SteelCentral™ Flow Gateway User's Guide

Version 10.13.x

March 2018

riverbed®

riverbed

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

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

Part Number
712-00234-09

Contents

CHAPTER 1 Introduction

Overview

This guide covers SteelCentral™ Flow Gateway hardware-based appliance and virtual edition. The virtual edition operates the same as the hardware-based appliance except for a small difference in licensing.

The Flow Gateway receives traffic flow data from multiple sources including NetFlow (versions 1, 5, 7 and 9), IPFIX, SteelFlow Net, sFlow (versions 2, 4 and 5), and Packeteer (versions 1 and 2). It aggregates the data, de-duplicates it, compress it by 5 to 10 times, encrypts it using AES 256-bit encryption, and then transmits it to up to five SteelCentral™ NetProfiler or SteelCentral™ NetExpress appliances using a TCP-based protocol over port TCP/41017. Additionally, the Flow Gateway can forward flow data, in the format in which it is received, to up to five other destinations.

The Flow Gateway appliance “NetProfiler Export” page provides an option for buffering flow data so that network visibility is not lost when connections to NetProfiler appliances are temporarily interrupted. See “NetProfiler Export” on page 31.

If Flow Gateway is sending data to a NetProfiler that becomes unreachable, such as during a maintenance or update period, the Flow Gateway appliance saves the data locally until the connection can be reestablished.

When the target NetProfiler becomes available again, Flow Gateway resumes sending data normally and also sends the buffered data. The transfer of on-time data takes precedence over the transfer of buffered data.

The amount of flow data that Flow Gateway can buffer depends on network traffic characteristics and licensed capacities. But typically, a Flow Gateway appliance that is receiving 30 million raw flow records per minute can store up to two hours of de-duplicated flow data.

The flow buffering feature is not available on the virtual edition of Flow Gateway.

NetProfiler can process buffered data received from two Flow Gateway appliances. It combines the buffered data with the normal data to provide continuity of visibility in reports based on historical flow data. If, for the same time period, NetProfiler receives both buffered data from a Flow Gateway and on-time data from other sources, including other Flow Gateway appliances, it does not de-duplicate that data. Consequently, packets and bytes may be over-counted in reports for that time period.

Compatibility

Web browsers

The Flow Gateway user interface requires a web browser that supports HTML 3.2, JavaScript 1.2, and Java 1.4. If your browser does not support these, you will be prompted to update.

The user interface has been successfully tested using Microsoft Internet Explorer 9, 10 and 11; Mozilla Firefox ESR 52.0.x; and Chrome.

The browser settings must allow full JavaScript activity.

Some browser plug-ins and add-ons that modify page content may cause the user interface to slow down. They may also prevent large pages from loading and prevent the help system from displaying correctly. It may be necessary to add Riverbed appliances as exceptions to plug-ins that are found to cause problems. If display problems occur, try disabling any browser add-ons or plug-ins that you have loaded.

Ethernet

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

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.

Getting help

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 on line help system table of contents, index, and search features. The help system is available from the Help menu near the upper right-hand corner of all top-level GUI pages.

Additional information is available from the Riverbed Support site at **https://support.riverbed.com**. This includes:

- **Release Notes** - posted in the software section of the page for your product.
- **Installation Guides** - posted in the documentation section of the page for your product.

- **Tech Notes** - posted in the documentation section of the page for your product where applicable.
- **Knowledge Base** - a database of known issues and how-to documents. You can browse titles or search for key words and strings. Choose “Search the Knowledge Base” from the Knowledge Base menu.

Safety Guidelines

Follow the safety precautions outlined in the *Safety and Compliance Guide* when installing or servicing your Riverbed product.

Important: Failure to follow these safety guidelines can result in injury or damage to the equipment. Mishandling of the equipment voids all warranties. Please read and follow safety guidelines and installation instructions carefully.

Many countries require the safety information to be presented in their national languages. If this requirement applies to your country, consult the *Safety and Compliance Guide*.

Contacting Riverbed

Options for contacting Riverbed include:

- **Internet** - Find out about Riverbed products at **http://www.riverbed.com**.
- **Support** - If you have problems installing, using, or replacing Riverbed products, contact Riverbed Technical Support or your channel partner who provides support. To contact Riverbed Technical 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 engineers who can help you with installation, 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** - Riverbed continually strives to improve the quality and usability of its documentation. We appreciate any suggestions you may have about our on line documentation or printed materials. Send documentation comments to **techpubs@riverbed.com**.

CHAPTER 2

Reporting

Once configured and operating, the SteelCentral™ Flow Gateway reports its status on the Overview page and the System Information page. You can also audit its activity by running an Audit report on the System > Audit Trail page.

Accessing Flow Gateway

You can access the Flow Gateway GUI from the network or from the NetProfiler or NetExpress web user interface. You can also access it through the Flow Gateway REST API. Command Line Interface access to Flow Gateway is supported for only initial setup and maintenance purposes. Installing software or modifying configurations via the CLI are not supported and may cause unexpected behavior or stability issues.

Accessing Flow Gateway from the network

To access the Flow Gateway user interface:

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

Accessing Flow Gateway from NetProfiler or NetExpress

The System > Devices/Interfaces page lists all Flow Gateway appliances that are accessible.

1. Go to the NetProfiler or NetExpress System > Devices/Interfaces page.
2. On the Devices & Interfaces (Tree) tab, find the Flow Gateway that you want to access.
3. Click **Go**. This opens a browser session for you to log in to the Flow Gateway.

Accessing the Flow Gateway RESTful API

1. Configure Flow Gateway to allow REST access as described in “RESTful API access” on page 31.
2. Refer to the Flow Gateway REST API specifications on the Riverbed Support site for information about accessing the API.

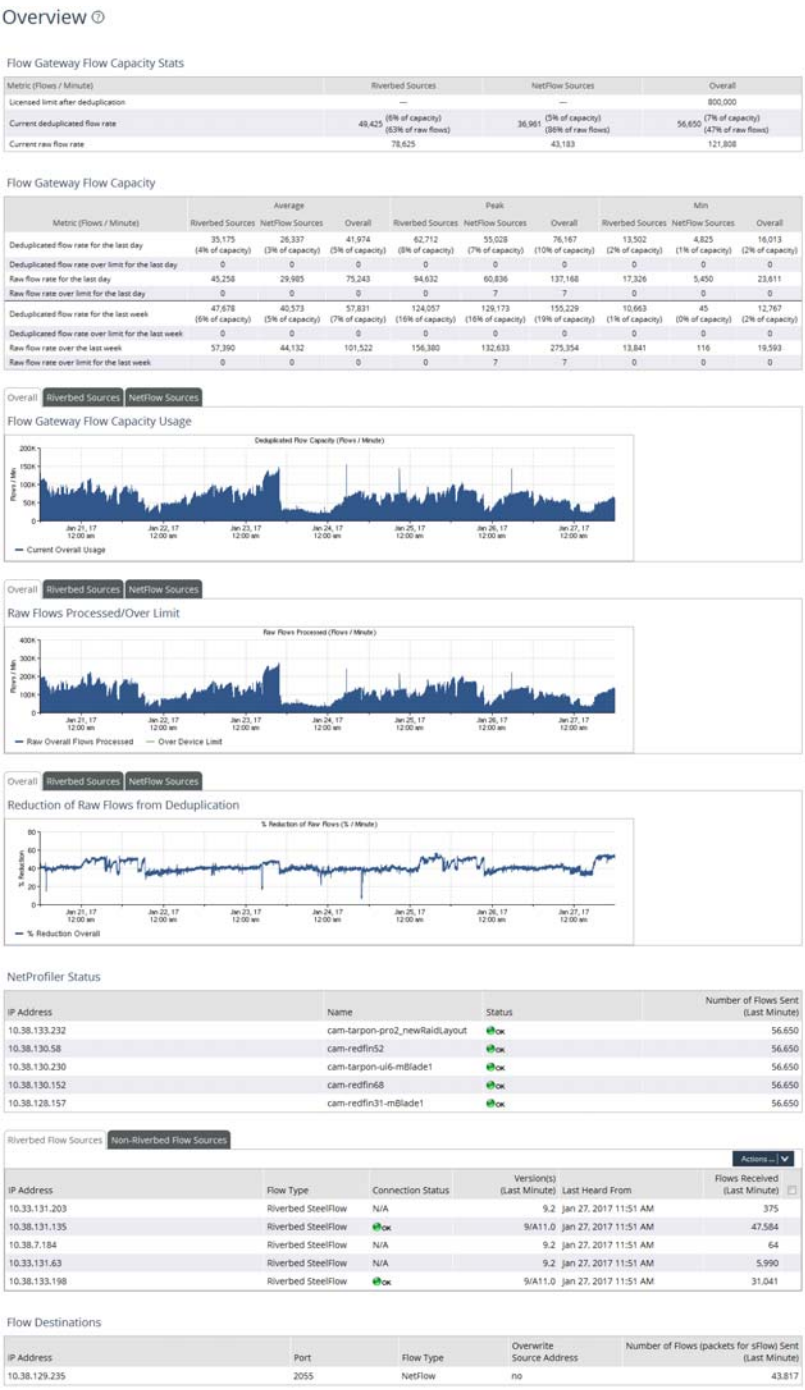
Overview page

Logging in to the Flow Gateway web user interface opens the Overview page.

The Overview page is divided into the following sections:.

- Flow Capacity Stats
- Flow Capacity
- Flow Capacity Usage
- Raw Flows Processed/Over Limit
- Reduction of Raw Flows from Deduplication
- NetProfiler Status
- Flow Sources
- Flow Destinations

Figure 2-1. Overview page



Flow Capacity Stats

The Flow Capacity Stats section summarizes the flow statistics based on the latest data. Flow Gateway saves the IP address of the reporting device and information the device reports about the flow for use in topology reports. It 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. The deduplicated flow rate is also reported as a percent of licensed capacity and as a percent of total raw flows. “Raw flows” are flows reported by switches and routers that are sending flow data to the Flow Gateway appliance.

Figure 2-2. Flow Gateway Flow Capacity Stats

Flow Gateway Flow Capacity Stats

Metric (Flows / Minute)	NetShark Sources	NetFlow Sources	Overall
Licensed limit after deduplication	---	---	1,400,000
Current deduplicated flow rate	0 (0% of capacity) (0% of raw flows)	30,535 (2% of capacity) (96% of raw flows)	30,535 (2% of capacity) (96% of raw flows)
Current raw flow rate	0	31,922	31,922

Flow Capacity

The Flow Capacity section reports the average, peak and minimum flow rates for both deduplicated and raw 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 2-3. Flow Gateway Flow Capacity History

Flow Gateway Flow Capacity

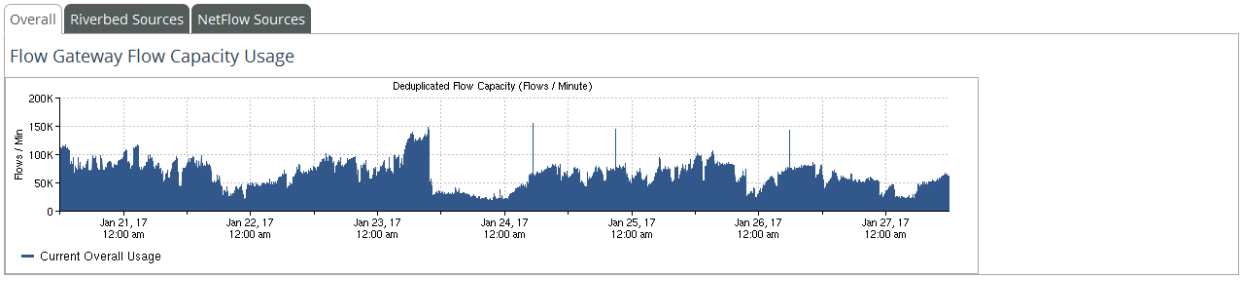
	Average			Peak			Min		
Metric (Flows / Minute)	NetShark Sources	NetFlow Sources	Overall	NetShark Sources	NetFlow Sources	Overall	NetShark Sources	NetFlow Sources	Overall
Deduplicated flow rate for the last day	0 (0% of capacity)	28,838 (2% of capacity)	28,838 (2% of capacity)	0 (0% of capacity)	130,799 (9% of capacity)	130,799 (9% of capacity)	0 (0% of capacity)	5,043 (0% of capacity)	5,043 (0% of capacity)
Deduplicated flow rate over limit for the last day	0	0	0	0	0	0	0	0	0
Raw flow rate for the last day	0	31,237	31,237	0	133,291	133,291	0	5,600	5,600
Raw flow rate over limit for the last day	0	0	0	0	0	0	0	0	0
Deduplicated flow rate for the last week	0 (0% of capacity)	41,737 (3% of capacity)	41,737 (3% of capacity)	0 (0% of capacity)	130,799 (9% of capacity)	130,799 (9% of capacity)	0 (0% of capacity)	0 (0% of capacity)	0 (0% of capacity)
Deduplicated flow rate over limit for the last week	0	0	0	0	0	0	0	0	0
Raw flow rate over the last week	0	45,885	45,885	0	156,210	156,210	0	0	0
Raw flow rate over limit for the last week	0	0	0	0	0	0	0	0	0

Flow Capacity Usage

The Flow Capacity Usage section shows how much of the licensed flow capacity is being used. Separate tabs report Overall capacity usage, Riverbed Sources, NetFlow usage. Riverbed Sources include AppResponse 11 and NetShark.

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.

Figure 2-4. Flow Gateway Flow Capacity Usage



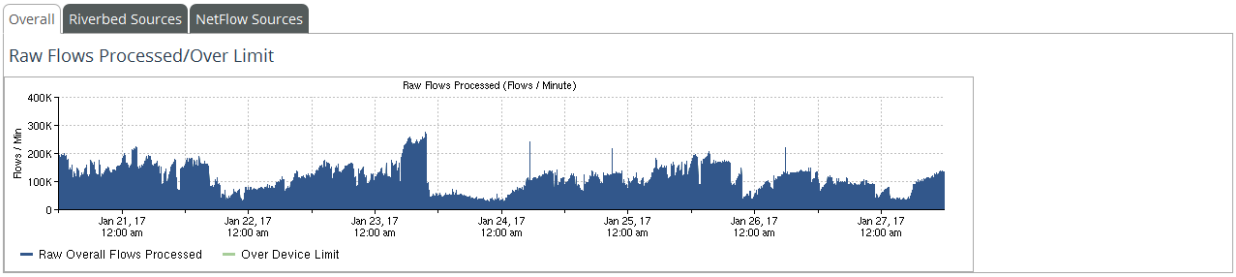
Raw Flows Processed/Over Limit

The Raw Flows Processed/Over Limit section displays the number of flows per minute that have been processed. Separate tabs report Overall flows processed, flows from Riverbed Sources processed, and NetFlow flows processed.

Processing includes collecting and storing topology information and deduplicating flow data. For example, assume that a router sends a flow record to 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.

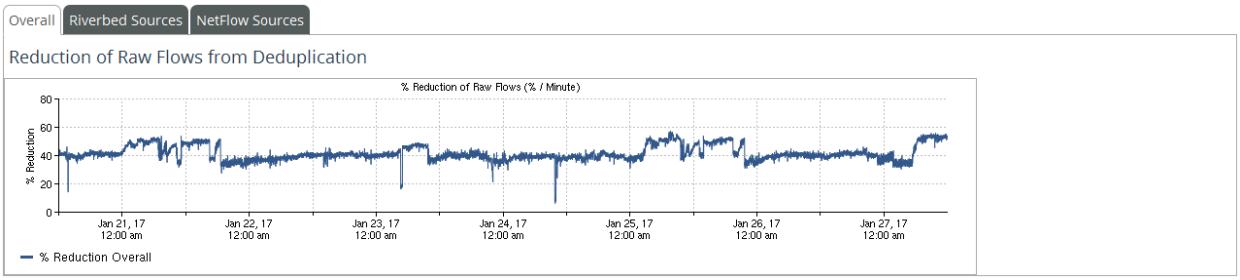
Figure 2-5. Raw Flows Processed/Over Limit



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. Separate tabs report Overall percentage of reduction, Riverbed Source percentage, and NetFlow Source percentage.

Figure 2-6. Reduction of Raw Flows from Deduplication



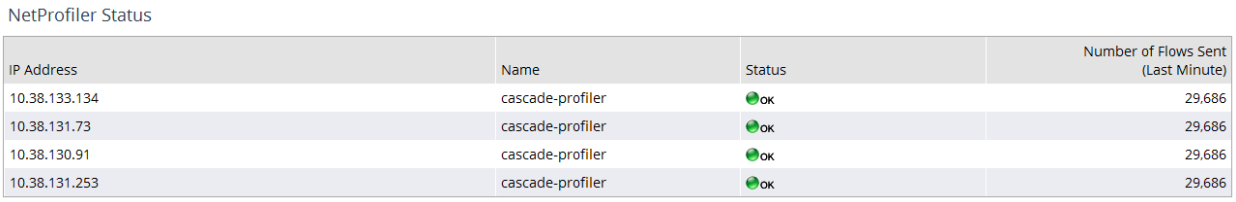
NetProfiler Status

The NetProfiler Status section displays the following information about each NetProfiler or NetExpress appliance with which the Flow Gateway is communicating:

- IP address and the name returned by DNS, if DNS name resolution is enabled. The IP address is specified on the Configuration > Profilers page.
- NetProfiler or NetExpress name as specified in the Hostname field of the Configuration > General Settings page of the NetProfiler or NetExpress appliance.
- NetProfiler or NetExpress appliance status (OK or Offline).

- Number of flows per minute sent to the NetProfiler or NetExpress appliance during the most recent 1-minute reporting period. This may be less than the number of packets received because the flows are deduplicated before being sent to the NetProfiler or NetExpress appliance. This flow summary can also be viewed on the NetProfiler or NetExpress.

Figure 2-7. NetProfiler Status



NetProfiler Status

IP Address	Name	Status	Number of Flows Sent (Last Minute)
10.38.133.134	cascade-profiler	ok	29,686
10.38.131.73	cascade-profiler	ok	29,686
10.38.130.91	cascade-profiler	ok	29,686
10.38.131.253	cascade-profiler	ok	29,686

Flow Sources

The Flow Sources section shows the addresses of the flow data sources and the types of flow data that the Flow Gateway is receiving. It also shows the number of flow records that the Flow Gateway received from the flow data source during the most recent 1-minute reporting period.

Separate tabs report the number of flow records received from Riverbed flow data sources and Non-Riverbed flow data sources.

The Non-Riverbed Flow Sources tab includes a column labeled “Slice Violation (Last Minute).” This column indicates two conditions on the flow data source device that could result in errors in packet counts:

- The flow collector is caching NetFlow records before sending them, thereby causing them to arrive late.
- The flow collector has an active timeout set to greater than 60 seconds.

If a flow data source stops sending data to the Flow Gateway, the number of flows reported the last time the Flow Gateway received data from the source is preserved. However, after 2 minutes, it is displayed in red to indicate that no new flows are being received.

Figure 2-8. Flow Sources

Riverbed Flow Sources | Non-Riverbed Flow Sources

Actions ...

IP Address	Flow Type	Version(s) (Last Minute)	Last Heard From	Flows Received (Last Minute)	Slice Violation (Last Minute)
10.38.128.9	NetFlow	5	Jan 15, 2017 7:43 PM	209	true
10.38.1.6	NetFlow	5	Jan 15, 2017 7:43 PM	2,032	true
10.38.128.8	NetFlow	5	Jan 15, 2017 7:43 PM	27,153	true
10.38.128.1	NetFlow	9	Jan 15, 2017 7:43 PM	117	true
10.38.151.2	NetFlow		Jan 15, 2017 7:42 PM	0	N/A

Flow Destinations

The Flow Destinations section shows the address, port number and type of flow data for each destination to which the Flow Gateway forwards flow data. It also shows the number of flow records that the Flow Gateway has forwarded to the destination during the most recent 1-minute reporting period. For NetFlow, it displays the number of flow records forwarded. For sFlow, it displays the number of sampled packets forwarded.

Additional information about the status of the Flow Gateway can be monitored on the System Information > System Status page.

Figure 2-9. Flow Destinations

Flow Destinations

IP Address	Port	Flow Type	Overwrite Source Address	Number of Flows (packets for sFlow) Sent (Last Minute)
10.38.129.64	1349	NetFlow	no	34,274
10.38.134.53	2003	NetFlow	no	34,274
10.38.133.185	2055	NetFlow	no	34,274
10.38.133.227	2003	NetFlow	no	34,274

System information

The System > Information page displays information about the operation of the Flow Gateway itself and the status of the Riverbed devices to which it is sending information. The page includes the following sections:

- <*Flow Gateway_name*> - displays internal operating parameters.

Figure 2-10. System > Information page - Flow Gateway internal

Information

cascade-gateway

System status:	OK
System date:	Jun 4, 2016 4:37:09 PM EDT
System uptime:	Up since Jun 2, 2016 11:57:36 AM
Load average for last minute:	0.14
Memory (used / free):	3,760,612 / 4,429,084 kB
Swap (used / free):	0 / 7,807,984 kB
Disk space (used / available):	6,064,732 / 17,160,268 kB
Kernel version:	2.6.32-573.12.1.el6.rvbd.1.x86_64
Product release version:	10.9 (release 20160601_1019)

- **NetProfiler Status -** Shows the addresses, names, and status of the NetProfiler appliances to which the Flow Gateway is sending traffic information. It also shows the number of flows that the Flow Gateway reported to the NetProfiler or NetExpress during the most recent 1-minute reporting period.

Figure 2-11. System > Information page - NetProfiler Status

NetProfiler

IP Address	Name	Status	Number of Flows Sent (Last Update)
10.38.133.134	cascade-profiler	OK	30847
10.38.131.73	cascade-profiler	OK	30847
10.38.130.91	cascade-profiler	OK	30847
10.38.131.253	cascade-profiler	OK	30847

- **Storage Status** - (Does not apply to the Gateway Virtual Edition.) The Overall status of the **Flow Gateway** storage system can be:
  - Green - OK; everything performing normally
  - Yellow - Warning; low disk space
  - Red - Alert; an alert condition is displayed

Figure 2-12. System > Information page - Storage Status

- **Storage Status Drives or Partitions Subsection** - 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

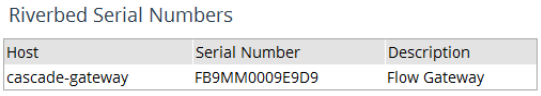
  In addition to the status messages, an image of the chassis is displayed to indicate the location of disks drives. The image shows a red box outline over the location of a disk drive that is missing or reporting a problem. Hover your mouse over the red box to display the name and serial number of the disk drive.

  The image indicates the good disk drives with gray boxes over their locations.

Figure 2-13. System > Information page Storage Status section

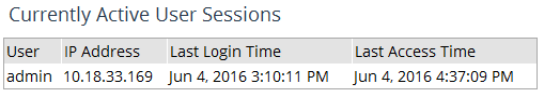
- **Riverbed Serial Numbers** - Serial number of the Flow Gateway.

Figure 2-14. System > Information page - Riverbed Serial Numbers



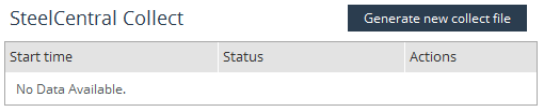
- **Currently Active User Sessions** - List of users logged in to the Flow Gateway.
- **SteelCentral Collect** - Troubleshooting feature. If you need assistance on a problem, a Riverbed Support engineer may ask you to click **Generate new collect file** to run a feature that collects information about the internal status and performance of the product. The Status column in this section displays **Running** while internal data is being collected. It may require 20 minutes to an hour for the data to be collected.

Figure 2-15. System > Information page - Currently Active User Sessions



When data collection has completed, the Status column displays Completed and the Action column displays a links for downloading or deleting the data file. You can download the collected data file to your local system and send it to the Riverbed engineer for analysis.

Figure 2-16. System > Information page - SteelCentral Collect



Audit reports

For information about changes and activities occurring on the Flow Gateway, the System > Audit Trail page enables you to generate a report of all significant configuration and usage activities that have occurred on the Flow Gateway. Running and saving audit reports is described in Chapter 5, “Audit trail reports.”

CHAPTER 3 Configuration

This chapter describes configuration of the SteelCentral™ Flow Gateway. It chapter includes the following sections:

Appliance security configuration is described in Chapter 4, "Appliance security."

UI Preferences

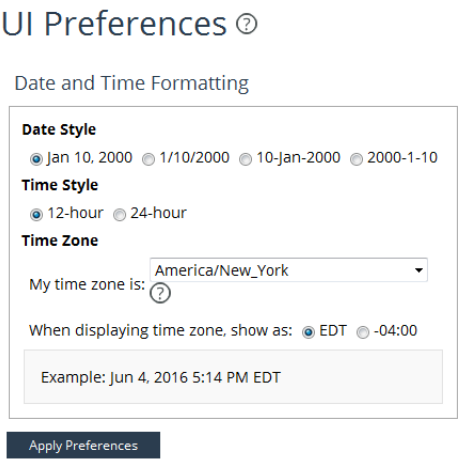
The Configuration > UI Preferences page controls:

- **Date Style** - the date convention used throughout the displays.
- **Time Style** - the time convention - AM/PM or 24-hour day - used throughout the displays.
- **Time Zone** - the time zone for your user account. 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 rather than the Country/Zone convention or its abbreviation.

  You can display the time zone either by its name or as an offset from UTC.

Note that this time zone selection applies to only your user account. The Flow Gateway also has its own system time zone setting.

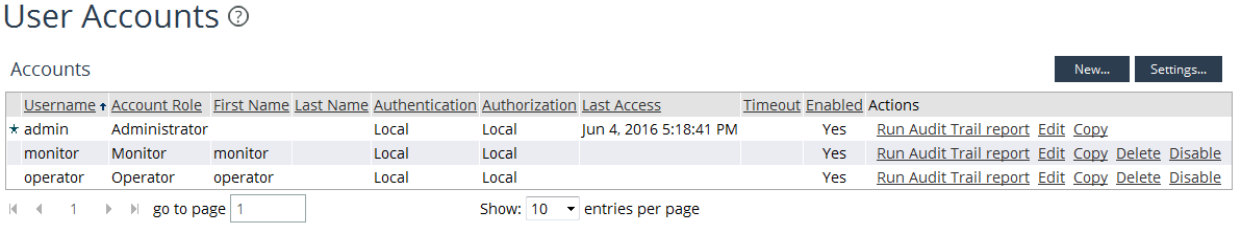
Figure 3-1. Configuration > UI Preferences page



User Accounts

Administrators create new accounts by clicking **New** on the Configuration > Account Management > User Accounts page. The New User Profile page has sections for specifying the user login name, the user's real name and email address, user role, time zone and authentication method (local or remote). If an email server is specified on the Configuration > General Settings page, then a notification will be sent to the user's email address when the password is changed.

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



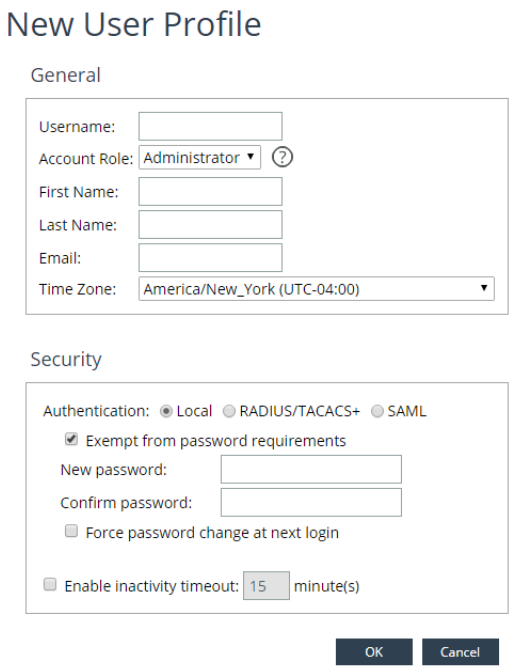
The New User Profile page has sections for specifying the user name, role, time zone and authentication method (local or by remote authentication). It also controls password characteristics. On this page you can exempt the user account from the strict password requirements that are defined on the Global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

Account permission levels

The permissions associated with the user roles are as follows:

- **Administrator** - can add, delete, or modify the permissions of all other user accounts, and has access to all Flow Gateway functionality.
- **Operator** - can make all setting changes except for adding, deleting, or modifying user accounts and permissions.

Figure 3-3. Configuration > Account Management > User Accounts > New User Profile



- **Monitor** - can access all views, but cannot change settings.

Access and role considerations

Flow Gateway setup and administration tasks are assumed to be the responsibility of those with an Administrator account on the NetProfiler or NetExpress and a Administrator account on the Flow Gateway. However, users with Flow Gateway Operator accounts can perform all the setup and administration tasks described in this section except for managing Flow Gateway user accounts.

Managing user accounts

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).

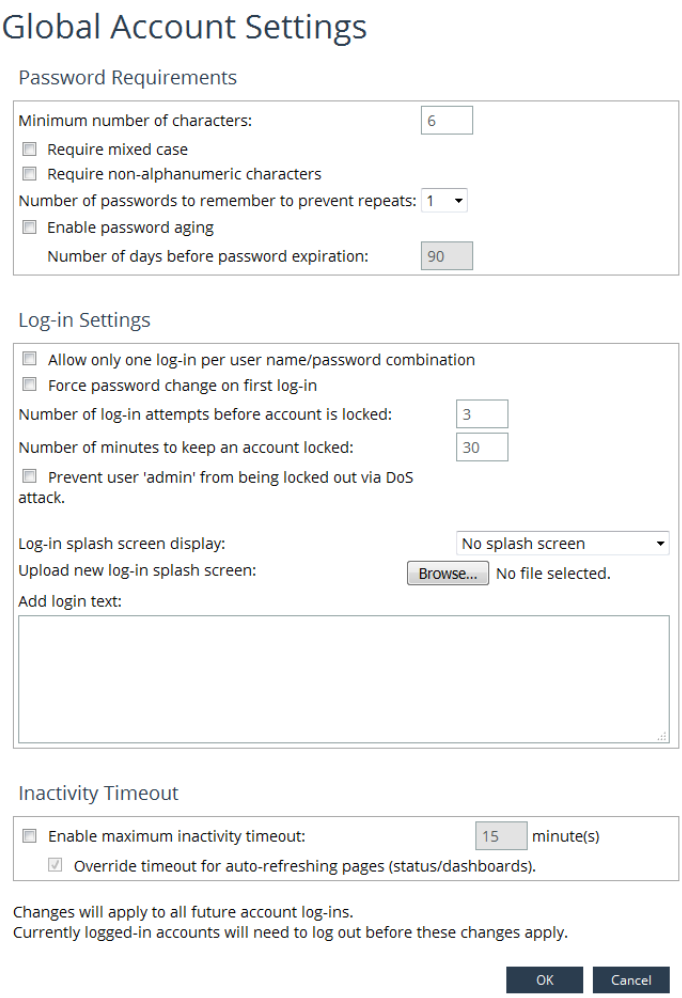
To add, audit, modify or delete a user account, change the password of another user, or to modify global account settings, you must be logged in as `admin` or another account with Administrator permission.

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:

Figure 3-4. Configuration > Account Management > User Accounts > Global Settings page



- **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. Flow Gateway 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 are cannot be modified when the appliance is in the Strict Security mode.

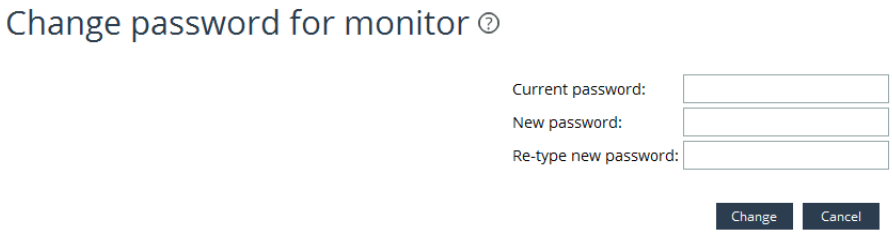
Passwords

Users with Operator or Monitor privileges can change their own passwords on the Configuration > Change Password page. Use this page to change the password of the user account under which you are logged in.

Administrators can replace the password on any user account, including their own, by going to the Configuration > Account Management > User Accounts page and using the Edit feature for the account. Therefore, the Change Password page is not displayed on Administrator accounts.

If configured, the appliance sends a notification of the password change to your email account..

Figure 3-5. Configuration > Change Password page



Users with Administrator privileges can change passwords on all accounts on the Configuration > Manage Accounts > User Accounts page.

Remote authentication and authorizationi

The Configuration > Account Management > Remote Authentication page specifies the sequence in which Flow Gateway checks authentication sources when a user logs in. It also provides tabs for setting up authentication and authorization using RADIUS, TACACS+ or SAML 2.0.

Types of authentication and authorization

Flow Gateway authenticates and authorizes user logins in three ways:

- Authenticated and authorized by Flow Gateway - The user has an account on Flow Gateway. This account specifies their login credentials and their user role. If Flow Gateway 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 Flow Gateway - The user has an account on Flow Gateway. This account specifies their user role, but not their login credentials. It specifies that their credentials are to be authenticated remotely. If Flow Gateway 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 Flow Gateway. When the user attempts to log in, Flow Gateway uses a remote authentication server to both authenticate their login credentials and authorize permissions based on their user role.

Flow Gateway can use RADIUS, TACACS+ or SAML 2.0 authentication servers.

Authentication sequence

When Flow Gateway is in the SAML 2.0 authentication mode, it does not log a user on unless the user can be authenticated by a SAML Identity Provider (IdP). Users cannot be authenticated locally or by RADIUS or TACACS+ when SAML authentication is enabled.

When Flow Gateway is not in the SAML 2.0 authentication mode, it logs a user on if the user can be authenticated locally or by RADIUS or TACACS+. The authentication sequence when Flow Gateway is not in the SAML 2.0 authentication mode proceeds as follows.

Flow Gateway always checks its local database first to authenticate a user's login credentials. If it cannot authenticate the user locally, it attempts to authenticate the credentials using the protocol specified in the Authentication Sequence section of the page.

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

Flow Gateway 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, Flow Gateway contacts RADIUS servers in the order in which they are listed on the RADIUS tab. When searching for TACACS+ authentication, Flow Gateway 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, Flow Gateway 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, Flow Gateway 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 Flow Gateway to use RADIUS involves:

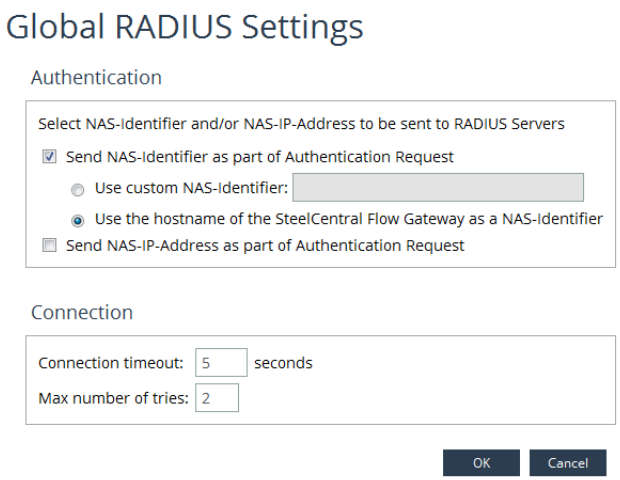
- Global Settings - Click Settings and specify the global RADIUS settings. These apply to all RADIUS servers that Flow Gateway connects to.
- Specifying RADIUS servers - Specify the IP address, port number, authentication protocol and shared secret of each RADIUS server that Flow Gateway is to use for authenticating users.
- Mapping roles to authorization attributes - For users who have no account on the appliance, map the Flow Gateway user roles to RADIUS authorization attributes.

Global RADIUS settings

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

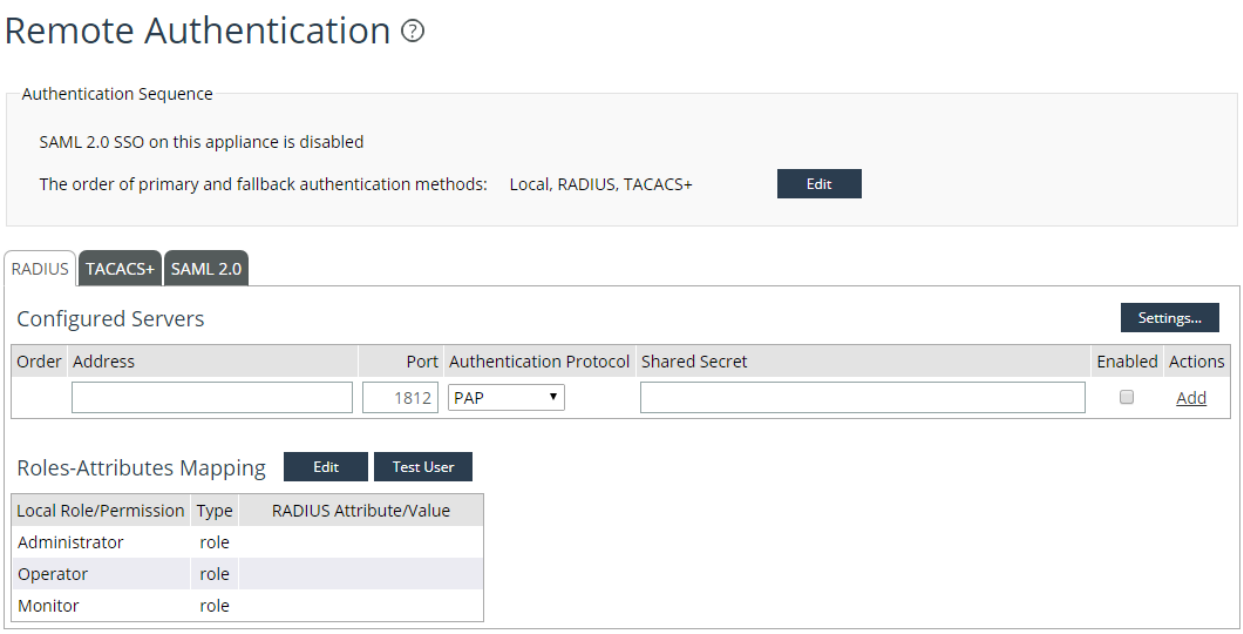
Figure 3-6. Global RADIUS Settings page



Specifying RADIUS servers

You can specify multiple RADIUS servers. Flow Gateway 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.

Figure 3-7. Configuration > Account Management > Remote Authentication > RADIUS tab



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 Flow Gateway 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 Flow Gateway 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.

Mapping roles to RADIUS authorization attributes

Users who do not have a Flow Gateway 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 Flow Gateway.

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 Flow Gateway must match for the user to be logged on.

To map the Flow Gateway 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 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, Flow Gateway attempts to log the user in using RADIUS authentication and reports the test results.

A user who does not have a Flow Gateway account logs in by entering the login name and password that are specified on the RADIUS server. Flow Gateway 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 Flow Gateway, 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 Flow Gateway 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 Flow Gateway 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 Flow Gateway logs the user on, it automatically creates an account for the user. However, subsequent logins by the RADIUS user do not create multiple Flow Gateway 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 family products. The Local-User attribute is for use with Riverbed Steelhead appliances. The appliance 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 Flow Gateway 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 Flow Gateway is to use for authenticating users.

3. Mapping roles to authorization attributes - For users who have no account on Flow Gateway, map the appliance user roles to TACACS+ authorization attributes.

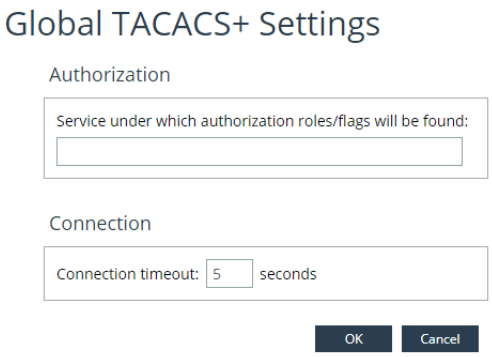
Global TACACS+ settings

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. Check with the TACACS+ server administrator if you need a service defined exclusively for Sensor users.

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

Figure 3-8. Global TACACS+ Settings page



Specifying TACACS+ servers

You can specify multiple TACACS+ servers. Flow Gateway 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.

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.

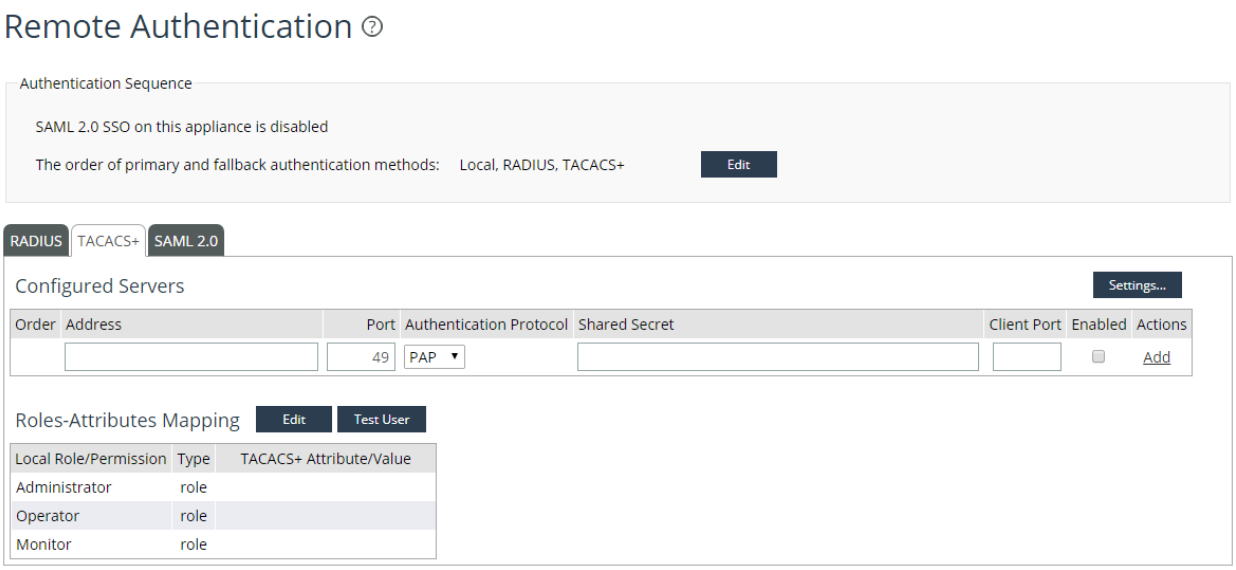
3. Select **Enabled** for the Flow Gateway to use the server.

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 Flow Gateway 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.

Figure 3-9. Configuration > Account Management > Remote Authentication > TACACS+ tab



Mapping roles to TACACS+ authorization attributes

Users who do not have a Flow Gateway 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 Flow Gateway.

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 Flow Gateway must match for the user to be logged on.

To map the Flow Gateway 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 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 Global TACACS+ Settings page.

5. If applicable, click **Add new attribute** to add another mapping.

6. Continue with the next user role that is to be authorized by TACACS+.

7. When the TACACS+ authorization attributes and values have been mapped to their corresponding 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, Flow Gateway attempts to log the user in using TACACS+ authentication and reports the test results.

A user who does not have a Flow Gateway account logs in by entering the login name and password that are specified on the TACACS+ server. Flow Gateway 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 Flow Gateway, 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 Flow Gateway finds a match between the TACACS+ definition of the authorization attribute and the Flow Gateway 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 Flow Gateway logs the user on, it automatically creates an account for the user. However, subsequent logins by the TACACS+ user do not create multiple Flow Gateway accounts for the user.

SAML 2.0 authentication

Users logging in to Flow Gateway can be authenticated remotely by a SAML 2.0 (Security Assertion Markup Language 2.0) Identity Provider (IdP). The IdP can also authorize a Flow Gateway user role for the user.

SAML authentication is configured on the IdP and on the SAML 2.0 tab of the Configuration > Account Management > Remote Authentication page.

Product behavior in SAML authentication mode

Enabling SAML 2.0 authentication makes the following changes to Flow Gatewa operation:

- All current user sessions are terminated when you enable SAML authentication. All new logins must be authenticated by a SAML 2.0 Identity Provider, with one exception: If "Allow local logins" was enabled on the SAML tab when SAML 2.0 was enabled, then an administrator can browse to <*product URL*>/local_login.php to access a login page.
- Logging out of Flow Gateway ends the session with Flow Gateway. It does not close sessions, if any, with the IdP that were part of the initial authentication process or those for any other Riverbed product involved in cross-product drill downs. Therefore, it is recommended that you close all browser tabs and close the browser when you are finished accessing Flow Gateway using SAML 2.0 authentication.
- Users whose user profile identifies them as being authenticated by SAML cannot log in through the REST API.

When SAML authentication is enabled on Flow Gateway, the log-in process proceeds as follows:

1. The user enters the name or IP address of Flow Gateway in a web browser.

2. Instead of displaying the login page, Flow Gateway redirects the user's browser to the IdP.

3. The IdP authenticates the user and redirects the user's browser back to Flow Gateway.

4. If the user does not have an account, Flow Gateway creates one.

5. If the user is to be both authenticated and authorized by SAML, then the IdP must send an assertion containing an authorization attribute, which the Flow Gateway administrator maps to a corresponding use role.

6. If the user is to be authenticated by SAML but not authorized by SAML, the user must already have an account on Flow Gateway. Flow Gateway uses the local account authorization information to log the user on with the specified user role.

7. Flow Gateway creates a web user interface session and displays the opening page in the user's browser.

Configuring for SAML authentication

Flow Gateway supports configurations that require XML metadata and also configurations that require individual properties. Setting up the Flow Gateway side of SAML authentication is generally as follows.

1. On the Configuration > Account Management > Remote Authentication page, provide the required IdP information in the top section of the SAML 2.0 tab.

2. If the IdP is to providing authorization in addition to authentication, then map the Flow Gateway user roles to their corresponding IdP authorization attribute values in the lower section of the page.

3. If user roles are to be assigned by Flow Gateway and not by the IdP, add or edit the user accounts on the Configuration > Account Management > User Accounts page. Specify the user role and select SAML authentication on the user profile popup. Ensure that at least one administrator account is specified before enabling SAML authentication.

4. On the SAML 2.0 tab of the Configuration > Account Management > Remote Authentication page, click **Test** to verify that SAML authentication is configured correctly and functioning.

5. After the SAML authentication test has completed successfully, click **Apply**. This saves your configuration and prepares Flow Gateway for SAML authentication.

6. When you are ready to terminate all current user sessions and restrict new user logins to SAML authentication, select **Enable SAML 2.0** and click **Apply**.

Specifying SAML properties

SAML properties are specified on the SAML 2.0 tab of the Configuration > Account Management > Remote Authentication page. Depending on which IdP you are using, entries or selections in the following fields and controls may be required.

NameID Attribute

When this field is left empty, Flow Gateway uses the value of the IdP NameID attribute as the user name for the user attempting to log in. This is typically the user's email address.

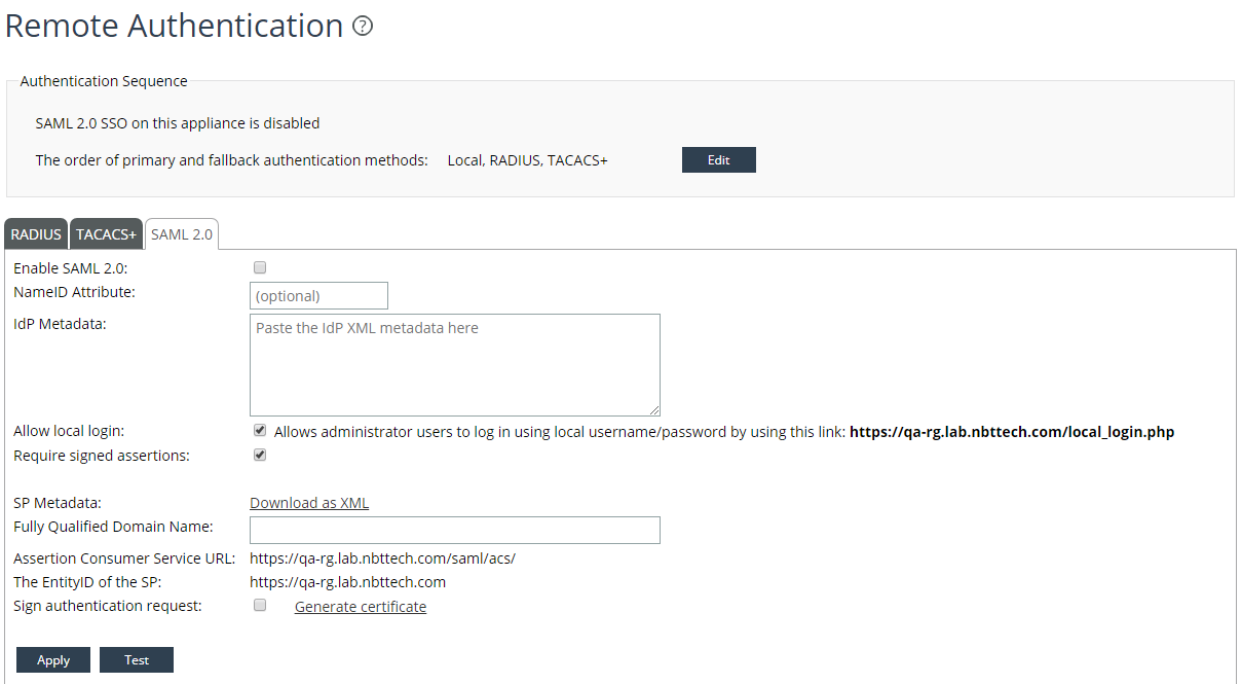
You can specify an alternative attribute for identifying the user's name. If the IdP is configured to use some other attribute to identify user's names, enter the name of that attribute in this field. Flow Gateway looks for the attribute you specify and uses its value as the user name.

Certain special characters are not accepted in user names. However, domain style names and email addresses are supported.

IdP Metadata

If your configuration requires Flow Gatewa to use Identity Provider metadata, paste it into the IdP Metadata box.

Figure 3-10. Configuration > Account Management > Remote Authentication > SAML 2.0 tab - properties



Allow local login

When SAML 2.0 authentication is enabled, the Flow Gateway web user interface login page is not displayed. However, you can allow administrators to log in to locally-authenticated administrative accounts. Select this check box to allow administrators to access a local login page. Record the link for administrators who may have no other means of logging in to Flow Gateway.

Require signed assertions

As an additional level of security, you can select this check box to require assertions from the IdP to be signed. When this checkbox is selected, the response from the IdP to Flow Gateway is signed with the IdP private key. This option requires the configured IdP metadata to contain the IdP certificate and public key. The public key is used to verify that an assertion received by Flow Gateway was signed with the IdP private key and is therefore genuine.

SP Metadata

If your configuration requires Flow Gateway “Service Provider” XML metadata, click **Download as XML** to generate a file containing the metadata. Copy and paste the contents of this file into the IdP so it can communicate with Flow Gateway.

Fully Qualified Domain Name

This field is automatically filled in with the fully qualified domain name of the Flow Gateway. The field can be edited if necessary. This is used when Flow Gateway redirects the user’s browser to the IdP and the IdP redirects the browser back to Flow Gateway.

Assertion Consumer Service URL

If an IdP does not support obtaining the URL of the assertion consumer (Flow Gateway in this case) from the Service Provider metadata, then the IdP may require manual configuration. If manual configuration is required, add this URL to the IdP so it can access the Flow Gateway assertion consumer service.

The EntityID of the SP

This is the entity identifier of the Flow Gateway. It is based on the value in the Fully Qualified Domain Name fields and is the login URL.

Sign authentication request

Select this checkbox to require signing on the authentication request that Flow Gateway sends to the IdP. This requires generating a client certificate and adding it to the IdP. Authentication requests are then signed with the Flow Gateway SAML private key and verified by the IdP using the Flow Gateway SAML certificate and public key.

Click **Generate certificate** to generate the client certificate. The certificate is stored in Flow Gateway and listed on the Local Credentials tab of the Configuration > Appliance Security > Encryption Key Management page. If you need to use your own certificate, you can change the certificate on the Encryption Key management page.

Apply

Click **Apply** to save changes. If you navigate away from the page or end your browser session with Flow Gateway without clicking Apply, any changes you have made to the settings on this page are lost.

Test

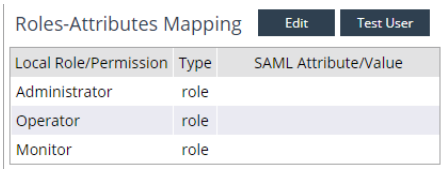
The Test button causes Flow Gateway to send an authentication request to the IdP. The user running the test is presented with a log in screen. They log in with a name known to the IdP. The IdP authenticates the user and sends Flow Gateway the user's name, user role and SAML attributes. Flow Gateway displays these on a test screen for the user to verify.

This test should run successfully before you enable SAML 2.0 authentication on Flow Gateway.

Mapping user roles to SAML authorization attribute values

Authorization attributes sent to Flow Gateway by the IdP are mapped to Flow Gateway user roles in the lower section of the Configuration > Account Management > Remote Authentication page SAML 2.0 tab.

Figure 3-11. Configuration > Account Management > Remote Authentication > SAML 2.0 tab - mapping



Users who do not have a Flow Gateway account must have both their authentication information (login name, password) and their authorization information (role; permissions) specified on an authentication server. For SAML authentication and authorization, the Flow Gateway user roles must be mapped to the corresponding SAML authorization attribute values that the IdP sends.

Ensure that you know the authorization attributes the SAML administrator is using and what values are assigned to them. The values on the IdP and the values on Flow Gateway must match for the user to be logged on.

To map the Flow Gateway user roles to SAML authorization attributes

1. Click **Edit** in the Roles-Attributes Mapping section of the SAML 2.0 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. Enter the SAML authorization attribute as it is defined on the IdP.
4. Enter the value that the IdP sends to authorize this user role.
5. If applicable, click **Add new attribute** again to add another mapping.
6. Continue with the remaining user roles to be authorized by SAML.

7. When the user roles and permissions have been mapped to their corresponding SAML authorization attributes and values, click **Save**.

8. Click **Test User** to open a page on which you can specify a user name and password to be tested. Flow Gateway sends an authentication request to the IdP. The IdP authenticates the user and sends Flow Gateway the user's name, user role and SAML attributes.

   Flow Gateway displays this information on a test screen for you to check.

SAML authorization examples

Depending on its configuration, the IdP may send authorization attribute values regardless of how the remotely-authenticated accounts are authorized on Flow Gateway. There are two authorization cases for a user who is authenticated by SAML.

SAML authentication; Local authorization

If you create a user account on Flow Gateway and set it for SAML authentication, Flow Gateway uses the role you specified for the account and ignores any authorization values received from the IdP for that account.

For example, assume that an account for user "someone@abc.com" is specified on the IdP and also manually created on Flow Gateway. Assume that the value of the IdP authorization attribute maps to the Administrator role, but the user profile setting on NetProfiler or NetExpress specifies the Monitor role.

When the user logs in and is authenticated by the IdP, Flow Gateway ignores the IdP authorization attribute value and logs the user in with the Monitor role.

SAML authentication; SAML authorization

Initially, no account for this type of user exists on Flow Gateway. The first time the user logs in, Flow Gateway creates an account using the authentication and authorization it receives from the IdP. (If no authorization information is received, then no user account is created and the login attempt fails.)

On each subsequent login, Flow Gateway assigns the user role based on the information it receives from the IdP during that login.

The user role assigned to this automatically-created account cannot be changed on Flow Gateway. If you need to change the user role of an automatically-created user account, you can delete the account and recreate it manually as a SAML-authenticated, locally authorized user account. From then on, the user will still be authenticated by SAML, but the account will use the role you specify instead of the role mapped to the IdP authorization attribute.

Note on attribute values for role mapping

Flow Gateway does not support comma separated values within SAML attributes. The value of any attribute sent to Flow Gateway in an IdP assertion is treated as a single string and is not parsed. For example, if an assertion sent to Flow Gateway contains a value such as:

```
<AttributeStatement>
    <Attribute Name="MyAttribute">
        <AttributeValue>A, B, C</AttributeValue>
    </Attribute>
</AttributeStatement>
```

Flow Gateway treats the <AttributeValue> as a single string and does not parse it.

RESTful API access

Information that the appliance collects is made available for use by other products through a RESTful API. Access to the API is protected by authentication. The API can authenticate users by Basic, Session (Cookie) or OAuth 2.0 authentication. The Configuration > Account Management > OAuth Access page generates an access code that allows a service or script to gain access to the RESTful API without providing a user name and password. The appliance uses the access code to authenticate the script or service instead of login credentials.

Figure 3-12. Configuration > Account Management > OAuth Access page

To generate an access code

1. On the OAuth Access page, click **Generate new**.
2. Enter a short description for the script that will be accessing the RESTful API and click **OK**. The appliance generates an access code and displays it in a popup window.
3. Copy the access code and save it for use in your application or script.
4. Close the OAuth Access Code window and observe that there is now an entry for your access code on the OAuth Access page.

You can view the access code or delete it using the controls on the OAuth Access page.

NetProfiler Export

Specify the addresses of NetProfiler or NetExpress appliances that are to receive traffic flow data from the Flow Gateway.

To specify NetProfiler addresses

To specify NetProfiler or NetExpress appliances that are to receive traffic flow data from the Flow Gateway:

1. Go to the Configuration > NetProfiler Export page.
2. If the Flow Gateway is receiving data from one or more NetShark appliances, specify the IP address of the NetProfiler or NetExpress to which the NetShark appliances should synchronize their definitions for ports, port groups and applications.
3. If you want the Flow Gateway to save data when a NetProfiler destination is unreachable and send it after the connection is reestablished, select the “Enable flow buffering for offline NetProfilers” option.
4. Click **Add New Entry** to open a blank entry for specifying a destination NetProfiler.

5. In the NetProfiler IP Address box, enter the IP address of the management interface for a Standard NetProfiler or the address of the Analysis Module for an Enterprise NetProfiler.

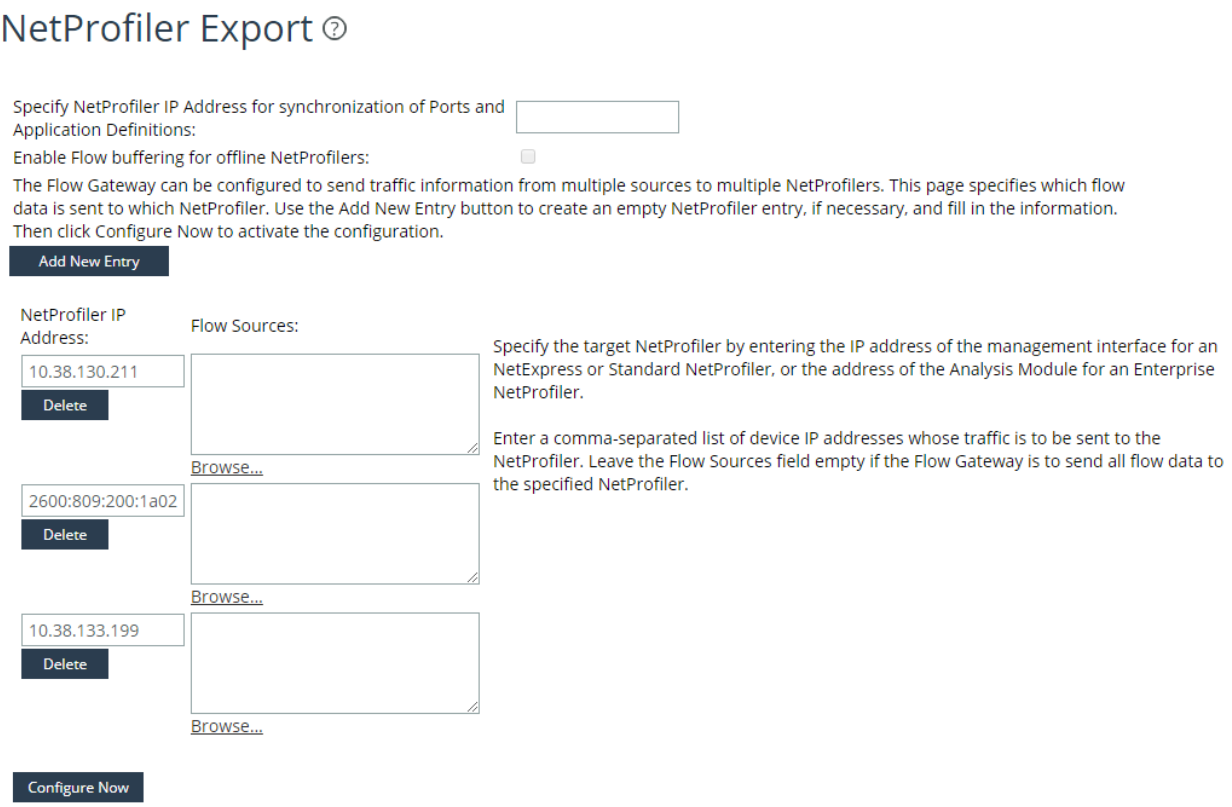
6. In the Flow Sources box, either:
   - Leave the box blank to forward all flow data to the specified NetProfiler, or
   - Enter a comma-separated list of the IP addresses of flow source devices whose traffic is to be sent to the NetProfiler.

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

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

The Flow Gateway begins sending flow data to the NetProfiler or NetExpress within 5 minutes after you click Configure Now.

Figure 3-13. Configuration > NetProfiler Export page



NetShark synchronization

A NetShark can export data to two destinations. Each destination can be a NetProfiler, NetExpress or Flow Gateway. When a NetShark is exporting flow data to a Flow Gateway, the Flow Gateway can export the data to up to 20 NetProfiler or NetExpress appliances.

In order to synchronize its port, port group and application definitions with a NetProfiler, the NetShark must know which NetProfiler to synchronize with. The Flow Gateway Configuration > NetProfiler Export page provides a text box in which you can specify the IP address of the NetProfiler that the NetShark should synchronize with.

A NetShark sending data to a Flow Gateway cannot synchronize its definitions with a NetProfiler unless the NetProfiler IP address is specified on the Configuration> NetProfiler Export page. If multiple NetShark appliances are configured to send flow data to a Flow Gateway, they will all synchronize to the one, specified NetProfiler.

The presence or absence of this NetProfiler specification has no effect on other devices that are sending flow data to the Flow Gateway.

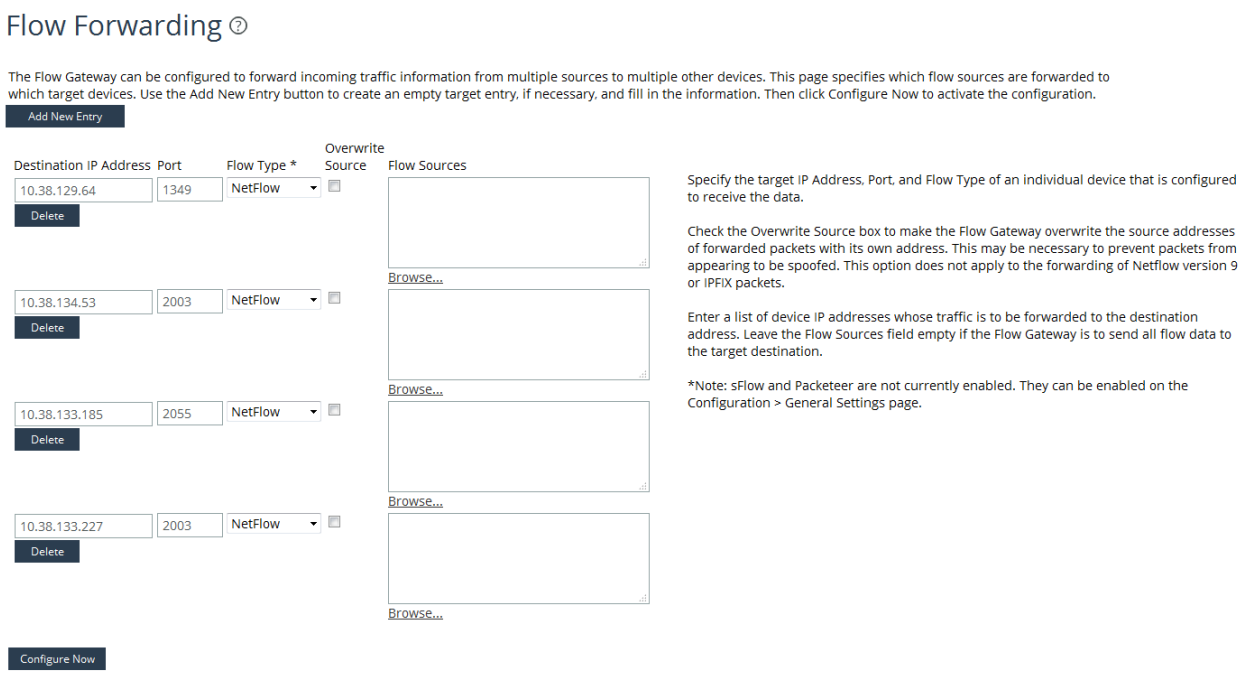
Flow data forwarding

The Flow Gateway can forward flow data to five destinations. Unlike the data sent to NetProfiler or NetExpress appliances, which is compressed and encrypted, the flow data forwarded to other destinations is sent in the format in which it was received.

If you are using a flow collector with a limited capacity for sending flow data to monitoring devices, you can conserve that capacity by sending the data to Flow Gateway instead of to the original destination. Flow Gateway can then transparently forward the data to the original destination, while also sending it to the NetProfiler or NetExpress appliances.

Additionally, you can use the **Overwrite Source** option to make the forwarded data appear to be coming from Flow Gateway. 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 3-14. Configuration > Flow Forwarding page



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. For IPFIX data, select NetFlow.

4. If you need to have the data identified as coming from the Flow Gateway, select **Overwrite Source** to use the Flow Gateway 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.

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

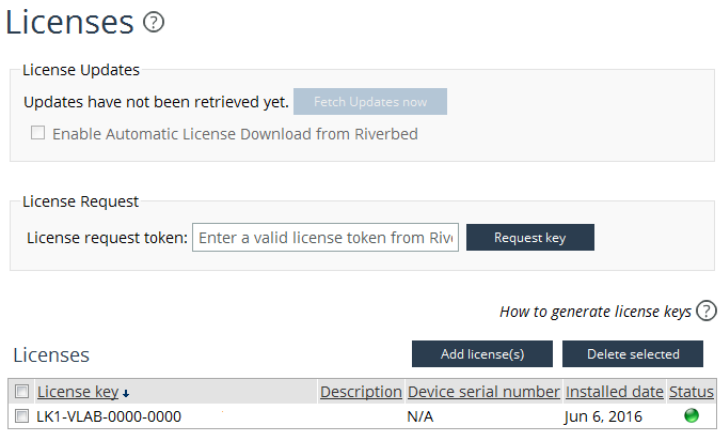
All flow data that is available for forwarding to other devices is also processed and sent to NetProfiler or NetExpress. Flow data cannot be forwarded without also reporting it to NetProfiler or NetExpress.

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 (virtual edition only)

The Flow Gateway requires 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 3-15. Flow Gateway virtual edition Configuration > Licenses page



To activate a license, you enter a token that you receive when you purchase the license. The Flow Gateway 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 to 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.

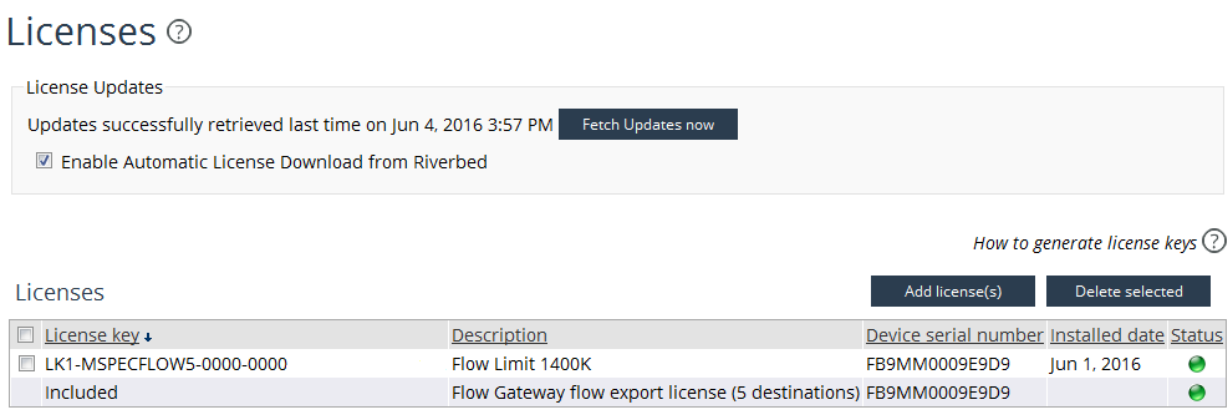
If you purchase and download a license for a higher capacity than a current license, the appliance uses the license with the higher capacity.

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.

Licenses (hardware-based appliance only)

The appliance requires 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 3-16. Configuration > Licenses page



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 installation guide.

General Settings

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

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

Note: Flow Gateway can be placed on both IPv4 and IPv6 networks (dual homed). The Management Interface Configuration section and the Auxiliary (AUX) Interface Configuration section accept both IPv4 and IPv6 addresses. All other sections on this page that include address specifications accept either IPv4 or IPv6 addresses, except for the Baseboard Management Controller section. Where present, the Baseboard Management Controller section accepts an IPv4 address. The Baseboard Management Controller can be placed on an IPv6 network by accessing its user interface through the console port.

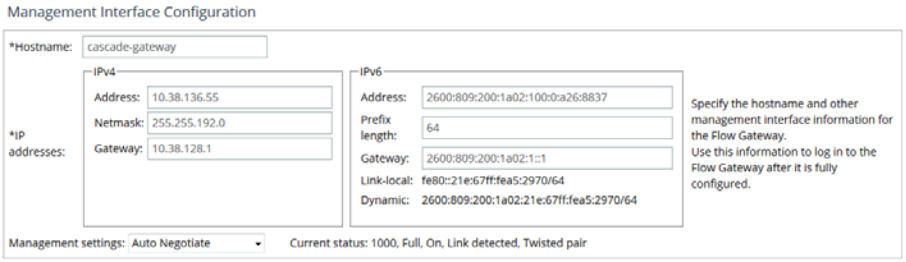
Management Interface Configuration

Go to the Configuration > General Settings page to change the host name, IP address and other information necessary for the Flow Gateway to be reachable on your network. The Management Interface Configuration section of the General Settings page controls how the Flow Gateway connects to the network.

Note: If you were to misconfigure the control interface settings, the Flow Gateway would become unreachable, and it would be necessary to reinstall the software in order to access it.

Changes you make on the Configuration > General Settings page take effect when you click **Configure Now** at the bottom of the page. If your changes include the host name or IP address of the Flow Gateway, your browser session will be terminated and you must log in using the new information.

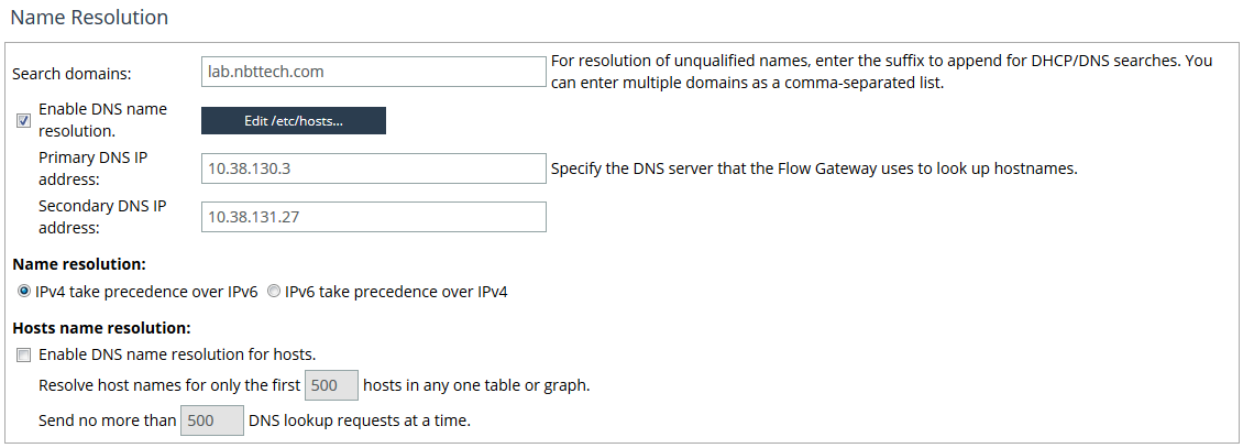
Figure 3-17. Configuration > General Settings page Management Interface Configuration section



Name Resolution

Go to the Configuration > General Settings page Name Resolution section to specify how the Flow Gateway is to resolve host names and network device names.

Figure 3-18. Configuration > General Settings page Name Resolution section



Search domains

When the Flow Gateway looks up the address of host name that does not include a domain name, it appends a specified domain name to the host name in order to perform the search. You can specify multiple search domains as a comma-separated list. The Flow Gateway tries to resolve the host name using each domain in the search list in the order in which it appears in the list.

DNS servers - You can enable or disable the resolution of host names and addresses. You can specify the addresses of the DNS servers that the Flow Gateway accesses to look up the host name associated with an IP address or the IP address associated with a host name. If the primary DNS server is unreachable, the Flow Gateway uses the secondary DNS server. Leaving the primary and secondary DNS server address fields blank disables the use of DNS.

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.

Name resolution

If Flow Gateway can resolve names on both IPv4 and IPv6 networks, you can specify which takes precedence.

Host name resolution

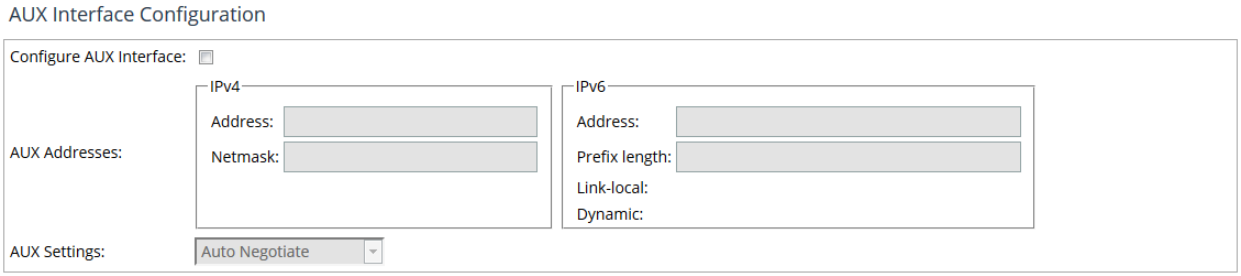
This section enables DNS name resolution for hosts and sets limits to protect your DNS server from excessive traffic loads. You can limit the number of host lookups that the Flow Gateway appliance requests at one time. For example, if you specify that the Flow Gateway is to resolve no more than 1000 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.

Auxiliary Interface Configuration

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

Figure 3-19. Configuration > General Settings page Aux interface configuration section



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 Flow Gateway 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, 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.

Configuring interfaces for separate data and control networks

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

- There are two separate networks with non-overlapping IP addresses.
- The Flow Gateway 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, sFlow, Packeteer FDR, etc.) to the Aux port of the Flow Gateway 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 Flow Gateway 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.

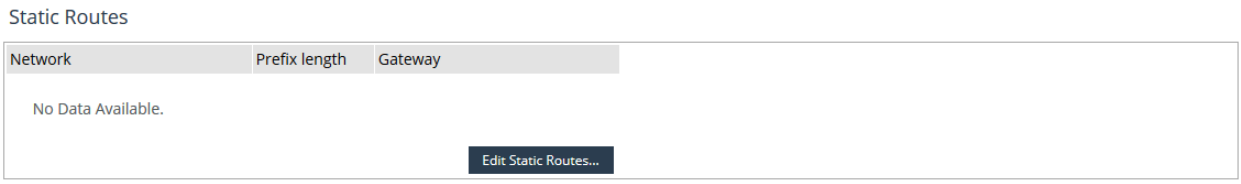
3. If any static routes were added for the configuration that used separate networks for data and control, remove them in the Static Routes section of the page.

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

Static Routes

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 3-20. Configuration > General Settings page Static Routes section



Time Configuration

The time zone selected in the Configuration > General Settings page Time Configuration section is the time zone used by the Gateway software itself. The system time zone setting is independent of the user account time zone setting on the Configuration > UI Preferences page.

The system time zone is typically set to the time zone in which the Gateway is located, but that is not a requirement. For example, you could set it to the same time zone as the NetProfiler or NetExpress to which it is reporting. Alternatively, it could be set to the time zone of the location in which the most network operations people are working, or the time zone that your organization uses for logging events for possible future analysis.

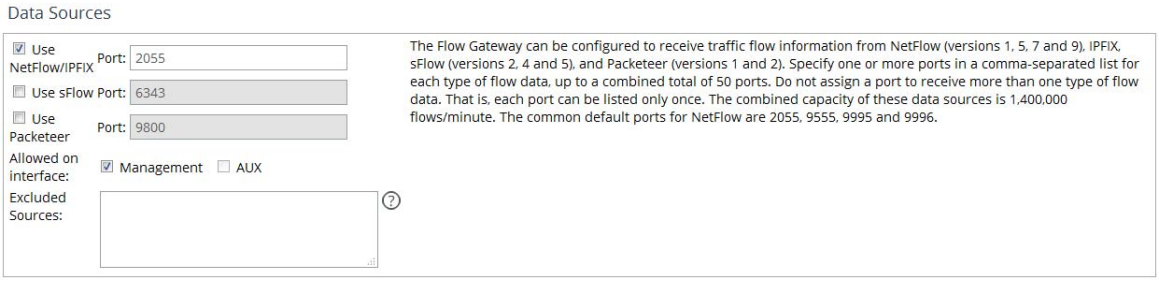
You can select a time zone using the Continent/City convention, the Country/Zone convention, or the time zone abbreviation. However, to ensure that the selected time zone is automatically adjusted for summer and winter time changes, it is preferable to select it using the Continent/City convention instead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

Figure 3-21. Configuration > General Settings page Time Configuration section

Data Sources

The Flow Gateway can be configured to receive traffic flow information from devices using NetFlow (versions 1, 5, 7 and 9), IPFIX, SteelFlow Net, 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.

Figure 3-22. Configuration > General Settings page Data Sources section



You can also exclude data sources. Flow Gateway 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.

To specify the types of source data

1. Go to the Configuration > General Settings page and scroll to the Data Sources section.
2. Select the data type and enter the port number or numbers on which Flow Gateway is to receive it. Flow Gateway does not require flow data to use particular ports. However, you must identify the port that the sending device is configured to send to. Each port can receive only one type of flow data. For SteelFlow Net select NetFlow.
3. Click **Configure Now** at the bottom of the page to apply the settings.

The number of sources that you can configure to send flow data to Flow Gateway depends on the amount of data each is sending. The total from all sources combined must not exceed your licensed capacity. Refer to your license agreement for the flow capacity of your Flow Gateway.

When Flow Gateway 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.

To exclude data from specified sources

1. Go to the Configuration > General Settings page and scroll to the Data Sources section.
2. In the Excluded Sources box, specify the data sources to be excluded. These can be specified as:
   - IP address
   - Range of addresses in CIDR format
   - Comma-separated list of IP addresses, CIDR blocks, or both
3. Click **Configure Now** at the bottom of the page to apply the settings.

Excluded data sources cannot be forwarded to other devices.

Additional data filtering

In addition to excluding all flow data from a specified flow data source, you can drop incoming flow data based on its IP address, protocol, and/or port. This excludes the specified flow data regardless of which device is sending it. The excluded flow data does not count toward the license limit.

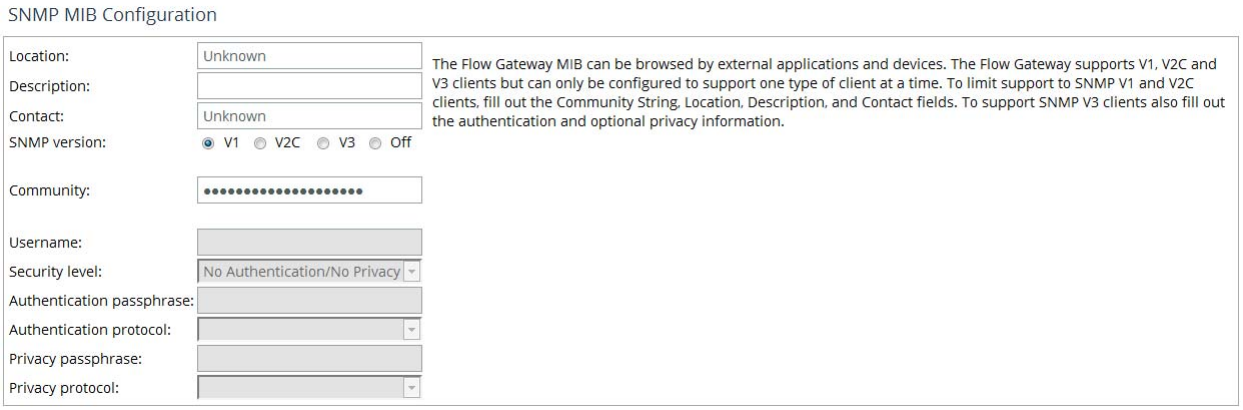
This type in raw data filtering requires creating a filter specification in an XML file and loading it into the Flow Gateway using the command line interface. Instructions are provided in Knowledge Base article S28800, “Incoming Flow Filtering on a SteelCentral Flow Gateway,” which is available on the Riverbed Support site.

SNMP MIB Configuration

The Flow Gateway MIB can be browsed by external applications and devices. The Flow Gateway supports browsing by Version 1, 2c and 3 clients, but it can support only one type of client at a time. This choice is made on the Configuration > General Settings page in the SNMP MIB Configuration section.

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 3-23. Configuration > General Settings page SNMP MIB Configuration section



The SNMP MIB configuration fields on the Configuration > General Settings page include:

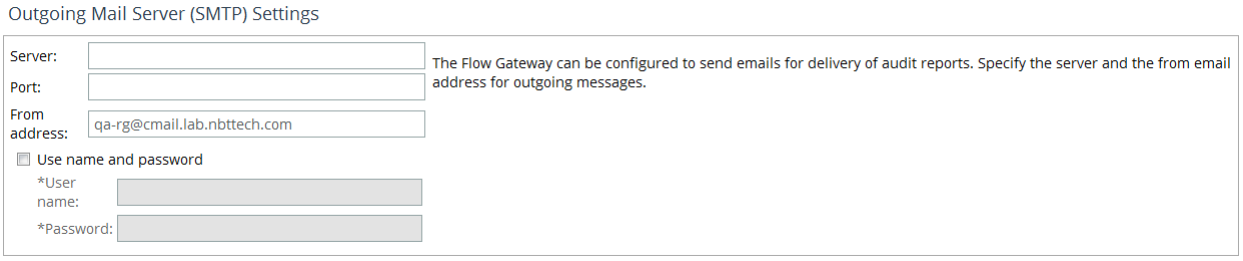
- **Username** - SNMP security name that the application attempting to browse the Flow Gateway MIB must use.
- **Authentication passphrase** - String that the application attempting to browse the Flow Gateway MIB must use to authenticate itself to Flow Gateway.
- **Authentication protocol** - Algorithm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

Outgoing Mail Server (SMTP) Settings

This section specifies the IP address or name and the port number of the mail server that the appliance uses when it sends email with audit reports and password change notifications. 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 3-24. Configuration > General Settings page Outgoing Mail Server (SMTP) Setting section



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 Flow Gateway 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 Flow Gateway 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 Flow Gateway 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.

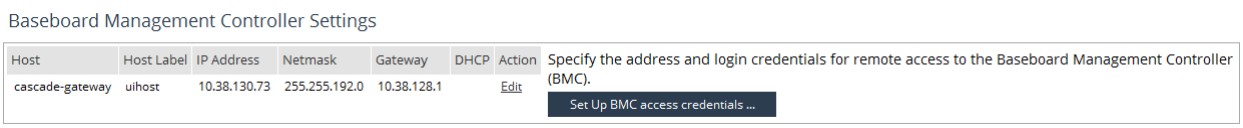
Use the Flow Gateway web user interface to assign login credentials to the BMC web user interface. Do not change the user name or password from within the BMC web user interface.

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.

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**.

Figure 3-25. Baseboard Management Controller Settings section of the Configuration > General Settings page



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**.

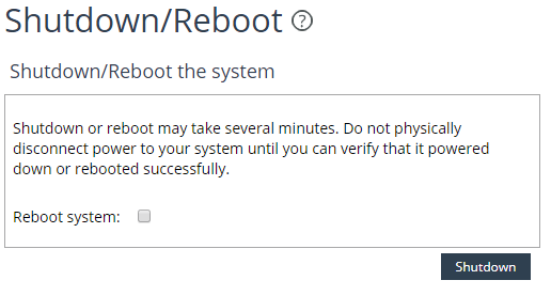
Shutdown/Reboot

The System > Shutdown/Reboot page enables users with Administrator accounts to shut down or reboot the appliance

- Select the **Reboot** option if you want to restart the product without powering off the appliance.
- Click **Reboot** or **Shutdown**, as applicable, to initiate the process.

Note: If you shut down the appliance, do not disconnect chassis power until the appliance has powered off.

Figure 3-26. System > Shutdown/Reboot page



Updates

When a SteelCentral™ NetProfiler or SteelCentral™ NetExpress is updated, it automatically transfers the update files to the downloads directory of each Flow Gateway that is connected to it. Each appliance checks its download directory twice per day. When it detects an update package that 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 your product is up to date and no updates are available.

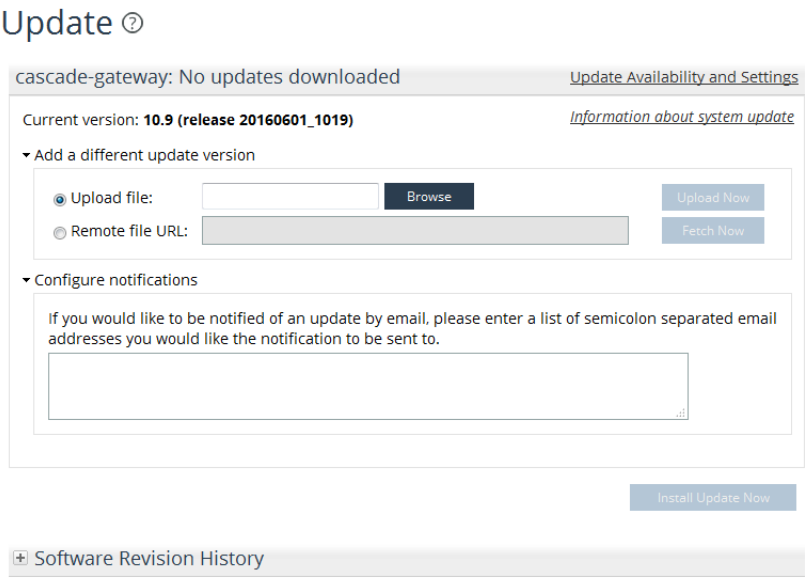
If an update package has been automatically downloaded to the appliance, the System > Update page displays a popup message asking you if you want to add it to the list of update packages available for installing. Click **OK** to add it to the **Update to version** list.

If there is no popup message in front of the System > Update page, then no new update package has been downloaded since the last one was added to the list. Update packages are downloaded from the NetProfiler or NetExpress, or from the Riverbed download web site.

To check if there is an update package on the NetProfiler or on the download site that is ready to be downloaded, click **Update Availability and Settings** in the title bar.

The title bar of the first section of the System > Update page displays a message to tell you if a new update package has been downloaded and is available for installation. If an update is available, it is listed in the **Update to version list**. If no updates are available for installation, the Update to version list does not appear.

Figure 3-27. System > Update page



If you want to install an update that you have on your local machine or on a remote server, you must load that version into the appliance before it can be installed. Refer to the on line help system for details.

To update this appliance,

- In the Update to version list, select the version to which you want to update.
- Click Install **Update Now**. The update process begins immediately. All users are logged off the appliance. Your browser is redirected to a page that displays a progress bar indicating the percentage of completion of the update and an estimate of how much more time is required.
- After update process completes, your browser is redirected to the login page.

When you log back into the appliance, you can return to the Update page and check that the current version is the version to which you have updated.

CHAPTER 4 Appliance security

Overview

SteelCentral 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

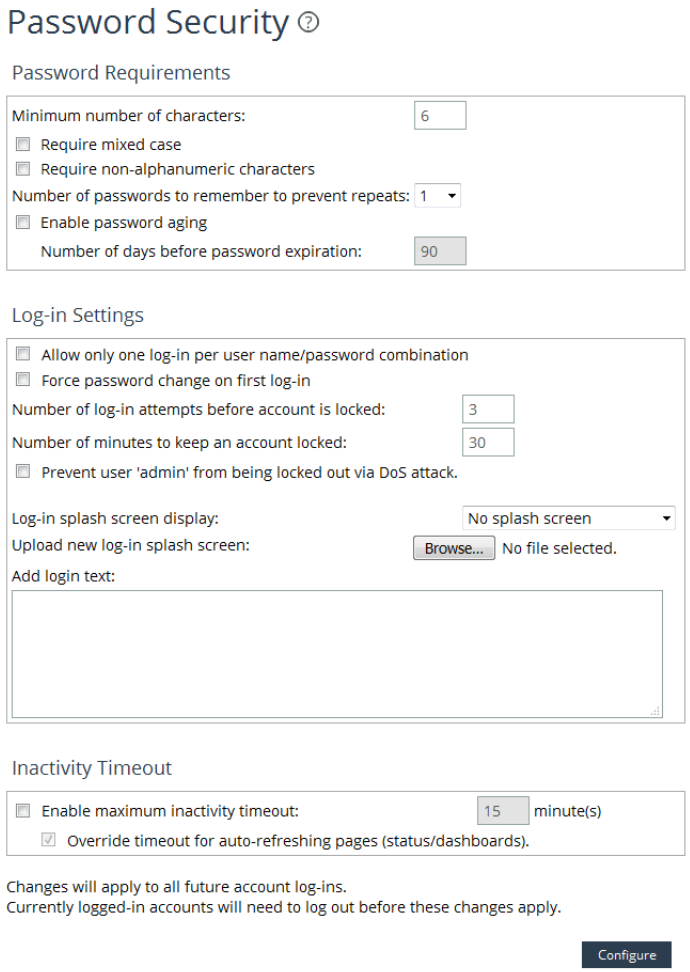
This chapter describes these features. Additional security-related features include:

- 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 4-1. Configuration > Appliance Security > Password Security page



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. Flow Gateway 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.

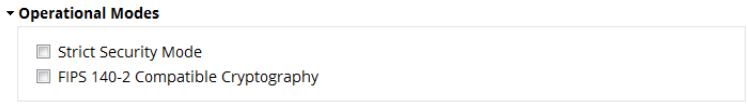
Note: Do not change the Shell Access selection in the Accounts section unless you understand the impact. Shell access cannot be restored once it is disabled.

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 4-2. Configuration > Appliance Security > Security Compliance page Operational Modes section



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:

- Selects enhanced password protection.
- Restricts access to the appliance.

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.
- 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.

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

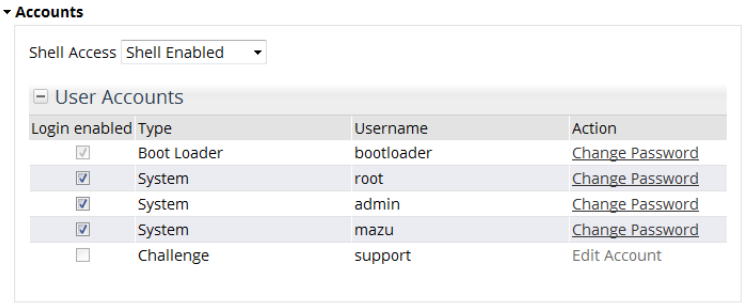
When both the Strict Security mode and FIPS 140-2 Compatible Cryptography are enabled, the appliance is restricted to the limitations of each. The combined effects of enabling both options are:

- 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.

Accounts

The Accounts section enables you to specify a shell access mode and to change the passwords of system accounts.

Figure 4-3. Configuration > Appliance Security > Security Compliance page Accounts section



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 - not ssh accessible; 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 appliance cannot download updates from NetProfiler 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

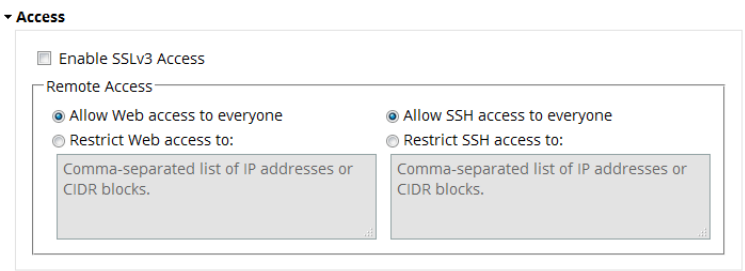
The Shell Disabled mode permanently disables login access to the shell. This is useful in environments that must not allow any form of shell access.

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 allows you to restrict access to the appliance by web browsers and SSH connections.

Figure 4-4. Configuration > Appliance Security > Security Compliance page Access section



Enable SSLv3 Access – The Enable SSLv3 Access option allows other systems to access Flow Gateway 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).

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 Flow Gateway 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 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.

Encryption Key Management

SteelCentral appliances use encryption for communicating with users and with 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

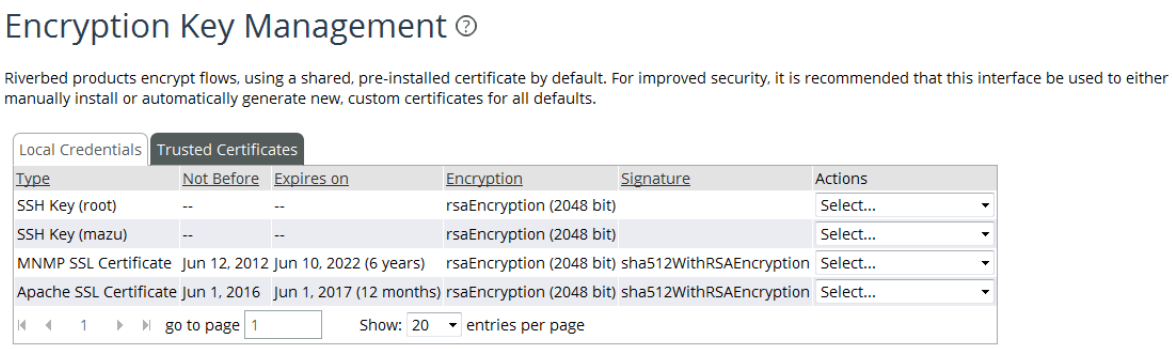
The Encryption Key Management page has two tabs:

- **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 4-5. Configuration > Appliance Security > Encryption Key Management page Local Credentials tab



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
- 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 4-6. Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab

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 NetShark, Flow Gateway or Cascade Sensor appliances that are sending data to the NetProfiler or NetExpress appliance. However, you can regenerate all the certificates. The process is the same.

If you regenerate or replace a self-signed certificate on the NetShark, Flow Gateway or Cascade Sensor appliance, you must install the new certificate 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 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.

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 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 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/7lPkpGbewNrl
   ...
   CeNBbPMkGZONosCnmZvSycY/wFoslx9ozPPG/dRQHGmm7z6Ktw==
   -----END RSA PRIVATE KEY-----
   ```

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

NetShark, Flow Gateway and Cascade Sensor appliances secure the following SSL connections using certificates:

- MNMP – NetProfiler or NetExpress communicating with other SteelCentral appliances
- Apache – NetProfiler or NetExpress communicating with users' web browsers

The certificates that are currently in use can be replaced by:

- Regenerating the certificate – The 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 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, identify the NetProfiler or NetExpress appliances that this appliance connects to.

On a Cascade Sensor, check the NetProfiler Status section of the Configuration > Information page. On Flow Gateway, check the NetProfiler Status section of the Overview page.

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 this appliance can connect to them.

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 appliance 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.
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.
4. On each NetProfiler or NetExpress that this appliance communicates with, go to the Configuration > Appliance Security > Encryption Key Management page Trusted Certificates tab.
5. Click **Add New Certificate** to open a window into which you can paste the new NetProfiler or NetExpress MNMP certificate.
6. Paste the new certificate into the Key/Cert field.

7. 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.

8. 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 the Trusted Certificates first, and then replace the MNMP private key in this appliance.

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 local appliance, and the entire CA certificate chain must be pasted into the Trusted Certificates section of the local appliance and every NetProfiler or NetExpress appliance that it connects to.

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 NetProfiler or NetExpress appliance that this appliance is to communicate with,

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+ZMA0GCSqGSIb3DQEBBAUAMA8xDTALBgNVBAMTBE1henUwHhcNMDYxMDAyMTY0M
zQxWhcNMTYwOTI5MTY0MzQxWjAPMQ0wCwYD05BPDxKbb8Ic6HBPDxKbb8Ic6HWpTJpzs
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdEYZUSgpyAcws5PDyr2GVFMI3dfPnl28hVavIkR8r05BPDxKbb8Ic6HWpTZMA0GCSqGSIb3DQEBBAUAM
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 NetProfiler or NetExpress appliance.

8. If this appliance connects to more than one NetProfiler or NetExpress, then perform Steps 1 through 7 on the second NetProfiler or NetExpress appliance.

9. After all the NetProfiler or NetExpress appliances that this appliance connects to 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 NetProfiler or NetExpress appliance, the final step is to add the end entity certificate and the private key as the Local Credentials for this appliance.

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-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7CkgI/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.

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 NetProfiler or NetExpress appliance that this appliance is to communicate with,

1. Copy the self-signed certificate, including the BEGIN and END statements. The certificate will be in a format such as:

```
-----BEGIN CERTIFICATE-----
MIIBsTCCARqgAwIBAgIJAOqvgxZRcO+ZMA0GCSqGSIb3DQEBBAUAMA8xDTALBgNVBAMTBE1henUwHhcNMDYxMDAyMTY0M
zQxWhcNMTYwOTI5MTY0MzQxWjAPMQ0wCwYD05BPDxKbb8Ic6HBPDxKbb8Ic6HWpTJpzs
...
ehyejGdw6VhXpf4lP9Q8JfVERjCoroVkiXenVQe/zer7Qf2hiDB/5s02/
+8uiEeqMJpzsSdEYZUSgpyAcws5PDyr2GVFMI3dfPnl28hVavIkR8r05BPDxKbb8Ic6HWpTZMA0GCSqGSIb3DQEBBAUAM
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 NetProfiler or NetExpress appliance, the final step is to add the end entity certificate and the private key as the Local Credentials for this appliance.

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-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7CkgI/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.

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-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7CkgI/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. 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-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC7CkgI/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. 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

CHAPTER 5 Audit trail reports

This chapter describes the Audit Trail report and the Saved Reports feature. It includes the following sections:

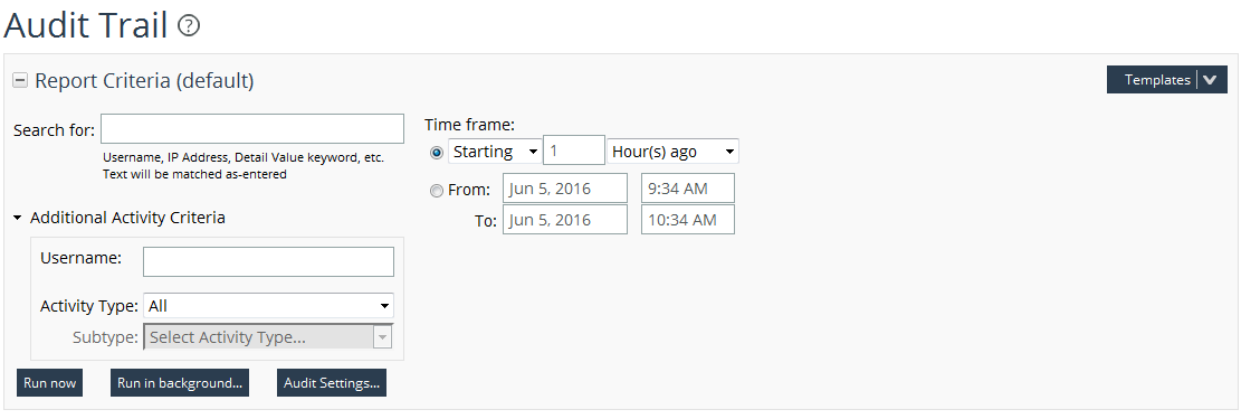
Audit trail

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 5-1. System > Audit Trail Report page Report Criteria section



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

Select either of two options to specify the time frame of the report:

Last -- Specify the most recent number of minutes, hours, days, weeks, months, or years that the report is to cover.

From/To -- Specify the time interval 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

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 system 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.

Report results

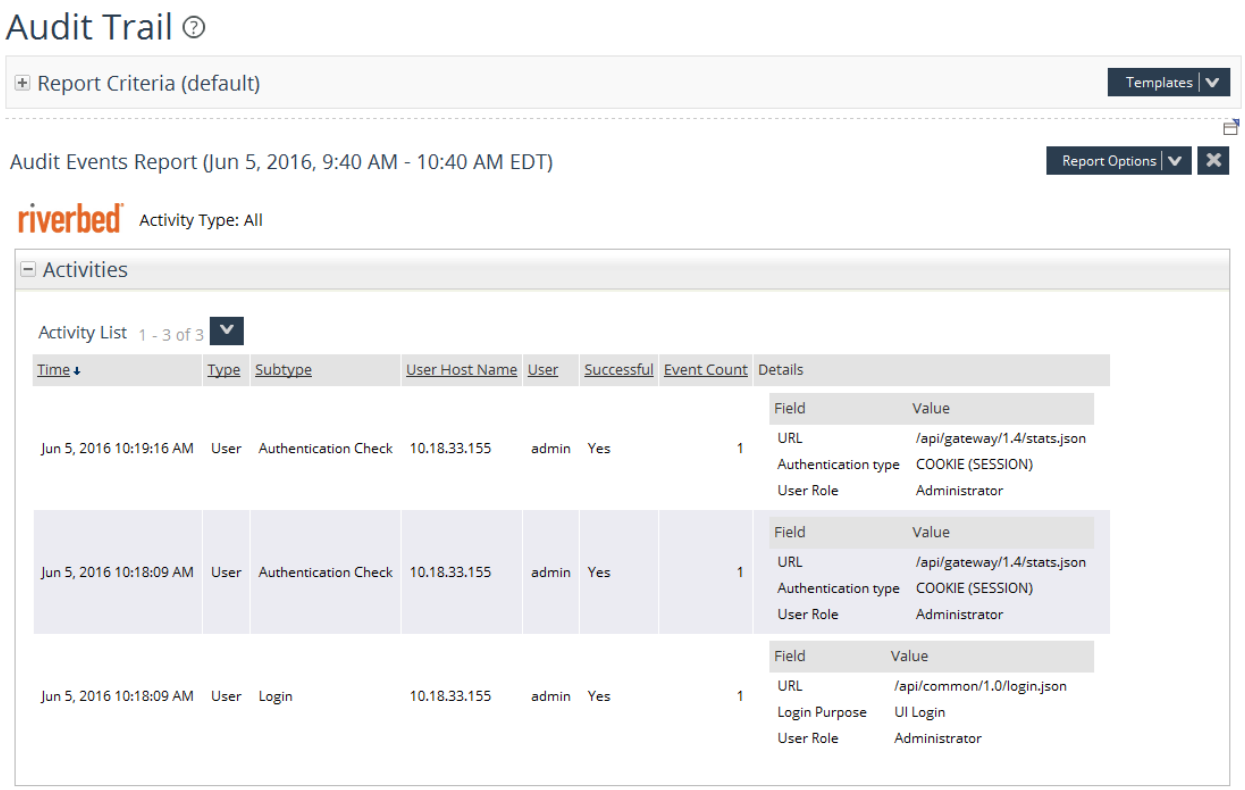
When the report completes it displays an activity list giving the:

- 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.

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

Figure 5-2. System > Audit Trail Report page - Report results



- 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 CVS – 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.

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 5-3. Page display control

Report Options menu

Use the Report Options menu to perform any of the following:

Save as – saves the report on the 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 checkbox 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 checkbox 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.
<	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 > Audit Trail > Audit Settings...
- Configuration > Account Management > RADIUS Settings > RADIUS Servers
- Configuration > Account Management > RADIUS Settings > Role mapping
- Configuration > Account Management > User accounts > Settings...
- Configuration > Appliance Security > Password Security
- Configuration > Appliance Security > Security Compliance
- Configuration > General Settings > Edit /etc/hosts...
- Configuration > Flow Forwarding
- Configuration > NetProfiler Export
- Configuration > Licenses
- Configuration > General Settings > Edit DNS settings
- Configuration > General Settings > Edit NTP settings
- Configuration > General Settings > Edit SNMP settings

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.

Notification activities

The Notification activity type includes the following:

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 zeroes. 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)
- System services stopped (as system account)
- System bootup (as system account)
- System 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.

Saved reports

The Saved Reports page lists completed reports and report templates.

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

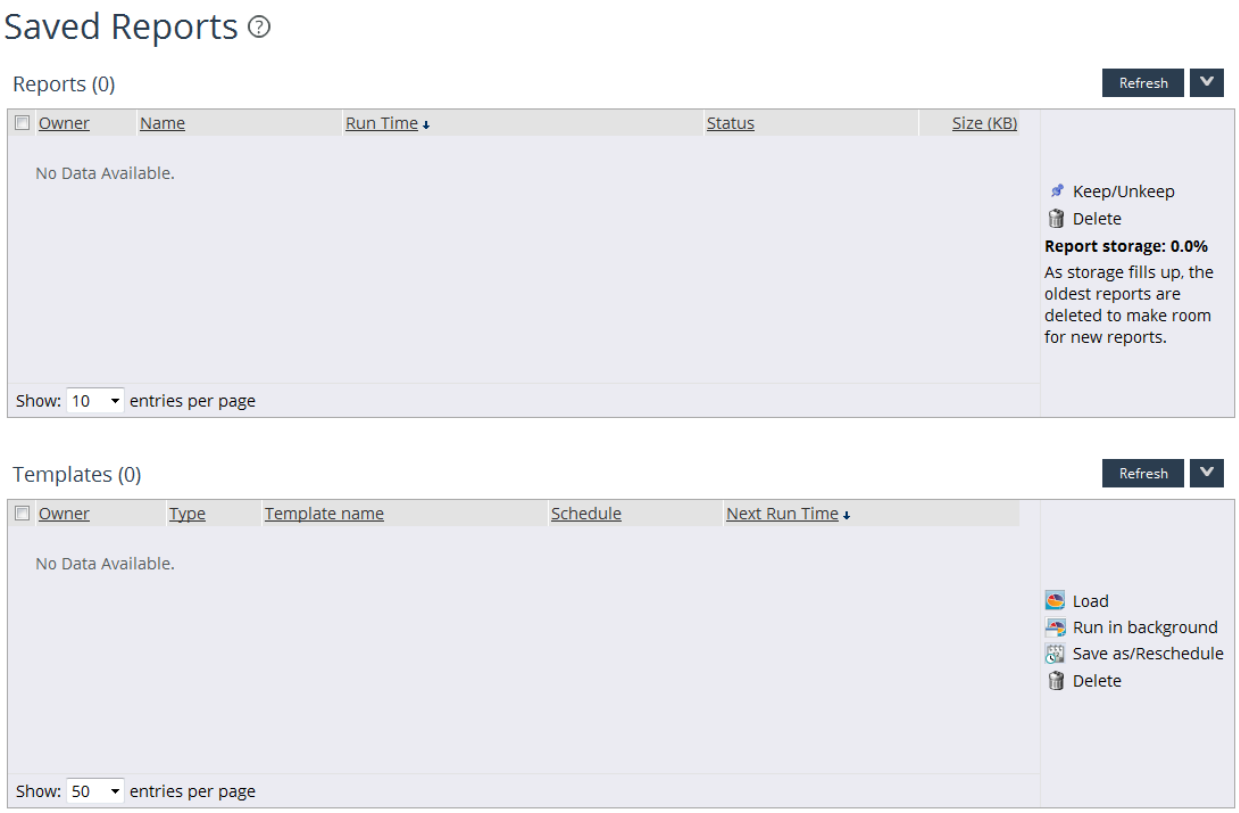
The Templates section lists templates; their owners, types and names; and their schedule and next run time. You can sort the templates by any of these attributes. The Templates section options menu allows you to filter the list of templates to limit the list to your own templates. Additionally, you can 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.

Figure 5-4. Saved Reports page



riverbed
Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

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

Part Number
712-00234-09