information for both the lookup router and the switches is entered on the Configuration > Mitigation > Switching Setup pages.

You can add devices either by specifying them in the GUI or by importing a comma-separated-list of device information.

To add mitigation switches and lookup routers

1. Go to the Configuration > Mitigation > Switching Setup page.
2. Click **Add Device....** This displays the Add Device page.
3. Enter the required information and click **Add** to add the specified device as a mitigation switch or lookup router.

Figure 14-2. Configuration > Mitigation > Switching Setup page

Switching Setup ?

Polling Settings

Total time to poll switches (min):

Number of simultaneous scans allowed:

[Apply](#)

Devices [Actions ...](#)

Name	IP Address	Type	Last Connection State	Last Good Connection	Last Connection Attempt	Actions
<input type="checkbox"/> dc_Switch1	10.100.100.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 1:29:00 PM	Poll now Edit
<input type="checkbox"/> Hartford_Switch1	10.99.18.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 3:09:00 PM	Poll now Edit
<input type="checkbox"/> Philadelphia_Switch1	10.99.17.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 1:49:01 PM	Poll now Edit
<input type="checkbox"/> Austin_Switch1	10.99.16.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 3:29:00 PM	Poll now Edit
<input type="checkbox"/> SanFrancisco_Switch1	10.99.15.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 2:29:01 PM	Poll now Edit
<input type="checkbox"/> Columbus_Switch1	10.99.14.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 3:49:00 PM	Poll now Edit
<input type="checkbox"/> Phoenix_Switch1	10.99.13.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 2:49:01 PM	Poll now Edit
<input type="checkbox"/> LosAngeles_Switch1	10.99.12.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 1:09:00 PM	Poll now Edit
<input type="checkbox"/> Seattle_Switch1	10.99.11.251	Switch	Scan failed due to improper configuration		Jun 12, 2016 2:09:01 PM	Poll now Edit

[1](#)
[go to page](#)
[Show: 10](#) entries per page

Column descriptions

- **Name** - Host name of the mitigation device.
- **IP address** - IP address of the device.
- **Type** - Either Switch for an actionable switch or Lookup Router for a router used to look up MAC-to-IP address bindings.
- **Read community** - Community string that the appliance should use to query the device.
- **Write community** - Community string that the appliance should use to enact changes on the switch.

To import a switch mitigation device list

1. Create a file specifying the devices. Each line of the file must contain a comma-separated list of information about one device using the following format:

```
host_name, IP_address, device_type, read_only_community_string, write_community_string
```

where:

host_name - is the name of the mitigation device

IP_address - is the IP address of the device

device_type - is either SWITCH for an actionable switch or ROUTER for a router used to look up MAC-to-IP address bindings.

read_only_community_string - is the string the appliance must use to obtain information from the device

write_community_string - is the string the appliance must use to enact changes on the switch (e.g., disable or enable switch ports)

2. Go to the Mitigation > Switching Setup page.

3. Click **Import**. This displays the Import devices page.
4. Enter or browse to the path to the file containing your device list.
5. Click **Import** to add the devices to the switching device list.

Modifying switch setups

The Configuration > Mitigation > Switching Setup page provides controls in the Actions column for polling switches, editing a switch setup, and deleting a switch setup.

The appliance polls the switches periodically for the latest address-to-port mappings. However, you can instruct the appliance to update its information immediately by clicking Poll now.

Router mitigation setup

Router mitigation requires a mitigation router that can distribute static routes on the network. You can use more than one mitigation router and specify different mitigation routers to cover different ranges of IP addresses.

Figure 14-3. Configuration > Mitigation > Routing Setup page

Routing Setup

Devices for Routing Mitigation Add Router...			
Name	Router IP Address ↓	Coverage	Actions
No Data Available.			

To be fully functional, the router mitigation feature requires routers on the network to use unicast Reverse Path Forwarding (uRPF). It does not require that all routers use uRPF. However, enabling uRPF on more routers makes mitigation more effective. Also, uRPF-enabled routers near the edge of the protected network are generally more effective than uRPF-enabled routers in the core of the network.

Mitigation routers are specified on the Configuration > Mitigation > Routing Setup pages.

To add a mitigation router

1. Go to the Configuration > Mitigation > Routing Setup page.
2. Click **Add Router....** This displays the Add Router page.
3. Enter the required information. Click **Help** for a description of the fields on the page.
4. Click **Add** to add the mitigation router.

Column descriptions

- **Router name** - Host name of the mitigation router.
- **IP address** - IP address of the router.
- **Connection method** - How the appliance must connect to the router; telnet or SSH.

- **Connection port** - Which port on the router that the appliance must connect to.
- **Username** - The name that the appliance must use to log in to the router.
- **Password** - Password that the appliance must use to log in to the router.
- **Enable password** - Password that the appliance must use to enact changes on the router; also known as the privileged password.
- **Max number of routes** - Maximum number of mitigation routes that the appliance can publish on this router.
- **Router coverage** - Area of the network for which this router can mitigate. This is expressed as a list of CIDR blocks separated by commas. Enter 0.0.0.0/0 when you are using one mitigation router to cover the entire network. Trusted hosts are automatically excluded from mitigation actions.

Modifying and testing router setups

The Configuration > Mitigation > Routing Setup page provides controls in the Actions column for testing the connection to a router, editing a router setup, and deleting a router setup.

The Test action for an entry in the list causes the appliance to attempt to connect to the router in that entry and display a message indicating whether the test connection succeeded or failed.

Enabling mitigation plan generation

The feature that automatically generates mitigation plans assumes that an administrator has already specified trusted hosts and set up the switch and router connectivity necessary for mitigation.

Generating a mitigation plan has no effect on the network. For mitigation actions to take effect, you must specifically activate a mitigation plan by selecting it and entering your password. This protects the network from the risk of someone accidentally blocking traffic.

Figure 14-4. Global Settings

Global settings for all Security Policies

Event detection delay

Global Event Delay	Generate events after the Profiler has collected data for	<input type="text" value="0"/> days
New Host Delay	For a new host, don't generate any events for	<input type="text" value="0"/> days

Mitigation settings

Plan generation threshold	Create plans for events with severity equal to or higher than	<input type="text" value="None"/>
----------------------------------	---	-----------------------------------

OK Cancel

To enable the appliance to automatically generate mitigation plans

1. Go to the Behavior Analysis > Policies page Security tab.
2. Click **Global Policy Settings....** This displays the Global settings for all Security Policies page.

3. In the Mitigation settings section, select the alert level that you want to trigger the automatic generation of a mitigation plan. For example, you might want the appliance to generate a plan only when there is a High alert. None disables automatic mitigation plan generation.
4. Click **OK**.

When a mitigation plan is ready, the status is indicated in the Current Events widget on the Dashboard page as an entry in the Mitigation plan column.

The mitigation plan status can be:

- **Ready** - a mitigation plan has been generated and is ready for use
- **Pending** - a mitigation plan is being generated, but it is not yet complete
- **Updated** - an existing mitigation plan that is already in use has been updated

If the Mitigation plan column is blank for an event in the event list, it means either that the event is not eligible for mitigation or the automatic plan generation is disabled.

Managing mitigation actions

You can select one or more recommended mitigation actions to put into effect by making choices on the Mitigation Plan Detail page. Conversely, you can deactivate one or more mitigation actions by making selections on this page.

There are several ways to display the Mitigation Plan Detail page:

- Go to the Configuration > Mitigation > Plans and Actions page, select the **Plans** view, and search by host, event ID, or plan ID for the desired mitigation plan. On the list entry for the plan, click the **Edit** link.
- On a Dashboard page that is displaying a Current Events widget, click the **Ready** link in the Mitigation plans column of the event you want to mitigate.
- On an Event Detail Report page, click the **View mitigation plan** link on the Summary tab. (This is not shown if automatic mitigation plan generation is disabled.)
- On an Events Report page, click the event ID for an event you want to mitigate. This displays the Event Detail Report. Click **Mitigate** on the Event Detail report.

All four of these links display the Mitigation Plan Detail page. This page provides a summary of the plan and lists the mitigation actions. Mitigation actions are actions to block the traffic to and from specified hosts or groups of hosts.

The **Actions taken** section lists mitigation actions that have been put into effect. The **Proposed actions** section lists mitigation actions that the appliance has proposed but which have not been put into effect.

The lists of hosts in the two sections provide the following information:

- **Host** - Name of the host and host group whose traffic is to be blocked. You can right-click this entry to access a selection for running a traffic report for the host or host group.
- **Router** - The router that the appliance will use for mitigation. An inactive (gray) box indicates that router mitigation is not available.
- **Switch Port** - The switch port that the appliance will use for mitigation. An inactive (gray) box indicates that switch port mitigation is not available.

- **Affected Hosts** - The number of hosts affected by the mitigation action. This number is linked to a page that lists the addresses of the hosts that the appliance believes reside on the switch port that it has identified for the mitigation action. This provides an indication of how many other hosts may be affected when the specified switch port is shut down. Multiple hosts may be affected when the switch port is not directly connected to the host (e.g., it is connected to another switch).
- **Current** - The current impact. This displays the number of peers that this host has transmitted to or received from in the last minute and its traffic rate in packets per second for the last minute. The appliance regularly updates these figures for all proposed actions. It updates about 2000 actions per minute.
- **History** - The number of peers and packets per second of traffic reported for this host by the profile that was active at the time the host was added to the mitigation plan. This historical impact figure is not updated.
- **Comments** - This displays notes that were added to the mitigation plan.
- **Actions** - You can remove the proposed mitigation action against a host or host group from the mitigation plan by clicking **Delete**. The Actions taken section does not have an Actions column because mitigation actions must be deactivated before they can be deleted.

You can add a host to the mitigation plan by clicking **Add Host** and entering the address of the host.

Additionally, you can click **Recalculate** to have the appliance update its address and routing records immediately instead of at the next polling time.

Activating mitigation actions

Mitigation actions that have been proposed but not yet put into effect are listed in the Proposed actions sections of the Mitigation Plan Detail page. The proposed mitigation actions can be put into effect either as a group or individually.

To activate all mitigation actions on a mitigation plan

1. On the Mitigation Plan Detail page, click the applicable link on the Activate line just above the Proposed actions section:
 - **All actions** - performs all mitigation actions using both switch and router mitigation (i.e., blocks traffic to and from all hosts) listed in this section.
 - **All router actions** - mitigates traffic on all hosts listed in this section, but uses only router mitigation and not switch port mitigation.
 - **All switch actions** - mitigates traffic on all hosts listed in this section, but uses only switch port mitigation and not router mitigation.

2. When prompted, enter your password.

Note that each of these choices activates all the proposed actions, regardless of whether or not the **Router** and **Switch port** check boxes are checked in the individual entries. Each of these choices moves all the entries from the Proposed actions section to the Actions taken section.

To activate a selected mitigation action

1. Select the **Router** and/or **Switch port** check boxes for the actions to be performed.
2. Click **Commit** at the bottom of the page and enter your password when prompted.

This moves all entries with checked check boxes from the Proposed actions section to the Actions taken section. Proposed actions that were not selected (i.e., have no check boxes checked) remain in the Proposed actions section.

Deactivating mitigation actions

Mitigation actions that have been placed into effect are listed in the Actions taken section of the Mitigation Plan Detail page. These mitigation actions can be deactivated either as a group or individually.

To deactivate all mitigation actions on a mitigation plan

1. On the Mitigation Plan Detail page, click the applicable link on the Deactivate line just above the Actions taken section:
 - **All actions** - deactivates all mitigation actions (i.e., unblocks traffic to and from all hosts listed in this section).
 - **All router actions** - deactivates all router mitigation in the plan, but leaves switch port mitigation active.
 - **All switch actions** - deactivates all switch port mitigation in the plan, but leaves router mitigation active.
2. When prompted, enter your password. Each of these choices moves all the deactivated entries from the Actions taken section back to the Proposed actions section.

To deactivate selected individual mitigation actions

1. In the Actions taken section, deselect (clear) the **Router** and **Switch port** check boxes for the actions.
2. Click **Commit** at the bottom of the section and enter your password when prompted.

This moves all entries that have no check boxes checked back to the Proposed actions section. Entries with checked check boxes remain active and listed in the Actions taken section.

Managing mitigation plans

Mitigation plans can be managed from the Configuration > Mitigation > Plans and Actions page. On this page, you can activate or deactivate mitigation plans and individual mitigation actions. You can create new mitigation plans or open existing mitigation plans.

The Actions view enables you to locate mitigation plans and mitigation actions by specifying the following search criteria:

- **Mitigation device** - switch or router or both
- **Event type** - the type of event that caused the alert which resulted in the mitigation plan being generated, or all
- **Activated by** - the login name of the user who activated the mitigation plan
- **State** - the state of the mitigation plan or action: active, inactive, or all
- **Host/CIDR** - the address or block of addresses of the affected host or hosts
- **Event ID** - the Event ID is available from an Dashboard page with a Current Events widget or from the Event Reports pages.
- **Plan ID** - the identification of the mitigation plan
- **Span** - the number of seconds, minutes, hours, days, weeks or months, ending now or ending at a time and date you specify

Figure 14-5. Configuration > Mitigation > Plans and Actions page, Actions view

Plans and Actions ?

Search Criteria

Mitigation Device: Host/CIDR: Span: day(s)

Policy: Event ID:

Activated by: Plan ID:

State:

Show:

End: ☒ Now ☐ On

View: ☐ Plans ☒ Actions

Switch Action

<input type="checkbox"/>	Host +	Group	Method	Device	Plan ID	Event ID	Policy	State	Activated on	Activated by	Actions
<input type="checkbox"/>								Inactive			Edit Delete

Working with Plans and Actions

You can view the results of a search either by Plans or by Actions. In both views, the information can be sorted in ascending or descending order by any column except the Actions column.

Plans view

When viewing the results by Plans, you can use the following controls:

- **Activate Selected** and **Deactivate Selected** activate and deactivate mitigation plans. This activates or deactivates all actions in the selected plans.
- **Delete** to delete an entire mitigation plan.
- **Edit** to open the Mitigation Plan Detail page, where you can modify or recalculate the plan.
- **Event ID** link to open the Event Detail report.

Actions view

When viewing the results by Actions, you can use the following controls:

- **Activate Selected** and **Deactivate Selected** to activate and deactivate mitigation actions. This activates or deactivates only the selected actions.
- **Delete** to delete a mitigation action.
- **Host** entry that can be right-clicked to display a selection for a traffic report for the host.
- **Edit** to open the Mitigation Plan Detail page, where you can modify or recalculate the plan.
- **Event ID** link to open the Event Detail report.

To create a mitigation plan

1. Go to the Configuration > Mitigation > Plans and Actions page and choose **Plans** view.

2. Click **Create plan**. This displays an empty Mitigation Plan Detail page.
3. In the Proposed actions section, click **Add Host**.
4. Enter the name of the host and click **Add**. The appliance creates an entry for the host in the list in the Proposed actions section and proposes the mitigation action.
5. Add more hosts, as necessary.
6. If you want to recheck the impact on current traffic before activating the plan, click the **Refresh** link beside the Current column.
7. When you are ready to activate the plan, either:
 - Click the appropriate Activate link: **All actions**, **All router actions**, or **All switch actions**, or
 - Select the appropriate check boxes for each mitigation action and then click **Commit** in the Proposed actions section.
8. When prompted, enter your password.

The appliance performs the selected mitigation actions and moves their entries to the Actions taken section.

CHAPTER 15 Appliance Security

- [“Overview,”](#) next
- [“Password Security”](#) on page 288
- [“Security Compliance”](#) on page 289
- [“Encryption Key Management”](#) on page 296
- [“Replacing SSH keys”](#) on page 298
- [“Replacing SSL certificates”](#) on page 299

Overview

The NetProfiler and NetExpress appliances are secured by strong password controls, restricted access and encrypted communication with other appliances. These features are controlled by three Appliance Security pages that are accessible from the Configuration menu:

- Password Security
- Security Compliance
- Encryption Key Management

This chapter describes these features. Additional security-related features include:

- Password-protected email server and encrypted time server configuration on the Configuration > General Settings page
- Audit Trail Report on the System > Audit Trail page
- Account privilege levels for assigning new accounts on the Configuration > Account Management > User Accounts page

Password Security

On the Configuration > Appliance Security > Password Security page, a user logged into an Administrator account can specify password security settings for all users. This page has three sections:

Figure 15-1. Configuration > Appliance Security > Password Security page

Password Security ⓘ

Password Requirements

Minimum number of characters:	<input type="text" value="6"/>
<input type="checkbox"/> Require mixed case	
<input type="checkbox"/> Require non-alphanumeric characters	
Number of passwords to remember to prevent repeats:	<input type="text" value="1"/>
<input type="checkbox"/> Enable password aging	
Number of days before password expiration:	<input type="text" value="90"/>

Log-in Settings

<input type="checkbox"/> Allow only one log-in per user name/password combination	
<input type="checkbox"/> Force password change on first log-in	
Number of log-in attempts before account is locked:	<input type="text" value="3"/>
Number of minutes to keep an account locked:	<input type="text" value="30"/>
<input type="checkbox"/> Prevent user 'admin' from being locked out via DoS attack.	
Log-in splash screen display:	<input type="text" value="No splash screen"/>
Upload new log-in splash screen:	<input type="button" value="Browse..."/> No file selected.
Add login text:	<div style="border: 1px solid #ccc; height: 40px;"></div>

Inactivity Timeout

<input type="checkbox"/> Enable maximum inactivity timeout:	<input type="text" value="15"/> minute(s)
<input checked="" type="checkbox"/> Override timeout for auto-refreshing pages (status/dashboards).	

Changes will apply to all future account log-ins.
Currently logged-in accounts will need to log out before these changes apply.

[Configure](#)

Password Requirements – specifies password length, case usage, and requirement for non-alphabetic characters. Specifies the number (from 1 to 16) of previous passwords the appliance should save and test to ensure that the user is not recycling a small set of passwords. Also specifies the lifespan of a password. When a password expires, the user is forced to change it upon their next login.

Login Settings – allows you to:

- Limit the number of user sessions to one per name/password combination.
- Require users of new accounts to change their password on their first log in.
- Specify the number of consecutive failed login attempts the appliance allows before disabling logins for an account.
- Specify how long logins are disabled on an account after the allowed number of failed login attempts has been exceeded. If a user needs access before the lockout period has expired, the Administrator can edit the account profile to specify a new password for the account.

- Exempt the admin account from being locked out by repeated unsuccessful login attempts.
- Specify if the splash screen is dismissed automatically after 5 seconds, is displayed until the user clicks Acknowledge, or is not displayed.
- Specify the path to a splash screen graphic file, such as a company banner in a gif, jpg, png or tiff file. NetProfiler uploads the file and saves it until it is overwritten by a subsequent splash screen file upload. The file can be up to 1 Megabyte in size. Additional file formats are also supported: aiff, jb2, jp2, jpc, jpf, pad, swc, swf, wbmp and xbm.
- Add text to be displayed to a user before they log in.

Inactivity Timeout – specifies how long an account can remain inactive before being automatically logged off.

- This global setting can be overridden by a shorter time set for an individual user account, but not by a longer time.
- When the appliance is in the Strict Security mode, this setting is automatically limited to no more than 10 minutes.
- The timeout can be overridden when the appliance is displaying the main pages used for monitoring the network.

Settings made on this page are linked to the settings made on the Global Account Settings page. To view that page, go to the Configuration > Accounts Management > User Accounts page and click Settings.

Security Compliance

The Configuration > Appliance Security > Security Compliance page controls security features that are used to comply with various contractual and regulatory requirements. The page has three sections:

- Operational modes – control the security posture of the appliance by automatically enabling sets of security features and disabling certain types of access to the appliance.
- Accounts – controls system account access and passwords.
- Access – controls remote access to the appliance.

Changes made to the settings in these sections are not applied to the appliance configuration until you click **Configure Now** at the bottom of the page.

Note: Do not change the Shell Access selection in the Accounts section unless you understand the impact. Shell access cannot be restored once it is disabled.

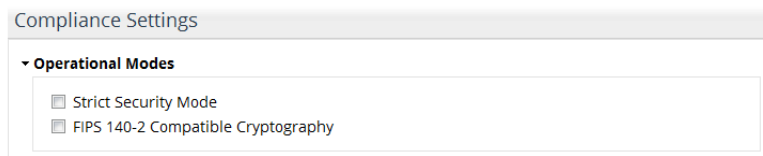
Operational modes

The security posture of the appliance is determined by its operational mode. There are four operational modes that control the security features:

- Standard
- Strict Security
- FIPS 140-2 Compatible Cryptography
- Strict Security and FIPS 140-2 Compatible Cryptography.

Figure 15-2. Configuration > Appliance Security > Security Compliance page Operational Modes section

Security Compliance ⓘ



These operational mode selections are independent of the shell access selection. The effects of the shell access selections (Shell Enabled, Challenge Mode, Shell Disabled) are described in the Account Access topic.

Standard Security

The appliance is in the standard security operational mode when neither the Strict Security mode nor FIPS 140-2 Compatible Cryptography are selected on the Configuration > Appliance Security > Security Compliance page. When neither of these options are selected, security features can be chosen individually. In the Strict Security mode and FIPS 140-2 Compatible Cryptography mode, more secure configurations are selected automatically and less secure features are disabled.

Strict Security Mode

When the Strict Security mode is selected on the Configuration > Appliance Security > Security Compliance page, the appliance:

- Disables the use of certain features.
- Selects enhanced password protection.
- Restricts access to the appliance.

Disabled features

The Strict Security mode prevents the use of the following features:

- Reporting API access control list – the ACL section of the Configuration > Integration > API Authorization page is disabled. This prevents scripts from bypassing the login requirements when accessing the reporting API. Tools that must access the reporting API while the appliance is in the Strict Security mode must be able to handle the login page.
- Vulnerability scanning setup – the Configuration > Integration > Vulnerability Scanning setup page is disabled and not displayed. The appliance cannot access any vulnerability scanners while it is in the Strict Security mode.
- Mitigation – All Configuration > Mitigation pages are disabled and not displayed.
- ODBC DB Access – the Configuration > Account Management > ODBC DB Access page is disabled and not displayed.

Password protection

The Strict Security mode automatically selects the following global password protection options. Some settings can be manually overridden to provide a higher level of security, but not a lower level. Other settings, as noted below, cannot be changed while the appliance is in the Strict Security mode.

- Minimum number of characters: 8; Can be set to a number greater than 8, but not lower than 8.
- Require mixed case; Cannot be changed while the Strict Security mode.

- Require non-alphanumeric characters; Cannot be changed while the Strict Security mode.
- Remember 12 prior passwords; Can be set to a number greater than 12, but not lower than 12.
- Enable password aging; Cannot be changed while the Strict Security mode.
- Number of days before password expiration: 60; Can be set to a number lower than 60, but not greater than 60.
- Force password change on first log-in; Cannot be changed while the Strict Security mode.
- Number of attempts before account locked: 3; Can be set to a number lower than 3, but not greater than 3.
- Number of minutes to keep account locked: 30; Can be set to a number greater than 30, but not lower than 30.

These settings can be viewed on the Configuration > Appliance Security > Password Security page. They are also visible when you click Settings on the Configuration > Account Management > User Accounts page.

Access restrictions

The Strict Security mode also automatically:

- Sets the inactivity time out for sessions on the console port and SSH connections to the Primary port to 10 minutes and limits login attempts to these ports to 3.
- Disables Ctrl+Alt+Delete on the console.
- Implements additional firewall rules restricting source routed packets and some ICMP requests.

FIPS 140-2 Compatible Cryptography

When the FIPS 140-2 Compatible Cryptography option is selected on the Configuration > Appliance Security > Security Compliance page, the appliance uses FIPS 140-2 Level 1 encryption, which is approved for use by the U.S. government for Sensitive (but unclassified) information.

Additionally, selecting the FIPS 140-2 Compatible Cryptography option has the following effects:

- Product updates – the System > Update page displays a note that product updates are not available while in the FIPS 140-2 Compatible Cryptography mode.
- NTP encryption – In the Time Configuration section of the Configuration > General Settings page, NTP connections must use either SHA1 encryption or no encryption. Any NTP servers that are currently configured to use MD5 encryption will be disconnected when the FIPS 140-2 Compatible Cryptography mode is enabled.

Note: There is no notification when switching to the FIPS 140-2 Compatible Cryptography mode disconnects NTP connections using MD5 encryption.

- In the SNMP MIB Configuration section of the Configuration > General Settings page, the settings are modified as follows:
 - If the SNMP MIB Configuration had been set to use SNMPv3 with Authentication and Privacy, then the settings are not changed when the FIPS 140-2 Compatible Cryptography mode is enabled.
 - If the SNMP MIB Configuration had been set to anything else (SNMPv1, SNMPv2, SNMPv3 with No Authentication/No Privacy or Authentication/No Privacy), then the SNMP server of the appliance is switched off when the FIPS 140-2
 - Compatible Cryptography mode is enabled.
 - If the SNMP server of the appliance had been switched off, then it remains off when the FIPS 140-2
 - Compatible Cryptography mode is enabled.

- Vulnerability scanning setup – the Configuration > Integration > Vulnerability Scanning setup page is disabled and not displayed.
- Mitigation – All Configuration > Mitigation pages are disabled and not displayed.
- ODBC DB Access – the Configuration > Account Management > ODBC DB Access page is disabled and not displayed.

Note: TLSv1 must be enabled on your web browser in order to connect to the appliance when it is in the FIPS 140-2 Compatible Cryptography mode.

Strict Security Mode with FIPS 140-2 Compatible Cryptography

When both the Strict Security mode and FIPS 140-2 Compatible Cryptography are enabled, the appliance is restricted to the limitations of each. The combined effects of enabling both options are:

- Reporting API access control list – the ACL section of the Configuration > Integration > API Authorization page is disabled. This prevents scripts from bypassing the login requirements when accessing the reporting API. Tools that must access the reporting API while the appliance is in the Strict Security mode must be able to handle the login page.
- NTP encryption – In the Time Configuration section of the Configuration > General Settings page, NTP connections must use either SHA1 encryption or no encryption. Any NTP servers that are currently configured to use MD5 encryption will be disconnected when the FIPS 140-2 Compatible Cryptography mode is enabled.

Note: There is no notification when switching to the FIPS 140-2 Compatible Cryptography mode has disconnected NTP connections using MD5 encryption.

- In the SNMP MIB Configuration section of the Configuration > General Settings page, the settings are modified as follows:
 - If the SNMP MIB Configuration had been set to use SNMPv3 with Authentication and Privacy, then the settings are not changed when the FIPS 140-2 Compatible Cryptography mode is enabled.
 - If the SNMP MIB Configuration had been set to anything else (SNMPv1, SNMPv2, SNMPv3 with No Authentication/No Privacy or Authentication/No Privacy), then the SNMP server of the appliance is switched off when the FIPS 140-2
 - Compatible Cryptography mode is enabled.
 - If the SNMP server of the appliance had been switched off, then it remains off when the FIPS 140-2
 - Compatible Cryptography mode is enabled.
- Password protection – increased as described above.
- Product updates – the System > Update page is disabled and not displayed.
- Vulnerability scanning setup – the Configuration > Integration > Vulnerability Scanning setup page is disabled and not displayed.
- Mitigation – All Configuration > Mitigation pages are disabled and not displayed.
- ODBC DB Access – the Configuration > Account Management > ODBC DB Access page is disabled and not displayed.

Accounts

The Accounts section enables you to specify a shell access mode and to change the passwords of system accounts.

Figure 15-3. Configuration > Appliance Security > Security Compliance page Accounts section

▼ Accounts

Shell Access: Shell Enabled ▼

[-] User Accounts

Login enabled	Type	Username	Action
<input checked="" type="checkbox"/>	Boot Loader	bootloader	Change Password
<input checked="" type="checkbox"/>	System	root	Change Password
<input checked="" type="checkbox"/>	System	admin	Change Password
<input checked="" type="checkbox"/>	System	mazu	Change Password
<input checked="" type="checkbox"/>	System	dhcp	Change Password
<input type="checkbox"/>	Challenge	support	Edit Account

The User Accounts list displays only system accounts. It does not include user accounts for the web user interface.

When the Shell Access mode is set to Shell Enabled, you can enable or disable logins individually for each system account. When you switch to a different Shell Access mode, access is restricted.

There are three Shell Access modes:

- Shell Enabled
- Challenge Mode
- Shell Disabled

It is extremely important to understand the effects of changing the Shell Access mode before doing it. Some effects are irreversible.

Shell Enabled

The appliance is shipped with shell access enabled. Shell access is not required for normal operation of the appliance. All routine operational features are available from the web user interface. However, shell access is required for integrating the appliance with other assets in your network and for troubleshooting in the event of a problem.

While in the Shell Enabled mode, you can enable or disable the following system accounts individually and change their passwords:

- bootloader - used strictly to manage the boot loader password, for added security. The boot loader controls what image and options the operating system is loaded with. There is no login access to this account.
- root - accessible only through ssh from other modules in an Enterprise NetProfiler; not ssh accessible otherwise; has shell access from the console if login is enabled.
- admin - accessible only through the console port; for initial setup only; no shell access; login can be disabled.
- mazu - accessible through ssh; has shell access unless disabled.
- dhcp - accessible through ssh using keys and not password.
- support - for the “challenge and response” user. When Challenge Mode is enabled, the user can gain shell access provided they can pass the challenge, which requires a code from Riverbed Support. The account name can be changed to a user name other than “support.”

Challenge Mode

The Challenge Mode is the condition in which access to the appliance is limited to a single user account, and access to that account cannot be gained without providing the correct response to a challenge question from the system. The response must be obtained from Riverbed Support. Riverbed Support provides the response to only those individuals authorized to receive it.

The Challenge Mode restricts user operations to only features that are available from the web user interface. Access to the command line functionality is available to only those authorized to use the challenge account.

The default name for the challenge account is “support.” A challenge account user can change the name of the account as well as the password. Additionally, the support account name can be changed on the Configuration > Appliance Security > Security Compliance page. In the Accounts section, click the Edit Account link in the Action column.

Once the appliance has been switched to the Challenge Mode, it can be placed back into the Shell Enabled mode by only the Challenge account user. It cannot be restored to the Shell Enabled mode by use of the web user interface.

Placing the appliance in the Challenge Mode has the following effects:

- The support account becomes the only means of user access to the shell. This account is available only when the appliance is in the Challenge Mode.
- Password-based access is disabled for all system accounts.
- The NetProfiler or NetExpress appliances cannot download updates to Cascade Sensor or Flow Gateway appliances that are running in Challenge Mode.

Note: If you lose your support account password, you can change it on the Configuration > Appliance Security > Security Compliance page.

Shell Disabled

The Shell Disabled mode permanently disables login access to the shell. This is useful in environments that must not allow any form of shell access.

Note: Switching to the Shell Disabled mode is irreversible. The only way to regain access to the shell after it has been disabled is by reloading the software and starting over from a fresh installation.

Access

The Access section of the page controls ODBC access to the appliance database and remote access to the appliance by other devices.

ODBC access

The Enable ODBC Access option allows other systems to access the database of the appliance if they have been set up as database users on the Configuration > Account Management > ODBC DB Access page. Deselect this option to prevent ODBC access to the appliance database and to hide the Configuration > Account Management > ODBC DB Access page.

Figure 15-4. Configuration > Appliance Security > Security Compliance page Access section

▼ Access

☐ Enable ODBC Access
☐ Enable SSLv3 Access

Remote Access

☒ Allow Web access to everyone
☐ Restrict Web access to:
 Comma-separated list of IP addresses or CIDR blocks.

☒ Allow SSH access to everyone
☐ Restrict SSH access to:
 Comma-separated list of IP addresses or CIDR blocks.

Configure Now

SSLv3 access

The Enable SSLv3 Access option allows other systems to access NetProfiler or NetExpress using SSLv3. This option is deselected by default because of SSLv3 vulnerabilities. If the FIPS 140-2 operational mode is selected, this option is set to off and is inactive (grayed out).

Some programs, such as ADConnector 1.5, require SSLv3 access.

Remote access

This section allows you to restrict access to the appliance by web browsers and SSH connections.

Restrict Web access to – allows you to specify the IP addresses of hosts and devices that are allowed to access the appliance using port 80 (HTTP) redirect and port 443 (HTTPS). Anyone attempting to use a web browser to connect to the NetProfiler appliance from a host outside the specified addresses will be denied access.

Restrict SSH access to – allows you to specify the IP addresses of hosts and devices that are allowed to access the appliance using port 22 (SSH). Anyone attempting to SSH to the NetProfiler appliance from a host outside the specified addresses will be denied access.

The permitted access is specified as a comma-separated list of IP addresses or address ranges in CIDR format.

Note: Ensure that the IP address of your own computer is included in the list for web access or SSH access. If you do not include your own address, you will be unable to access the appliance except through the console port.

Note: On the Enterprise NetProfiler appliance, restricting access to the UI module automatically restricts all access to the other modules. That is, the devices with addresses you list will be permitted access to the UI module but the other modules will be completely inaccessible except to one another as required for operation.

Encryption Key Management

SteelCentral appliances use encryption for communicating with:

- Users
- Sources of user identity information (Active Directory Domain Controllers)
- Other SteelCentral products

This requires encryption keys and certificates for each type of communication. Encryption keys and certificates are managed on the Configuration > Appliance Security > Encryption Key Management page.

SteelCentral appliances are shipped with default encryption certificates so that the appliances to interoperate when installed. Many customers replace the default certificates as a security precaution. However, SteelCentral appliances cannot communicate with one another while the certificate for that communication is being replaced.

Displays and controls on the page

The Encryption Key Management page has two tabs:

- **Local Credentials** – lists the keys and certificates that this appliance is using.
- **Trusted Certificates** – lists the trusted CA (Certificate Authority) certificates that this appliance trusts for communicating with other SteelCentral products. When the other appliance is using a self-signed certificate, that certificate must be listed here because it is itself the CA.

Local Credentials

The Local Credentials tab lists the types of certificates installed in the appliance you are logged in to, the dates for which they are valid, the encryption algorithm and signature, and actions that you can take on this tab.

Figure 15-5. Configuration > Appliance Security > Encryption Key Management page Local Credentials tab

Encryption Key Management

Riverbed products encrypt flows, using a shared, pre-installed certificate by default. For improved security, it is recommended that this interface be used to either manually install or automatically generate new, custom certificates for all defaults.

Local Credentials

Trusted Certificates

Type	Not Before	Expires on	Encryption	Signature	Actions
SSH Key (root)	--	--	rsaEncryption (2048 bit)		Select...
SSH Key (mazu)	--	--	rsaEncryption (2048 bit)		Select...
MNMP SSL Certificate	Jun 12, 2012	Jun 10, 2022 (5 years)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...
Identityd SSL Certificate	Jun 10, 2016	Jun 10, 2017 (12 months)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...
Apache SSL Certificate	Jun 10, 2016	Jun 10, 2017 (12 months)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...

⏪

⏩

1

⏪

⏩

go to page

1

Show: 20 entries per page

The columns list credentials as follows:

Type – type of credential: key or certificate

- SSH – private keys for shell access
- MNMP – SSL certificate for communication with other SteelCentral appliances
- Identityd – SSL certificate for communicating with user identity sources: Mazu AD Connector 1.5 and Cascade AD Connector 2.0.

- Apache – SSL certificate for the web server for sessions with users' web browsers

Not Before – date on which the certificate became valid

Expires On – date after which the certificate is no longer valid

Encryption – encryption algorithm and strength

Signature – type of certificate signature

Actions – actions that can be taken for the credentials.

- For SSH keys:
 - View Public Key – displays the public key that the appliance sends while connecting to other devices that need to be authenticated.
 - Regenerate Key Pair – regenerates the private key/public key pair.
 - Change Private Key – opens a window in which you can replace the current key.
 - Download Public Key – downloads this appliance's public key to a location you specify.
- For SSL certificates:
 - View Certificate – displays the certificate that the appliance sends while connecting to other devices.
 - Regenerate Key/Certificate – regenerates the private key and the self-signed certificate with the suitable certificate extensions for its use.
 - Change Key/Certificate – opens a window in which you can paste in a new private key and certificate.
 - Download Certificate – downloads this appliance's certificate to the system a location you specify.

Trusted Certificates

This tab lists the trusted CA certificates that this appliance should trust while communicating with other SteelCentral products. When the other appliance's certificate is issued by a chain of CAs, the entire chain of CAs up to the root CA should be placed here. When the other appliance's certificate is self-signed, it should be placed here because it is itself a CA.

Figure 15-6. Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab

Encryption Key Management ?

Riverbed products encrypt flows, using a shared, pre-installed certificate by default. For improved security, it is recommended that this interface be used to either manually install or automatically generate new, custom certificates for all defaults.

Local Credentials		Trusted Certificates				
Description	Not Before	Expires on	Encryption	Signature	Actions	
/CN=Mazu	Oct 2, 2006	Sep 29, 2016 (3 months)	rsaEncryption (1024 bit)	md5WithRSAEncryption	Select...	
/CN=Cascade MNMP Default Certificate/O=Riverbed Te...	Jun 12, 2012	Jun 10, 2022 (5 years)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...	
/C=US/ST=Massachusetts/O=Riverbed Technology, Inc....	Mar 23, 2016	Mar 16, 2046 (2 decades)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...	
◀ ◁ 1 ▷ ▶ go to page <input type="text" value="1"/> Show: <input type="text" value="20"/> entries per page						
Add New Certificate						

The columns list credentials as follows:

Description – either a user-defined comment or the certificate's subject (Distinguished Name)

Not Before – date on which the certificate became valid

Expires On – date after which the certificate is no longer valid

Encryption – encryption algorithm and strength

Signature – type of certificate signature

Actions – actions that can be taken for the credentials:

- **View Certificate** – displays the CA certificate that the appliance uses to verify the certificate of the appliance that is connecting to it.
- **Change Entry** – opens a window in which you can modify the description of this CA certificate and/or paste in a new CA certificate. If you leave the description blank, the subject of the CA certificate is displayed as the description.
- **Download Certificate** – downloads this appliance's CA certificate to a location you specify.
- **Delete Certificate** – deletes the certificate.

Additionally, the tab has an **Add New Certificate** button. This opens a window in which you can add the CA certificate for an additional appliance.

Replacing Keys and Certificates

The certificate that secures communication between SteelCentral appliances is the MNMP certificate. It is normally not necessary to regenerate MNMP certificates in all interconnected SteelCentral products. Typically only the NetProfiler or NetExpress MNMP certificate is regenerated and the new certificate is given to all Sensor, NetShark or Flow Gateway appliances that are sending data to the NetProfiler or NetExpress appliance. However, you can regenerate all the certificates. The process is the same, although the other appliances have no identityd certificate and the NetShark web user interface is somewhat different. Each appliance (including the NetShark appliance) that generates a new self-signed certificate must have its new certificate installed in every other SteelCentral appliance that communicates with it.

The sections that follow provide procedures for replacing SSH keys and SSL certificates on the Configuration > Appliance Security > Encryption Key Management page.

Replacing SSH keys

SteelCentral shell accounts are secured by SSH. The SSH private key-public key pair is randomly generated in each SteelCentral appliance at the time it is installed. There are no default SSH keys.

The appliance uses the SSH public key to connect to a backup server for running backups. Additionally, the Enterprise NetProfiler uses it for communication between modules.

You can replace an SSH key pair either by regenerating them or by replacing the current pair with a pair obtained from another source.

Regenerating an SSH key pair

To regenerate a key pair,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the shell account of interest, choose the **Regenerate Key Pair** action.

3. Select **View Public Key** and observe that it has changed.

On an Enterprise NetProfiler, the new public SSH key is automatically distributed to all modules.

Changing SSH key pair

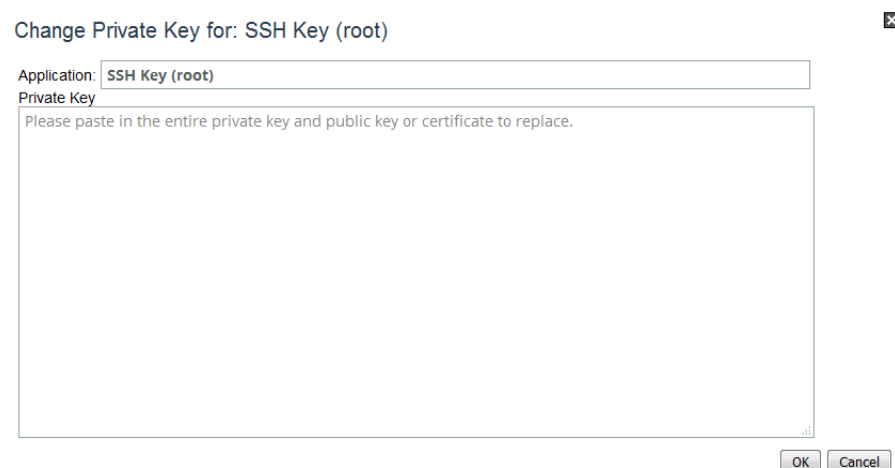
To change an SSH private key-public key pair,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the shell account of interest, choose the **Change Private Key** action. This opens a window into which you can paste a new private key.

When you copy the private key from the file where it is stored, be sure to include the header and footer lines:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEAtMUjEKBf5m9hq7mdSasWiYcB2D3qa1mGeRT/7lPkpGbewNr1
...
CeNBbPMkGZONosCnmZvSycY/wFoslx9ozPPG/dRQHGmm7z6Ktw==
-----END RSA PRIVATE KEY-----
```

Figure 15-7. Change Private Key for SSH



3. Paste the key into the window and click **OK**. This installs the new private key. The private key includes a public key within it, so this authorizes the public key as well.
4. Select **View Public Key** and observe that it has changed.

Replacing SSL certificates

The NetProfiler and NetExpress appliances secure the following SSL connections using certificates:

- MNMP – NetProfiler or NetExpress communicating with other SteelCentral appliances
- Identityd – NetProfiler or NetExpress communicating with the Cascade ADConnector program to obtain user information from Microsoft Active Directory domain controllers
- Apache – NetProfiler or NetExpress communicating with users' web browsers

The certificates that are currently in use can be replaced by:

- Regenerating the certificate – The NetProfiler or NetExpress appliance generates a new certificate.
- Replacing the certificate – The current certificate can be replaced by a CA-signed or self-signed certificate that you obtain or generate outside of the SteelCentral appliance.

There are slightly different procedures for replacing each type of certificate, as described below. You can locate the procedure for your task and skip the others.

Replacing the MNMP SSL certificate

Before you replace the MNMP certificate, go to the System > Devices/Interfaces page Devices tab and identify all the Cascade Sensor, Flow Gateway and NetShark appliances that connect to this appliance. These should be noted because after the MNMP SSL certificate in this appliance has been replaced, each of those appliances must have their Trusted Certificates list updated before they can connect to this appliance.

The connected appliances are displayed at the top level of the list on the Devices & Interfaces (Tree) tab. The tree view may be disabled to improve performance if the list is very large. Click the **Show all Devices and Interfaces** button to display the complete list. Note that the appliance performance may be impacted while a very large list is displayed.

Regenerating the MNMP SSL certificate

The Regenerate action creates a new private key and self-signed certificate. Note that when you regenerate the MNMP certificate, the NetProfiler or NetExpress will not be accessible to other SteelCentral appliances until you have installed the certificate in their Trusted Certificates section.

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the MNMP SSL Certificate, choose **Regenerate Key/Cert** from the Actions menu.

This generates a new certificate and a new private key. The certificate contains the new public key.

Figure 15-8. Configuration > Appliance Security > Encryption Key Management page Local Credentials tab

Encryption Key Management ?

Riverbed products encrypt flows, using a shared, pre-installed certificate by default. For improved security, it is recommended that this interface either manually install or automatically generate new, custom certificates for all defaults.

Local Credentials		Trusted Certificates			
Type	Not Before	Expires on	Encryption	Signature	Actions
SSH Key (root)	--	--	rsaEncryption (2048 bit)		Select...
SSH Key (mazu)	--	--	rsaEncryption (2048 bit)		Select...
MNMP SSL Certificate	Jun 12, 2012	Jun 10, 2022 (5 years)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...
Identityd SSL Certificate	Jun 10, 2016	Jun 10, 2017 (12 months)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...
Apache SSL Certificate	Jun 10, 2016	Jun 10, 2017 (12 months)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	View Certificate
					Regenerate Key/Cert
					Change Key/Cert
					Download Certificate

1 go to page 1 Show: 20 entries per page

3. Choose either **Download Certificate** or **View Certificate** from the Actions menu.
 - If you choose **Download Certificate**, follow the prompts to specify a location where the certificate file can be downloaded. You can then copy the certificate from the file.
 - If you choose **View Certificate**, copy the certificate from the window.

- On each SteelCentral appliance that communicates with this appliance, go to the Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab.

Figure 15-9. Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab

Encryption Key Management

Riverbed products encrypt flows, using a shared, pre-installed certificate by default. For improved security, it is recommended that this interface be used to either manually install or automatically generate new, custom certificates for all defaults.

Local Credentials

Trusted Certificates

Description	Not Before	Expires on	Encryption	Signature	Actions
/CN=Mazu	Oct 2, 2006	Sep 29, 2016 (3 months)	rsaEncryption (1024 bit)	md5WithRSAEncryption	Select...
/CN=Cascade MNMP Default Certificate/O=Riverbed Te...	Jun 12, 2012	Jun 10, 2022 (5 years)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...
/C=US/ST=Massachusetts/O=Riverbed Technology, Inc....	Mar 23, 2016	Mar 16, 2046 (2 decades)	rsaEncryption (2048 bit)	sha512WithRSAEncryption	Select...

⏪

⏩

1

⏪

⏩

go to page

1

Show:


20

 entries per page

Add New Certificate

- Click **Add New Certificate** to open a window into which you can paste the new NetProfiler or NetExpress MNMP certificate.
- Paste the new certificate into the Key/Cert field.
- Optionally, enter a description to be displayed in the Trusted Certificates list. Leave it blank if you want to use the certificate's subject. This can be changed later using the **Change Entry** action.

Figure 15-10. Configuration > Appliance Security > Encryption Key Management > Add New Public Certificate page

Add New Public Certificate


Description:
Certificate

- Click **OK** and confirm that the certificate is listed on the Trusted Certificates tab. The appliance will reestablish contact with the NetProfiler or NetExpress automatically within a few minutes.

Replacing the MNMP certificate with a CA-signed certificate

To minimize the time that the NetProfiler or NetExpress appliance is inaccessible, it is recommended that you set up all the Trusted Certificates first, and then replace the MNMP private key in the NetProfiler or NetExpress.

Prerequisites

A CA-signed certificate may include a hierarchical chain of certificates from several certification authorities (the certification chain). All these CA certificates must all be added as individual entries in the Trusted Certificates section of this appliance and all the SteelCentral appliances that connect to it.

Depending on your CA, you may receive these as a concatenation in one file and need to separate them before placing them in the Trusted Certificates sections. If you add more than one CA certificate at a time, the appliance will use the first one it finds, which may not be the correct one.

Alternatively, your CA may provide certificates in separate files. In this case, ensure that you have each certificate in the entire CA chain and not just the end entity certificate.

The end entity certificate and its private key must be pasted into the Local Credentials section of the NetProfiler or NetExpress appliance, and the entire CA certificate chain must be pasted into the Trusted Certificates section of the NetProfiler or NetExpress appliance and every Sensor, Flow Gateway and NetShark appliance that connects to it.

The certificates must include the following certificate extensions:

- X.509v3 Subject Key Identifier
- X.509v3 Authority Key Identifier

These are necessary in case the CA certificate is renewed and in case more than one CA certificate has the same subject.

Part 1 – Trusted Certificates

For each SteelCentral appliance that is to communicate with the NetProfiler or NetExpress,

1. Copy the first certificate of the CA certificate chain, including the BEGIN and END statements. The certificate will be in a format such as:

```
-----BEGIN CERTIFICATE-----
MIIBsTCCARqgAwIBAgIJJA0QvgxZRcO+ZMA0GCSqGSIb3DQEBAUAMA8xDTALBgNVBAMTB1henUwHhcNMDYxMDAyMTY0MzQxWmcNMTYwOTI5MTY0MzQxWjAPMQ0wCwYD05BPDxKbb8Ic6HBPDxKbb8Ic6HWpTJpzs
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdeYZUSgpyAcws5PDyr2GVFMI3dfPn128hVavIkr8r05BPDxKbb8Ic6HWpTZMA0GCSqGSIb3DQEBAUAM
A8xDTNMTYwOTI5MTY0MzQxBA
-----END CERTIFICATE-----
```

2. Go to the Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab.
3. Click **Add New Certificate** to open a window into which you can paste the CA-signed certificate.
4. Paste the certificate into the Certificate field.
5. Optionally, enter a description to be displayed in the Trusted Certificates list. Leave it blank if you want to use the certificate's subject. This can be changed later using the **Change Entry** action.
6. Click **OK** and confirm that the certificate is listed on the Trusted Certificates tab.
7. Repeat Steps 1 through 6 for each CA certificate in the chain until all CA certificates in the chain have been added as separate entries on the first SteelCentral appliance that communicates with the NetProfiler or NetExpress.
8. Then perform Steps 1 through 7 on all other SteelCentral appliances that connect to the NetProfiler or NetExpress appliance.

9. After all the connecting SteelCentral appliances have all the CA certificates, perform Steps 1 through 6 on this appliance.

Part 2 – Local Certificate and private key

After each certificate in the CA chain has been added to each appliance in your SteelCentral deployment as a trusted certificate, the final step is to add the end entity certificate and the private key as the Local Credentials for your NetProfiler or NetExpress.

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the MNMP SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the MNMP certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the MNMP certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the end entity certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCA+jgAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBAQUAMEIxCzAJBgNV
...
xnRRtSSStpDwBRwrPBX9wiih7X13I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----
```

If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

Replacing the MNMP certificate with a self-signed certificate

The procedure for a self-signed certificate is the same as for a CA-signed certificate except that you do not have to add the CA chain of certificates to the Trusted Certificates section. All you need to add is the self-signed certificate.

Part 1 – Trusted Certificate

For each SteelCentral appliance that is to communicate with the NetProfiler or NetExpress appliance,

1. Copy the self-signed certificate, including the BEGIN and END statements. The certificate will be in a format such as:

```
-----BEGIN CERTIFICATE-----
MIIBsTCCARqgAwIBAgIJAOqvgxZRcO+ZMA0GCSqGSIb3DQEBAUAMA8xDTALBgNVBAMTBElhenUwHhcNMDYxMDAyMTY0M
zQxWhcnMTYwOTI5MTY0MzQxWjAPMQ0wCwYD05BPDxKbb8Ic6HBPdXKbb8Ic6HWpTJpzs
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdeYZUSgpyAcws5PDyr2GVFMI3dfPn128hVavIkr8r05BPDxKbb8Ic6HWpTZMA0GCSqGSIb3DQEBAUAM
A8xDTNMTYwOTI5MTY0MzQxBA
-----END CERTIFICATE-----
```


2. Go to the Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab.
3. Click **Add New Certificate** to open a window into which you can paste the CA-signed certificate.
4. Paste the certificate into the Key/Cert field.
5. Optionally, enter a comment to be displayed in the Trusted Certificates list. Leave it blank if you want to use the certificate's subject. This can be changed later using the **Change Entry** action.
6. Click **OK** and confirm that the certificate is listed on the Trusted Certificates tab.

Part 2 – Local Certificate and private key

After the self-signed certificate has been added to each appliance in your SteelCentral deployment as a trusted certificate, the final step is to add the certificate and the private key as the Local Credentials for your NetProfiler or NetExpress.

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the MNMP SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the MNMP certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the MNMP certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCA+jgAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV
...
xnRRtSStpDwBRwrPBX9wiih7X13I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----
```

If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

Replacing the Identityd SSL certificate

The Identityd certificate secures communication between the Cascade ADConnector program and the NetProfiler or NetExpress appliance. The Cascade ADConnector program transfers user identity information from Microsoft Windows Active Directory domain controllers to a SteelCentral NetProfiler or NetExpress appliance.

The subject Common Name in the Identityd certificate must be: **CN=Mazu NetProfiler: Identity**

The appliance checks the validity dates when the certificate is loaded. Afterwards, it ignores the expiration date.

Regenerating the Identityd certificate

The Regenerate action creates a new private key and self-signed certificate. To regenerate the Identityd certificate,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the Identityd SSL Certificate, choose **Regenerate Key/Cert** from the Actions menu.
This generates a new certificate and a new private key. The certificate contains the new public key.
3. Click **OK** and confirm that the Identityd certificate is listed on the Local Credentials tab.
4. If the program collecting the user identity information is the Cascade ADConnector 1.5 program (Microsoft Windows 2000 or Windows 2003 Active Directory domain controllers), then resynchronize the program. Refer to Tech Note 029 for details.
5. If the program collecting the user identity information is the Cascade ADConnector 2.0 program (Microsoft Windows 2008 Active Directory domain controllers), then the program will resynchronize automatically and no further action is necessary.

Replacing the Identityd certificate with a CA-signed certificate

When replacing the Identityd certificate with a CA-signed certificate, it is not necessary to add these certificates to the device that is running the ADConnector program.

Prerequisites

A CA-signed certificate may include a hierarchical chain of certificates from several certification authorities (the certification chain). All these CA certificates must all be added as individual entries in the Trusted Certificates section of this appliance.

Depending on your CA, you may receive these as a concatenation in one file and need to separate them before placing them in the Trusted Certificates section. If you add more than one CA certificate at a time, the appliance will use the first one it finds, which may not be the correct one.

Alternatively, your CA may provide certificates in separate files. In this case, ensure that you have each certificate in the entire CA chain and not just the end entity certificate.

The end entity certificate and its private key must be pasted into the Local Credentials section of the NetProfiler or NetExpress appliance, and the entire CA certificate chain must be pasted into the Trusted Certificates section of this NetProfiler or NetExpress appliance.

The certificates must include the following certificate extensions:

- X.509v3 Subject Key Identifier
- X.509v3 Authority Key Identifier

These are necessary in case the CA certificate is renewed and in case more than one CA certificate has the same subject.

Part 1 – Trusted Certificates

To add the CA certificates to this NetProfiler or NetExpress appliance,

1. Copy the first certificate of the CA certificate chain, including the BEGIN and END statements. The certificate will be in a format such as:

```
-----BEGIN CERTIFICATE-----
```



```

MIIBsTCCARqgAwIBAgIJAOqvgxZRcO+ZMA0GCSqGSIb3DQEBAUAMA8xDTALBgNVBAMTBElhenUwHhcNMDYxMDAyMTY0M
zQxWhcNMTYwOTI5MTY0MzQxWjAPMQ0wCwYD05BPDxKbb8Ic6HBPDxKbb8Ic6HWpTJpzs
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdEYUSgpyAcws5PDyr2GVFMI3dfPnl28hVavIkR8r05BPDxKbb8Ic6HWpTZMA0GCSqGSIb3DQEBAUAM
A8xDTNMTYwOTI5MTY0MzQxBA
-----END CERTIFICATE-----

```

2. Go to the Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab.
3. Click **Add New Certificate** to open a window into which you can paste the CA-signed certificate.
4. Optionally, enter a description to be displayed in the Trusted Certificates list. Leave it blank if you want to use the certificate's subject. This can be changed later using the **Change Entry** action.
5. Paste the certificate into the Key/Cert field.
6. Click **OK** and confirm that the certificate is listed on the Trusted Certificates tab.
7. Repeat this procedure for each CA certificate in the chain until all CA certificates in the chain have been added as separate entries.

Part 2 – Local Certificate and private key

After each certificate in the CA chain has been added as a trusted certificate, add the end entity certificate and the private key as the Local Credentials for this NetProfiler or NetExpress.

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the Identityd SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the end entity Identityd certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the Identityd certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the end entity certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```

-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCA+jgAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV
...
xnRRtSStpDwBRwrPBX9wiih7X13I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----

```

If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

Part 3 – Cascade ADConnector program

If the program collecting the user identity information is the Cascade ADConnector 1.5 program (Microsoft Windows 2000 or Windows 2003 Active Directory domain controllers), then resynchronize the program. Refer to Tech Note 029 for details.

If the program collecting the user identity information is the Cascade ADConnector 2.0 program (Microsoft Windows 2008 Active Directory domain controllers), then the program will resynchronize automatically and no further action is necessary.

Replacing the Identityd certificate with a self-signed certificate

To replace the Identityd certificate with a self-signed certificate,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab of this appliance.
2. In the row for the Identityd SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the Identityd certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the Identityd certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCAj+gAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV
...
xnRRtSStpDwBRwrPBX9wiih7X13I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----
```

If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

5. If the program collecting the user identity information is the Cascade ADConnector 1.5 program (Microsoft Windows 2000 or Windows 2003 Active Directory domain controllers), then resynchronize the program. Refer to Tech Note 029 for details.
6. If the program collecting the user identity information is the Cascade ADConnector 2.0 program (Microsoft Windows 2008 Active Directory domain controllers), then the program will resynchronize automatically and no further action is necessary.

Replacing the Apache SSL certificate

The Apache certificate secures the NetProfiler appliance while it is communicating with users' web browsers. After you replace the Apache certificate it will be necessary to restart your browser to avoid browser errors. Additionally, all other users that are connected to the web user interface of this appliance should restart their browsers to avoid browser errors.

Regenerating the Apache certificate

The Regenerate action creates a new private key and CA-signed certificate. Each SteelCentral appliance has its own CA root for Apache.

To regenerate the SSL certificate for the Apache web server,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab.
2. In the row for the Apache SSL Certificate, choose **Regenerate Key/Cert** from the Actions menu.

This generates a new certificate and a new private key.

3. Restart your web browser before logging back in to the appliance. Advise all other users that are connected to the web user interface of this appliance to restart their browsers to avoid browser errors.

Replacing the Apache certificate with a CA-signed certificate

For the Apache certificate, there is no need to load the CA certificate chain. Only the end entity certificate and private key are necessary. The Apache certificate should have standard web server extensions (SSL Server, TLS Web Server Authentication, etc.). If it does not have these, the web browser's certificate verification process may fail.

To replace the Apache certificate with a CA-signed certificate,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab of this appliance.
2. In the row for the Apache SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the Apache certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the Apache certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCcwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCA+jgAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV
...
xnRRtSStpDwBRwrPBX9wiih7Xl3I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----
```


If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

5. Restart your web browser before logging back in to the appliance. Advise all other users that are connected to the web user interface of this appliance to restart their browsers to avoid browser errors.

Replacing the Apache certificate with a self-signed certificate

For the Apache certificate only the end entity certificate and private key are necessary. The Apache certificate should have standard web server extensions (SSL Server, TLS Web Server Authentication, etc.). If it does not have these, the web browser's certificate verification process may fail.

To replace the Apache certificate with a self-signed certificate,

1. Go to the Configuration > Appliance Security > Encryption Key Management page Local Credentials tab of this appliance.
2. In the row for the Apache SSL Certificate, choose **Change Key/Cert** from the Actions menu.
3. Paste both the Apache certificate and the private key into the Key/Cert field.
4. Click **OK** and confirm that the Apache certificate is listed on the Local Credentials tab.

Note: Ensure that you include both the private key and the certificate with their BEGIN and END statements. If you paste in just the certificate, you will get a certification error.

They will be in the format:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCcwggSjAgEAAoIBAQC7CkgI/yEMu0td
...
6Q1V08AwLd4fVrOGvmOeZKk=
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDVzCCA+jgAwIBAgIJAPy15+KVLMAxMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNV
...
xnRRtSStpDwBRwrPBX9wiih7X13I2n2Qs/c0Gh9OVhKqsmcoZmnHjCQrdQ==
-----END CERTIFICATE-----
```

If you subsequently view the Local Credentials, you will not see the private key. It is never visible except when you initially paste it into the Change window.

5. Restart your web browser before logging back in to the appliance. Advise all other users that are connected to the web user interface of this appliance to restart their browsers to avoid browser errors.

SSL certificate requirements

SteelCentral products require SSL certificates to follow ITU-T standard X.509 and base-64 encoding of DER with header and footer lines. This is generally referred to as PEM format.

SteelCentral products require an unencrypted private key in a PKCS#8 format encoded in the PEM format. Encrypted private keys and binary-encoded private keys (including PKCS#12) are not accepted. If your Certificate Authority issues the PKCS#12 file, you will need to convert it to the PEM format.

The Local Credential section expects:

```
-----BEGIN CERTIFICATE-----  
Base-64 encoded certificate  
-----END CERTIFICATE-----  
-----BEGIN PRIVATE KEY-----  
Base-64 encoded private key  
-----END PRIVATE KEY-----
```

Additionally, the certificates and keys must meet the minimum requirements of the operational security mode. If the certificates do not comply with FIPS 140-2 requirements when the appliance is switched into FIPS 140-2 Compatible Cryptography mode, they will automatically be replaced by the default certificates.

The key and certificate requirements are as follows:

- FIPS Compatible Cryptology mode:
 - SSH: 1024 bit or more RSA or DSA
 - SSL: X.509 certificate, 1024 bit or more RSA or DSA, signed with SHA1 or higher
- Not in FIPS Compatible Cryptology mode (minimum requirements):
 - SSH: 512 bit or more RSA or DSA
 - SSL:
 - X.509 certificate, 512 bit or more RSA or DSA, any signature
- The default values are:
 - SSH: 2048 bit RSA
 - SSL:
 - X.509 certificate, 2048 bit RSA, SHA512 signature

APPENDIX A SNMP Support

The SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliances send SNMP traps and support MIB browsing by MIB tools. This section describes the traps and access to the MIB. A copy of the MIB can be downloaded from the help system.

This appendix includes the following sections:

- [“Trap summary,” next](#)
- [“Variables common to all NetProfiler and NetExpress traps” on page 312](#)
- [“Additional trap variables” on page 314](#)
- [“SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliance MIB” on page 316](#)

Trap summary

The Cascade appliance sends SNMP Version 1, 2c or 3 traps, if enabled. The Behavior Analysis > Notifications page specifies two IP addresses and port numbers for the trap destinations.

Each trap is identified by an enterprise-specific trap number. This is an INTEGER, provided as the last part of the trap Object ID .1.3.6.1.4.1.7054.70.0.n, where n is the trap number as follows:

Event	Enterprise-specific trap numbers		
	Low	Medium	High
Denial of Service/Bandwidth Surge	11	12	13
Worm	15	16	17
Host Scan	19	20	21
Port Scan	23	24	25
Suspicious Connection	27	28	29
New Host	31	32	33
New Server Port	47	48	49
User-defined policy	55	56	57

Event	Enterprise-specific trap numbers		
	Low	Medium	High
Data Source Problem	-	-	65
Application Availability	79	80	81
Link Congestion	83	84	85
Link Outage	87	88	89
Application Performance	91	92	93
Service	95	-	97
Storage Problem	-	-	105
Module Problem	-	-	106
Hardware Problem	-	-	107
Test	-	-	99

Data Source Problem, Storage Problem, Module Problem and Hardware Problem events always generate high level alert traps.

Variables common to all NetProfiler and NetExpress traps

The appliance attaches variables to traps to provide information to the trap receiver. All traps include a set of variables describing the conditions that caused the trap. Traps for some types of policies include additional variables, which are listed separately by trap. Where applicable, the variables that are common to all the appliance traps include:

- **Trap Number** - an INTEGER, indicated by a component of the trap Object ID .1.3.6.1.4.1.7054.70.0.n, where n is the unique, enterprise-specific trap number as listed in the table above.
- **System Up Time** - an INTEGER, identified as .1.3.6.1.2.1.1.3.0, that is the length of time that the appliance operating system has been running, expressed in Time Ticks (hundredths of a second).
- **Severity** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.1.0, that indicates the severity, on a scale of 1 to 100, of the event that triggered the alert.
- **Event Description** - a human-readable OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.3.0, that provides the name of the type of policy that caused the alert.
- **Event ID** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.4.0, that is the appliance's Event ID number for the event that triggered the alert. This is the ID number displayed on the Dashboard page and the Event Reports page.
- **Event URL** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.5.0, that is the URL of the Event Details report for the event that triggered the alert. This is given in the format `https://<appliance_name>/event_viewer.php?id=<event_ID>`. A login (Event Viewer role or higher) and password on the appliance are required to view the report.
- **Alert Level** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.7.0, that indicates the level of the alert, where 1 is Low, 2 is Medium, and 3 is High.
- **Start Time** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.8.0, that is the epoch time that the event started.
- **Source Count** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.16.0, that is the number of sources associated with the event.

- **Source List** - a sequence, identified as .1.3.6.1.4.1.7054.71.2.17.0, that lists the IP address and host name of sources associated with the event. The elements in this list are:

Index - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.17.1.1.*n*, where *n* is the number of the row.

Name - an OCTET STRING, which is the DNS name (if available) of the source host, and is identified as .1.3.6.1.4.1.7054.71.2.17.1.2.*n* where *n* is the number of the row.

Address - an IPAddress, which is the IP address of the source host, and is identified as .1.3.6.1.4.1.7054.71.2.17.1.3.*n* where *n* is the number of the row.

For example, the OIDs for the first three rows are:

Index: .1.3.6.1.4.1.7054.71.2.17.1.1.1

Name: .1.3.6.1.4.1.7054.71.2.17.1.2.1

Address: .1.3.6.1.4.1.7054.71.2.17.1.3.1

Index: .1.3.6.1.4.1.7054.71.2.17.1.1.2

Name: .1.3.6.1.4.1.7054.71.2.17.1.2.2

Address: .1.3.6.1.4.1.7054.71.2.17.1.3.2

Index: .1.3.6.1.4.1.7054.71.2.17.1.1.3

Name: .1.3.6.1.4.1.7054.71.2.17.1.2.3

Address: .1.3.6.1.4.1.7054.71.2.17.1.3.3

- **Destination Count** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.18.0, that is the number of destinations associated with the event.
- **Destination List** - a sequence, identified as .1.3.6.1.4.1.7054.71.2.19.0, that lists the IP address and host name of destinations associated with the event. The elements in this list are:

Index - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.19.1.1.*n*, where *n* is the number of the row.

Name - is an OCTET STRING, which is the DNS name (if available) of the destination host, and is identified as .1.3.6.1.4.1.7054.71.2.19.1.2.*n* where *n* is the number of the row.

Address - is an IPAddress, which is the IP address of the destination host, and is identified as .1.3.6.1.4.1.7054.71.2.19.1.3.*n* where *n* is the number of the row.

- **Protocol Count** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.20.0, that is the number of protocols associated with the event.
- **Protocol List** - a sequence, identified as .1.3.6.1.4.1.7054.71.2.21.0, that lists the protocols associated with the event. The elements in this list are:

Index - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.21.1.1.*n*, where *n* is the number of the row.

Name - is an OCTET STRING, which is the name of the protocol, and is identified as .1.3.6.1.4.1.7054.71.2.21.1.2.*n* where *n* is the number of the row.

Number - is an INTEGER, which is the number of the protocol, and is identified as .1.3.6.1.4.1.7054.71.2.21.1.3.*n* where *n* is the number of the row.

- **Port Count** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.22.0, that is the number of ports associated with the event.
- **Port List** - a sequence, identified as .1.3.6.1.4.1.7054.71.2.23.0, that lists the ports associated with the event. The elements in this list are:

Index - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.23.1.1.*n*, where *n* is the number of the row.

Name - is an OCTET STRING, which is the name of the port, and is identified as .1.3.6.1.4.1.7054.71.2.23.1.2.*n* where *n* is the number of the row.

Protocol Number - is an INTEGER, which is the numeric ID of the protocol associated with the port and is identified as .1.3.6.1.4.1.7054.71.2.23.1.3.*n* where *n* is the number of the row.

Port Number - is an INTEGER, which is the numeric ID of the port and is identified as .1.3.6.1.4.1.7054.71.2.23.1.4.*n* where *n* is the number of the row.

The length of the source, destination, protocol, and port lists is limited by the “Maximum length of lists attached to traps” setting in the SNMP MIB Configuration section of the Configuration > General Settings page. For compatibility reasons, the protocol/port-related variables are named in terms of “services” in the appliance MIB.

Additional trap variables

In addition to the variables that are common to all SteelCentral™ NetProfiler and SteelCentral™ NetExpress traps, the following traps include other variables:

- Denial of Service/Bandwidth Surge
- Suspicious Connection
- New Server Port
- Performance and Availability and User-defined
- Service

Denial of Service/Bandwidth Surge trap variables

In addition to the variables that are common to all the appliance traps, the Denial of Service/Bandwidth Surge traps include:

- **normal bytes per second** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.31.0, that is the normal number of bytes per second for the current profile.
- **current bytes per second** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.32.0, that is the current number of bytes per second.
- **normal packets per second** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.33.0, that is the normal number of packets per second for the current profile.
- **current packets per second** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.34.0, that is the current number of packets per second.

Suspicious Connection trap variables

In addition to the variables that are common to all the appliance traps, the Suspicious Connection traps include:

- **current number of connections** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.36.0, that is the current number of connections per second.

New Server Port trap variables

In addition to the variables that are common to all the appliance traps, the New Server Port traps include:

- **host or group switch** - An INTEGER, identified as .1.3.6.1.4.1.7054.71.2.41.1.0, that indicates whether the policy alerted on a host or on a group, where 1 indicates Host, and 2 indicates Group.
- **host name** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.41.2.0. If the policy alerts for only a specified host, then this is the host name.
- **host address** - an IPAddress, identified as .1.3.6.1.4.1.7054.71.2.41.3.0. If the policy alerts for only a specified host, then this is the host's IP address.
- **policy description** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.43.0, that describes the policy that was violated.
- **group type ID** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.41.4.0. If the policy alerts for only a given group, then this is the numeric ID of the group type.
- **group ID** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.41.5.0. If the policy alerts for only a given group, then this is the numeric ID of the group.

Performance, Availability, and User-defined trap variables

In addition to the variables that are common to all the appliance traps, the Performance and Availability traps and User-defined traps both include:

- **policy name** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.42.0, that is the name of the policy that was violated.
- **policy description** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.43.0, that describes the policy that was violated.
- **upper or lower bound** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.45.0, that identifies whether the threshold is an upper bound or lower bound, where 1 indicates upper bound and 2 indicates lower bound.
- **threshold value** - an INTEGER, identified as .1.3.6.1.4.1.7054.71.2.46.0, that identifies the traffic rate for the exceeded threshold.
- **threshold units** - a STRING, identified as .1.3.6.1.4.1.7054.71.2.47.0, that identifies the units of measure that the rule is using.

Service trap variables

In addition to the variables that are common to all NetProfiler traps, Service traps include:

- **policy name** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.42.0, that is the name of the policy that was violated.
- **policy description** - an OCTET STRING, identified as .1.3.6.1.4.1.7054.71.2.43.0, that describes the policy that was violated.

SteelCentral™ NetProfiler and SteelCentral™ NetExpress appliance MIB

The appliance MIB values can be read with any standards-based SNMP MIB tool, including those on the Windows and Linux operating systems. You can obtain a copy of the MIB definition file from the help system and save it locally for your MIB tool to use for labeling the values it retrieves from the appliance.

The SNMP Object ID for the MIB is 1.3.6.1.4.1.7054.70. You can use either Version 1 or Version 3 of SNMP for browsing the MIB.

Versions 1 and 2c

If you are using an SNMP Version 1 or 2c MIB tool, ensure that the correct configuration is selected in the SNMP MIB Configuration section of the Configuration > General Settings page and copy the Version 1 MIB definition file from the online help system SNMP Support > MIB page. This file is named MAZU-V1-COMPATIBILITY-MIB.txt.

Version 3

If you are using an SNMP Version 3 MIB tool, ensure that the Version 3 configuration is selected in the SNMP MIB Configuration section of the Configuration > General Settings page and copy the Version 3 MIB definition file from the online help system SNMP Support > MIB page. This file is named MAZU-MIB.txt.

Examples

The following examples use the Linux `snmpwalk` tool. In these examples, the command is entered as one line.

Version 3 without privacy

```
snmpwalk -m MIB_path -v 3 -u fred -l authNoPriv -a MD5 -A fredpass1 mgt_if .1.3.6.1.4.1.7054.70
```

where:

MIB_path is the path to the local copy of MAZU-MIB.txt

fred is the user name

MD5 is the authentication protocol

fredpass1 is the authentication password

mgt_if is the IP address or host name of the Standard NetProfiler or the Manager blade in an Enterprise NetProfiler. This is available in the Management Interface Configuration section of the Configuration > General Settings page.

Version 3 with privacy

```
snmpwalk -m MIB_path -v 3 -u fred -l authPriv -a MD5 -A fredpass1 -x DES -X fredpass2 mgt_if .1.3.6.1.4.1.7054.70
```

where:

MIB_path is the path to the local copy of MAZU-MIB.txt

fred is the user name

MD5 is the authentication protocol

fredpass1 is the authentication password

DES is the privacy protocol

fredpass2 is the privacy password

mgt_if is the IP address or host name of the Standard NetProfiler or the Manager blade in an Enterprise NetProfiler. This is available in the Management Interface Configuration section of the Configuration > General Settings page.

Version 1

```
snmpwalk -m MIB_path -v 1 -c community mgt_if .1.3.6.1.4.1.7054.70
```

where:

MIB_path is the path to the local copy of MAZU-V1-COMPATIBILITY-MIB.txt

community is the community name of the appliance. This is available in the SNMP MIB Configuration section of the Configuration > General Settings page.

mgt_if is the IP address or host name of the Standard NetProfiler or the Manager blade in an Enterprise NetProfiler. This is available in the Management Interface Configuration section of the Configuration > General Settings page.

APPENDIX B Restoring a system

This appendix describes restoring the SteelCentral™ NetProfiler and SteelCentral™ NetExpress logs from a backup copy.

Backup operations are performed using the web user interface System > Backup page, which is described in [“Update” on page 161](#).

Restore operations are performed using the mazu-sync command line utility. The “restore” operation copies system configuration information and traffic information from a customer-provided backup system.

Within the limitations listed in the Requirements section that follows, NetProfiler and NetExpress systems can be restored from backup copies as follows:

- A backup copy from a virtual system can be used to restore a:
 - Virtual system
 - Model xx60 hardware-based system
 - Model xx70 hardware-based system
- A backup copy from a Model xx60 hardware-based system can be used to restore a:
 - Model xx60 hardware-based system
 - Model xx70 hardware-based system
- A backup copy from a Model xx70 hardware-based system can be used to restore a Model xx70 hardware-based system.

Requirements

The “restore” operation requires:

- Platform compatibility between the system being restored and the system from which the backup was made
- Password-less access between the backup server and the system being restored
- Adequate link speed between the backup server and the system being restored
- The password that protects the backup copy
- Applicable licenses

Platform compatibility

Note that the NetProfiler or NetExpress being restored must be:

- Running the exact same software version as the backup copy.
- Running on the same platform as the system from which the backup copy was made, or a platform one step higher.

Specifically, a backup copy made from:

- A virtual NetExpress can restore a:
 - Virtual NetExpress
 - Hardware-based NetExpress
 - Virtual Standard NetProfiler
 - Hardware-based NetProfiler
- A hardware-based NetExpress can restore a:
 - Hardware-based NetExpress
 - Hardware-based NetProfiler
- A virtual Standard NetProfiler can restore a:
 - Virtual Standard NetProfiler
 - Hardware-based Standard NetProfiler
 - Enterprise NetProfiler with one Analysis Module
- A hardware-based Standard NetProfiler can restore a:
 - Hardware-based Standard NetProfiler
 - Enterprise NetProfiler with one Analysis Module
- An Enterprise NetProfiler can restore an Enterprise NetProfiler that has the same number of components or fewer.

Note that a backup copy made from a system that has a SAN device cannot restore a system that does not have the same SAN configuration.

Password-less access

Both backup and restore operations require the same system changes with respect to:

- Shell Access - Shell access must be enabled via the Configuration > Appliance Security > Security Compliance page in the user interface.
- SSH Access - Password-less SSH access is required between the NetProfiler or NetExpress and the backup server. This means you must share SSH keys between the NetProfiler or NetExpress and the backup server.

To set up password-less access to the backup server:

1. Log into the command line interface of the NetExpress, Standard NetProfiler or the UI Module of the Enterprise NetProfiler to be restored.
2. Run the following command:


```
cat /opt/cascade/vault/ssh/mazu/id_rsa.pub | ssh admin@10.38.7.2 "cat >> .ssh/authorized_keys2"
```

(where “admin@10.38.7.2” and “.ssh/authorized_keys2” are examples).

To set up password-less access from the backup server to the system being restored:

1. Log into the backup server.

2. Run the following command:

```
cat /home/admin/.ssh/id_rsa.pub | ssh mazu@10.38.7.2 "cat >> /opt/cascade/vault/ssh/mazu/authorized_keys2"
```

(where “home/admin” and “.ssh/id_rsa.pub” are examples).

Link speed

The backup system must be accessible via SSH at an effective speed of at least 10 Mbps.

Password

The image created by the backup operation is protected by a password. You must use this password when performing a restore operation.

Licenses

Before beginning the restore operation, install all applicable licenses on the system that is to be restored. Licenses are installed using the Configuration > Licenses page or the user interface.

Before you begin

The NetProfiler or NetExpress must be configured for your installation before you run the mazu-sync command to restore it. This includes any applicable licenses.

Note that there are also configuration tasks that must be performed after the restore operation. These include:

- Security settings - The settings on the Configuration > Appliance Security > Security Compliance page are specific to the appliance and are not included in the backup image. This includes FIPS mode, Strict Security mode, the Shell Access setting, system user passwords, the Bootloader password and appliance access settings. These must be set for each appliance after restoring the image.
- General Settings - Host name, IP address and other settings on the Configuration > General Settings page should be reviewed after the restore operation.

Restoring a Standard NetProfiler

The mazu-sync utility restores the NetProfiler to the state that existed when the backup was created, except that it does not change the basic network settings that are configured on the Configuration > General Settings page.

Current data on the NetProfiler is lost when the mazu-sync utility is run. The mazu-sync utility is run from the command line on the NetProfiler in the format:

```
mazu-sync --pull SOURCE-DIR [options]
```

where *SOURCE-DIR* is the backup directory and is specified using the [user@]host:path syntax as with the scp command. For example, to restore from a full backup:

1. Ensure that the restore requirements have been met.
2. Ensure that keyless SSH access between the backup server admin account and the NetProfiler **mazu** account is configured.
3. Ensure that all applicable licenses are installed on the NetProfiler to be restored. (This step does not apply to hardware platforms earlier than xx60 models.)
4. Initiate an SSH connection to the NetProfiler and log in as **mazu**.
5. If any changes were made in local.conf, copy <backup_directory>/profiler/emhost/usr/mazu/etc/device and <backup_directory>/profiler/emhost/usr/mazu/etc/local.conf from the backup server to /usr/mazu/etc/ of the NetProfiler.
6. On the NetProfiler, if no password is required for the backup image, run the restore command as follows:
 - To run a full restore of the NetProfiler (which requires that you ran a full backup), run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all
```
 - To restore a NetProfiler without restoring traffic flow logs or user identity logs, run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs
```
7. If the sensitive data in the backup image has been protected by a password and encryption, you must enter the password either on the command line or from STDIN.
 - For entering a password from the command line, use the following commands instead of the commands shown in Step 6:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass 'mypassword'
```

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --pass 'mypassword'
```
 - For receiving a password from STDIN, use the following commands instead of the commands shown above:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass STDIN
```

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --pass STDIN
```

Notes:

- To see other available options for mazu-sync, run mazu-sync --help on the NetProfiler command line.
- If there are multiple backup image folders in the path you specified, mazu-sync will restore the latest image available.
- The mazu-sync utility keeps a log locally at /usr/mazu/var/log/restore.log.

Restoring an Enterprise NetProfiler

The mazu-sync utility restores the Enterprise NetProfiler to the state that existed when the backup was created, except that it does not change the basic network settings that are configured on the Configuration > General Settings page.

Current data on the Enterprise NetProfiler is lost when the mazu-sync utility is run.

The mazu-sync utility is run from the command line on the NetProfiler in the format:

```
mazu-sync --pull SOURCE-DIR [options]
```

where *SOURCE-DIR* is the backup directory and is specified using the [user@]host:path syntax as with the scp command. For example, to restore from a full backup:

1. Ensure that the restore requirements have been met.
2. Ensure that keyless SSH access between the backup server admin account and the NetProfiler mazu account is configured.
3. Ensure that all applicable licenses are installed on the Enterprise NetProfiler that is to be restored. (This step does not apply to hardware platforms earlier than xx60 models.)
4. Initiate an SSH connection to NetProfiler Database Module and log in as **mazu**.
5. If any changes were made in local.conf, copy <backup_directory>/profiler/emhost/usr/mazu/etc/device and <backup_directory>/profiler/emhost/usr/mazu/etc/local.conf from the backup server to /usr/mazu/etc/ of the NetProfiler.
6. On the NetProfiler, if no password is required for the backup image, run the restore command as follows:
 - To run a full restore of the NetProfiler (requires that you ran a full backup), run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all
```
 - To restore a NetProfiler without restoring traffic flow logs or user identity logs, run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs
```
7. If the sensitive data in the backup image has been protected by a password and encryption, you must enter the password either on the command line or from STDIN.
 - For entering a password from the command line, use the following commands instead of the commands shown in Step 6:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass 'yourpassword'
```

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --pass 'yourpassword'
```
 - For receiving a password from STDIN, use the following commands instead of the commands shown above:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass STDIN
```

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --pass STDIN
```


Notes

- To see other available options for mazu-sync, run `mazu-sync --help` on the NetProfiler command line.
- If there are multiple backup image folders in the path you specified, mazu-sync will restore the latest image available.

Restoring a NetExpress

The mazu-sync utility restores the NetExpress to the state that existed when the backup was created, except that it does not change the basic network settings that are configured on the Configuration > General Settings page. Packet logs and index files are not backed up. Additionally, capture jobs are not restored if the backup and restore operations are performed from a physical appliance to a virtual edition or vice versa.

Current data on the NetExpress is lost when the mazu-sync utility is run.

The mazu-sync utility is run from the command line on the NetExpress in the format:

```
mazu-sync --pull SOURCE-DIR [options]
```

where *SOURCE-DIR* is the backup directory and is specified using the `[user@]host:path` syntax as with the scp command. For example, to restore from a full backup:

1. Ensure that the restore requirements have been met.
2. Ensure that keyless SSH access between the backup server admin account and the NetExpress mazu account is configured.
3. Ensure that all applicable licenses are installed on the NetExpress to be restored. (This step does not apply to hardware platforms earlier than xx60 models.)
4. Initiate an SSH connection to NetExpress and log in as **mazu**.
5. If any changes were made in `local.conf`, copy `<backup_directory>/profiler/emhost/usr/mazu/etc/device` and `<backup_directory>/profiler/emhost/usr/mazu/etc/local.conf` from the backup server to `/usr/mazu/etc/` of the NetExpress.
6. On the NetExpress, if no password is required for the backup image, run the mazu-sync command as follows:
 - To run a full restore of the NetExpress (which requires that you ran a full backup), run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all
```
 - To restore a NetExpress without restoring traffic flow logs or user identity logs, run the restore command in the following format:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs
```
7. If the sensitive data in the backup image has been protected by a password and encryption, you must enter the password either on the command line or from STDIN.
 - For entering a password from the command line, use the following commands instead of the commands shown in Step 6:


```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass 'mypassword'
```



```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --  
pass 'mypassword'
```

- For receiving a password from STDIN, use the following commands instead of the commands shown above:

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --all --pass STDIN
```

```
/usr/mazu/bin/mazu-sync --pull admin@backup-server.company.com:/backup/mazu --no-logs --pass STDIN
```

Notes

- To see other available options for mazu-sync, run `mazu-sync --help` on the NetExpress command line.
- If there are multiple backup image folders in the path you specified, mazu-sync will restore the latest image available.
- The mazu-sync utility keeps a log locally at `/usr/mazu/var/log/restore.log`.

APPENDIX C Securing the Environment

In most SteelCentral™ NetProfiler and SteelCentral™ NetExpress deployments, Sensors are not on the same subnetwork as NetProfiler or NetExpress appliance. Messages from the Sensor to appliance are typically routed. However, Sensors can be placed on the same subnetwork as the NetProfiler or NetExpress appliance. This presents the following threat scenario:

- If a Sensor is placed on the same subnetwork as NetProfiler or NetExpress appliance, and
- if an intruder can place an unauthorized device on that subnetwork, and
- if the intruder knows the IP address of the NetProfiler or NetExpress interface,
- then it could be possible for the intruder to assign the IP address of the NetProfiler or NetExpress appliance to the unauthorized device.

This scenario could result in some of the Sensor data being received by the unauthorized device instead of by the NetProfiler or NetExpress appliance. It is very unlikely that the unauthorized device could decipher the Sensor data because it is encrypted. Even if it could, having that information is unlikely to be of any value anyway. The security concern is that the NetProfiler or NetExpress appliance might not receive all the data the Sensor sends under this scenario.

You can protect against this type of threat by binding the NetProfiler or NetExpress IP and MAC addresses on the Sensor. This eliminates the possibility of the Sensor getting the MAC address of an unauthorized device that is using the IP address belonging to the NetProfiler or NetExpress appliance.

This precaution is not necessary when the Sensor and NetProfiler are on different subnetworks of a routed network. If an intruder duplicates the NetProfiler IP address on a routed network, the Sensor will see either the unauthorized device or the NetProfiler, but not both. In the first case, NetProfiler will indicate the loss of connectivity with the Sensor. In the second case, the unauthorized device will have no impact on the operation of the Sensor and NetProfiler, even without a static MAC/IP address binding.

Setting up a static MAC/IP address binding on a Sensor

To set up a static MAC/IP binding on a Sensor,

1. Obtain the NetProfiler MAC address and IP address. Use the command line interface to log in as mazu and run `ifconfig`.
2. Log on to the Sensor command line interface as root:
su root
3. Create the file `/etc/ethers` and edit it to contain a line that specifies the MAC address, followed by a tab, followed by the IP address. Use the format:
`xx:xx:xx:xx:xx:xx y.y.y.y`

4. Edit the `/etc/rc.local` file to add the following line:
`/sbin/arp -f /etc/ethers`
This ensures that this binding is used if the Sensor is rebooted.
5. Run the command to establish the binding now:
`/sbin/arp -f /etc/ethers`
6. Check the System > Devices/Interfaces page to ensure that the appliance is receiving Sensor data. If the Sensor status is listed as OK, connectivity has been established.

If the IP address changes (e.g., you move the NetProfiler or NetExpress appliance on the network), or the MAC address changes (e.g., you replace the interface card), this procedure will need to be performed again.



Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: <http://www.riverbed.com>

Part Number
712-00060-21